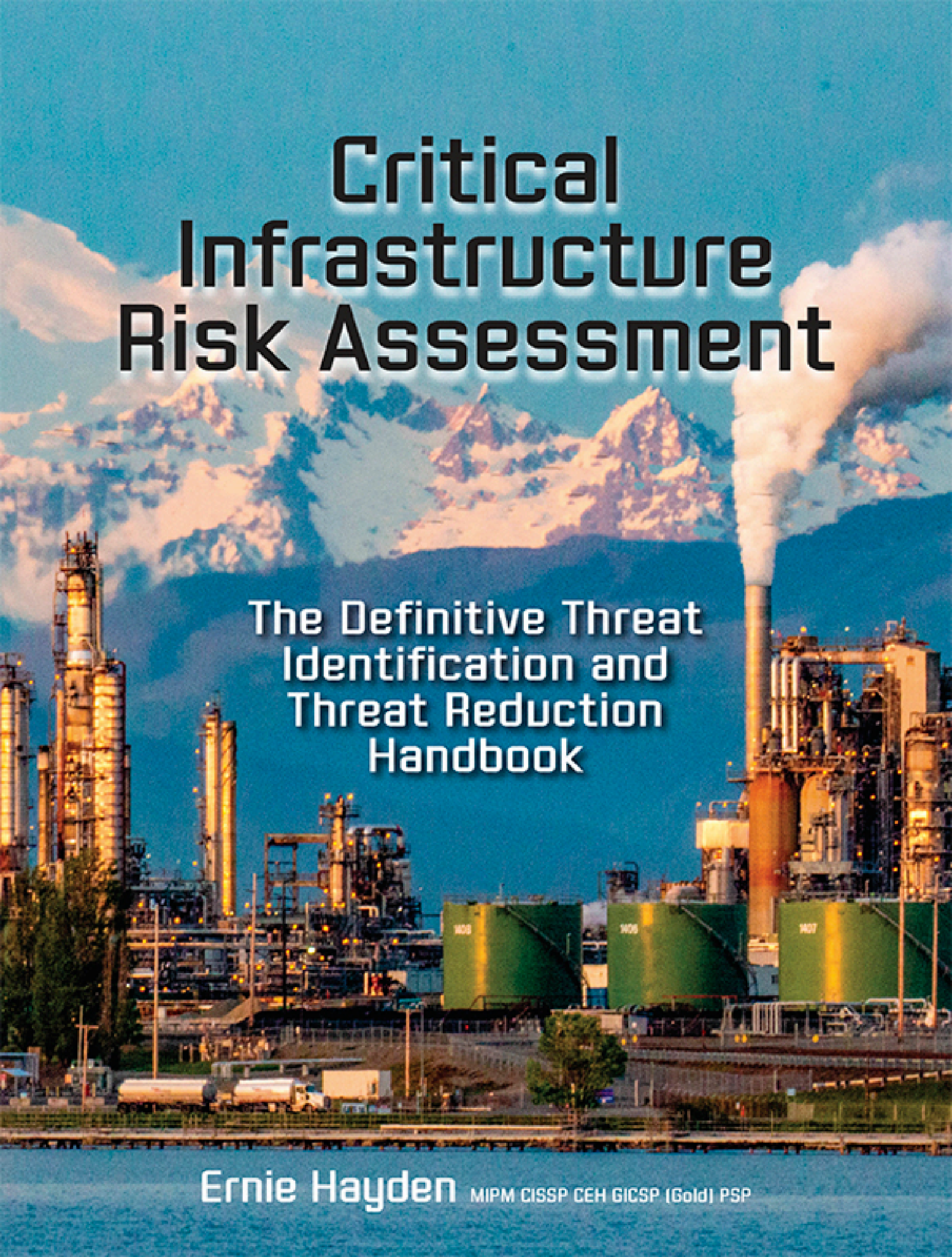
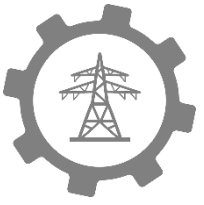

Critical Infrastructure Risk Assessment
The Definitive Threat Identification and Threat Reduction Handbook
Ernie Hayden MIPM CISSP CEH GICSP (Gold) PSP

Critical Infrastructure Risk Assessment

The Definitive Threat Identification and Threat Reduction Handbook

by Ernie Hayden

MIPM, CISSP, CEH, GICSP(Gold), PSP



Print – ISBN: 978-1-944480-71-4

EPUB – 978-1-944480-72-1

WEB PDF – 978-1-944480-73-8

www.rothsteinpublishing.com

Print – ISBN: 978-1-944480-71-4

EPUB – 978-1-944480-72-1

WEB PDF – 978-1-944480-73-8

Library of Congress Control Number: 2020938671

4 Arapaho Road

Brookfield, Connecticut 06804 USA

203.740.7400

info@rothstein.com

www.rothsteinpublishing.com

WHAT YOUR COLLEAGUES ARE SAYING ABOUT *CRITICAL INFRASTRUCTURE RISK ASSESSMENT*

"Critical Infrastructure Risk Assessment is an invaluable reference for assessors, business managers, operators, and planners. And given a rapidly evolving geopolitical situation with nations and other actors motivated to compete and fight across multiple domains, the book could not come at a better time."

Chuck Benson

Director of IoT Risk Mitigation Strategy

University of Washington

"What I particularly like about this book is how self-contained it is in its knowledge of statutes, approaches, resources, and recommendations. You need not look elsewhere for guidance in conducting infrastructure risk assessments. This book is a practitioner's guide that anyone involved in managing, securing, or operating critical infrastructure would find invaluable. The book's subtitle, "Critical Infrastructure Risk Assessment: The Definitive Threat Identification and Threat Reduction Handbook" is no boast as this book lives up to its title."

Tari Schreider

C|CISO, CRISC, MCRP

Cybersecurity Program Strategist, Author & Instructor

"Ernie Hayden has been in the industry for many years and offers a lot of practical advice in this book. The book is laid out in an easy-to-consume manner; it starts with foundational information and proceeds to detail the assessment process from start to finish. This book is a great reference for the facility manager, plant manager or consultant."

Matt B.

CISSP

"Ernie Hayden has provided an extraordinary work that goes beyond its title, addressing Risk Assessment for Critical Infrastructure, with all its elements: threat identification, vulnerability identification, and impact. But more than an academic exercise, Mr. Hayden has taken years of experience as a risk assessor, and provides a handbook that will be invaluable to both the novice assessor, the executive who has been charged with an assignment to have a risk assessment completed, and the seasoned assessor."

Matt Lampe

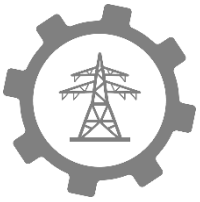
Partner, Fortium Partners

"This handbook was written for anyone involved in critical infrastructure risk assessment. Ernie Hayden guides you through the quagmire of complex terms and essential concepts to gain a clear understanding of critical infrastructure and risk assessment. The responsible executive or risk assessor will want to keep this reference by their side while planning, conducting, or using any risk assessment."

Gil Oakley

Retired

Institute of Nuclear Power Operations



DEDICATION AND ACKNOWLEDGEMENTS

The Genesis

Within the last few years – especially as my 65th birthday crept up on me – I decided to write a book on how to conduct risk assessments. Yes, there are multiple books on the theory of risk assessments but you simply cannot find handbooks identifying the practices and techniques to use when performing a risk assessment of a large facility. Therefore, I began the process of working on a book without a publisher with plans to simply self-publish.

Then, in 2019, Phil Rothstein of Rothstein Publishing posted an invitation to submit book ideas. Since I already had an outline, a chapter or two written, and even a business plan, I submitted the concept material for this book. Phil invited me to write this book for publication as part of the Rothstein Publishing family of books.

I've spent many hours working on this "letter to the industry." I've done this through two house moves and a knee replacement! But I've been persistent and excited to get this knowledge out to the industry and to new engineers who will be conducting risk assessments in the future.

Dedications

I dedicate this book to four people who have had such as strong influence on my life and my pursuit of this idea. First, on the professional front, I dedicate this book to my friends, mentors, and colleagues – Messrs. Mike Assante and Kirk Bailey.

Mike Assante passed away in July 2019. I've known Mike since about 2007 when I first met him in Chicago at an ***Information Security Magazine*** awards event. Since then Mike and I had occasionally exchanged emails as he moved up in the industry to Chief Security Officer of the North American Electric Reliability Corporation (NERC) and then to lead the SANS industrial control security efforts. Our paths literally crossed in 2018-2019 when we were both being treated for cancer at the Seattle Cancer Care Alliance, mine for melanoma and him for his leukemia. At that time, we exchanged many an email, text message, and phone call. Finally, on July 2, 2019, Mike sent me his final text message…" Love you shipmate." He died on July 5th. This book is dedicated to Mike's memory.

Kirk Bailey has been my security mentor and best friend since 2001 after the horrible events of 9/11. We first met when he was the Chief Information Security Officer (CISO) of the City of Seattle then later, when he was CISO of the University of Washington. We were even published on the cover of ***Information Security Magazine*** in January 2005. Kirk has been a positive intellectual influence on me. He has offered me ideas and perspectives on risk and security that I would never have considered without his stories, philosophies, and viewpoints regarding the world around us. Kirk is a brilliant man and I include him in this dedication.

My final, most loving dedication is to my wife, Ginny, and our daughter, Karina. Without their love, patience, and support through many interesting "opportunities" in my life, I would not be where I am today. I love you both so dearly!

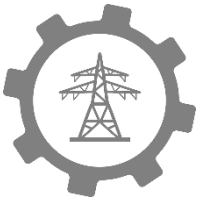
Acknowledgements

My work on this book has not been a solo journey. I would like to thank the following friends and colleagues for their support, counsel, and ideas: Gil Oakley, Jennifer Tavaglione, Jose' Alvarado, Brenda Serna, Kip Boyle, and Peter Gregory. I also want to thank Phil Rothstein and Glyn Davies for their support, encouragement, and editorial improvements.

Finally, I want to thank God for his foundational support and protection.

Ernie Hayden

August 2020



Foreword

by Kirk Bailey

Ernie Hayden knows what he's talking about. I'm not alone in this opinion. There is a long list of his colleagues and appreciative clients in both the public and private sectors who will also salute his expertise and wisdom. If you're a professional facing the challenge of assessing operational and institutional risks for a client or employer, you should keep this book handy – it's a heck of a reference and guide. You should use it and you can trust it.

Ernie and I started working closely together not long after the horrible events of 9/11. We had crossed paths professionally a few years earlier, but in 2002 we found ourselves in mutually challenging jobs. I had just been hired as the first ever chief information security officer (CISO) for the City of Seattle and Ernie was hired as the first ever CISO for the Port of Seattle. We both found ourselves immediately overwhelmed with significant risk management challenges exacerbated by limited budgets, lack of useful tools, growing regulation and compliance issues and the typical political realities found in local government operations. Seeking each other out for help was a necessity.

Seattle and the Port of Seattle own and operate significant essential services, facilities, and infrastructure critical to the Pacific Northwest region and the country in general. They represent the foundation of an economic engine for Washington State and the larger regional economy. The scope and size of the critical infrastructure integral to the City's and Port's operations is vast.

When I came on board as Seattle's CISO, local governments across the country were in hyper-reaction mode. Everyone was concerned about what they needed to do to prevent, prepare, and respond to potential terrorist attacks. There was high anxiety about protecting human life, iconic sites, and critical infrastructure. The Federal government was in overdrive trying to build threat information sharing systems and risk mitigation programs. I was working frantically to assess the cybersecurity-related threats and associated risks – especially as it related to critical infrastructure, essential services, and first responder operations. At the Port of Seattle, Ernie was up to his neck with the same scramble.

During the next few years we dug in and learned plenty about how to best assess and manage potent and complex risks. Early on, we knew that simply following government-issued security and operational checklists was not the answer considering the budget and resource issues in play. We forged a new risk management approach that took into consideration some tough realities.

The good news is that we both achieved some successes. Recalling those days, it's easy for me to say that a primary reason for those successes was Ernie's passion and energy for his work. He used creative approaches to educate his employer about risk issues and kept the focus on the highest priorities as well as what was achievable. His disciplined approach to problem solving and pragmatic thinking, his constant thirst for learning everything on every related subject, his professional connections, his common sense and sense of humor were a huge lift for our professional workloads and worries.

In 2005, I became the University of Washington's first ever CISO. I spent the last 15 years of my career working to build the University's cybersecurity program in a challenging and complex environment. Throughout those years I continued to rely on Ernie's experience and wisdom. Having Ernie as colleague has been like having a private professional consultant on staff all the time.

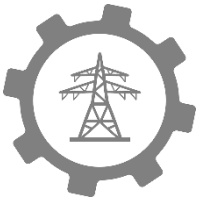
Now Ernie has written this book. That's a very good thing for anyone who will be tasked to perform professional risk assessments. Identifying and understanding risks is not an easy exercise; it is more of a craft than a practice. It requires more common sense, clear thinking, and a touch of imagination to do well. Blindly following checklists in manuals or requirement documents won't cut it. It requires a methodology and mindset that can bring clarity and wisdom into the final report. That's what Ernie is sharing in the following pages.

Kirk Bailey

CISO (retired)

University of Washington

Seattle, Washington



Foreword

by Peter Gregory

I first met Ernie Hayden in 2003 just as I stepped off the stage at the SecureWorld Expo conference in Seattle. Ernie attended my talk and came up to me afterward. He held up a book in his hands and exclaimed, “I’ve read your book!” referring to the first edition of CISSP For Dummies. That meeting would prove to be the start of a going-on-eighteen-years friendship.

Ernie was one of the early instigators of The Agora, a quarterly conclave of information security professionals in the Pacific Northwest. I attended as often as I could, which was usually 2-3 times each year. Ernie was always there, and I always made it a point to speak with him. While we didn’t get into many “deep dive” conversations, I knew right away that he was well learned in information security. As the CISO for the Port of Seattle (which included the shipping port, the cruise ship port, and the airport), Ernie was in the crucible of risk management for multiple high-profile critical infrastructure facilities that were very “out there” and visible to all.

Ernie and I, along with Dave Cullinane and Michael Ray of Washington Mutual Bank (WAMU), Kirk Bailey of the City of Seattle, Barb Padagas of Starbucks, Bruce Lobree of Costco, Ravila White of drugstore.com, and a few others, were co-founders of the Pacific CISO Forum, a peer roundtable of information security leaders in Seattle and beyond. Ernie was as involved as anyone there, and sometimes hosted our quarterly meetings at one of the port facilities.

Ernie was also involved in regional critical infrastructure disaster and attack simulation events. This is all to say that Ernie is a doer, and his community involvement is but one aspect of his professional testimony as a man who cares about his community and the people who live in it.

From then until now, Ernie has held a variety of positions in critical infrastructure protection, and this has taken him around the world where his services were needed. He has become one of the world's premier experts on the topic. For him to write this book is a gracious and generous gift to the profession as a whole. This book is a treasure for the profession and will serve to advance the state of the art of critical infrastructure protection and the professional growth of hundreds or even thousands of others in the profession.

This book is a well-organized, step-by-step, how-to treatise on risk assessment and risk management for critical infrastructure. This book is a high-quality, high-density, low-noise reference to help any professional excel at big-picture or detail-oriented risk management and risk assessment work. It explains the concepts of risk, risk assessment, and the steps for performing a proper risk assessment found in few other texts. I especially appreciate the chapter on observation that instructs the reader how to perform various types of evidence gathering and the value of tech technique. While this book is highly detailed, each chapter contains numerous references where the reader can go for even more in-depth information on each chapter's topics. The book's appendix contains a detailed, lengthy sample risk assessment report that puts many of the topics in the book to use.

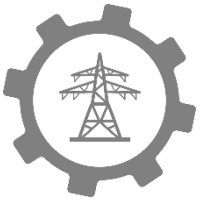
In my experience as an executive consultant and having served dozens of companies and agencies over the past six years, I can confidently say that half or more of all organizations practice little or no risk management at all.

As the need for risk management becomes more apparent in organizations, this book should be in the library of every risk manager as well as every consultant performing risk assessments of critical infrastructure facilities – not on the shelf, but on the desk as a regular desk reference.

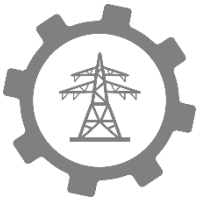
Peter Gregory

CISM, CISA, CIPM, CRISC, CISSP, CCSK, CCISO, QSA

Seattle, Washington



CONTENTS



Introduction

When eating an elephant, take one bite at a time.

– General Creighton Abrams, US Army

or,

A journey of a thousand miles must begin with a single step.

– Lao Tzu

"Oh, Crap!"

Your bosses are worried about the state of your facility. They heard of a major accident at one of your competitor's plants and there is worry your facility could suffer the same fate. During the daily Skype call with headquarters your boss, the Vice President of Operations, gives you the order. "Tell me if we are at risk for this same issue!!" he exclaims. "I want a report emailed to me in two weeks or less. Be sure to let me know if you have any questions or need any help."

The call ends and you begin to ponder – worry, actually. How am I going to "assess" my plant? You vaguely heard about your competitor's event but don't know any of the details. Also, your plant is huge. It covers a square mile including the fence-line, roads, etc. How am I going to "eat the elephant?"

Frankly, this story is not that unusual. There are many instances where seasoned managers are tasked with conducting major inspections and assessments of their operations. But, even new engineers, insurance adjustors, and quality assurance staff are confronted with this same dilemma. How do I start? Where do I start? Exactly what do I do?

Besides, even if I start with such an "assessment or inspection" what do I focus on? Why? What do I do with all the data I accumulate? How do I collect it? How do I organize it?

This book is written after conducting such inspections and assessments for the past 40+ years. I have performed inspections on power plants, factories, refineries, oil and gas pipelines, warships, major sports arenas, 30+ story business buildings, and even my own house. With this experience this book will offer you a methodology along with a collection of tools and techniques to use when conducting risk and vulnerability assessments of large and small industrial facilities and critical infrastructure.

In this chapter you will discover:

- The value of a Risk Assessment.
- Ideas on "where to begin" to perform a Risk Assessment.
- An overall view of the Risk Assessment Process.

Your journey in reading this book will offer you guidance on these key topics:

- What constitutes Critical Infrastructure.
- The fundamentals of risk and the risk equation.
- Overall risk assessment process and methodology.
- Ideas on how to prepare for the assessment.
- Guidance on performing the onsite assessment.
- Entry and exit Meetings.

- Interviewing site personnel.
- Reviewing client documentation.
- Conducting physical plant inspections.
- Performing and documenting observations.
- Developing the final report and findings.
- Details on identifying risk and risk severity ratings.
- Preparation of the initial draft.
- Issuing the report and follow-up.

The advice and suggestions in this book are intended to provide guidance and training for new as well as seasoned staff.

With this book I hope to offer some interesting stories of my own and from experienced assessors and inspectors you can use to become better at your job. You will learn new techniques for attacking the targeted facility, you'll have access to some new checklists and guidelines, and I hope you'll learn what the better "knives and forks" are to use when Eating the Elephant.

Who Should Read This Book?

So, who should read and study this book? Who should include this book on their reference shelf and among their well-worn handbooks? Some candidates include:

- Facility/Plant Maintenance/Operations Managers.
    - Benefit: New way to "look" at the plant, learn new techniques and approaches.
- Corporate and site quality assurance inspectors/auditors.
    - Benefit: Learn techniques to make the inspections valuable and worthwhile.
- Corporate and site training staff.
    - Benefit: Learn new way to teach people how to "inspect" and "assess."
- Corporate Risk Managers

    - Benefit: Have a technique at their fingertips to use for risk assessment and management.
- Consultants
    - Benefit: Learn new techniques and approaches to site visits, inspections, etc.
- Staffs at the Institute of Nuclear Power Operations (INPO), insurance companies, forensic investigators, etc.
    - Benefit: Learn a formal and consistent approach to inspecting/assessing large, complex facilities.

I trust you will find this book beneficial and will offer you many ideas to apply to your current and future jobs. I look forward to your feedback and comments on the book and encourage you to pass along your ideas, suggested changes, etc. to me.

What Risk?

Risk is a situation exposing an individual, machine, or building to danger. A simple definition defining risk is:

Figure 0-1 Classic Risk Equation

The three components of risk are threats, vulnerabilities, and impact or consequences.

You need to understand what constitutes risk before you can effectively perform a risk assessment.

Let's think about some experiences in our lives where we can frame the risk equation.

For example, imagine you are entering an intersection in your new pickup truck. You entered on a green light but to your right a large truck is rapidly driving into the intersection right at your pretty red crew cab!

What is the risk – besides messing up your trousers? The threat is the truck barreling at your truck. The vulnerability is your truck wasn't designed to be

hit at 35 miles per hour by a large vehicle – even with side and front air bags. The consequence could range from death or serious injury to you, death/injury to adjacent cars and pedestrians, death/injury to the truck driver, citations from the police, years of lawsuits, etc.

That is pretty obvious example. What about something more subtle?

I was recently driving by a refinery near my home. I noted a perimeter fence around the facility, but the top barbed wire array was facing towards the plant and not towards the threat (i.e., the terrorist/attacker) as it should. The risk is not particularly profound; however, there is a vulnerability with the barbed wire topper facing the wrong direction which would more readily allow an intruder to enter the refinery perimeter. The consequences could range from sabotage to simple vandalism; but, there are consequences to consider.

Risk is all around us and you really should have an innate sense of what risk includes so you can fix it later.

What is a Risk Assessment?

A comprehensive risk, threat, and vulnerability assessment offers an organized and systematic approach to assessing and documenting risks to the organization. The risk assessment provides an informed list of risks and recommended corrective actions to help the enterprise attack and correct the most serious risks identified. A risk assessment is generally a holistic view of the facility and is intended to view all activities and look for "all hazards" that can constitute risks to the company.

In the US Interagency Security Committee Standard, a risk assessment is the process of evaluating credible threats, identifying vulnerabilities, and assessing consequences. In the National Institute of Standards and Technology (NIST) Special Publication 800-30, ***Guide for Conducting Risk Assessments***, the authors define a Risk Assessment as:

> *The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation…*

As mentioned in his Newcastle Consulting Blog, "The Value of Security Risk Assessments," Mr. J. Kelly Stewart recognizes that properly performed risk assessments can offer the following:

- Reduce long-term costs to the enterprise.
- Improve future operations and aid the organization in achieving strategic objectives.
- Break down organizational barriers.
- Provide important self-analysis.
- Facilitate internal and external communications.
- Help the enterprise avoid major accidents and events.

The Risk Assessment Flow Chart

As we delve into the risk assessment process, it is easy to separate it into three primary phases:

Phase 1: Pre-Assessment Planning

Phase 2: Site Assessment, and

Phase 3: Reporting.

Figure 0-2 provides a map of the risk assessment process:

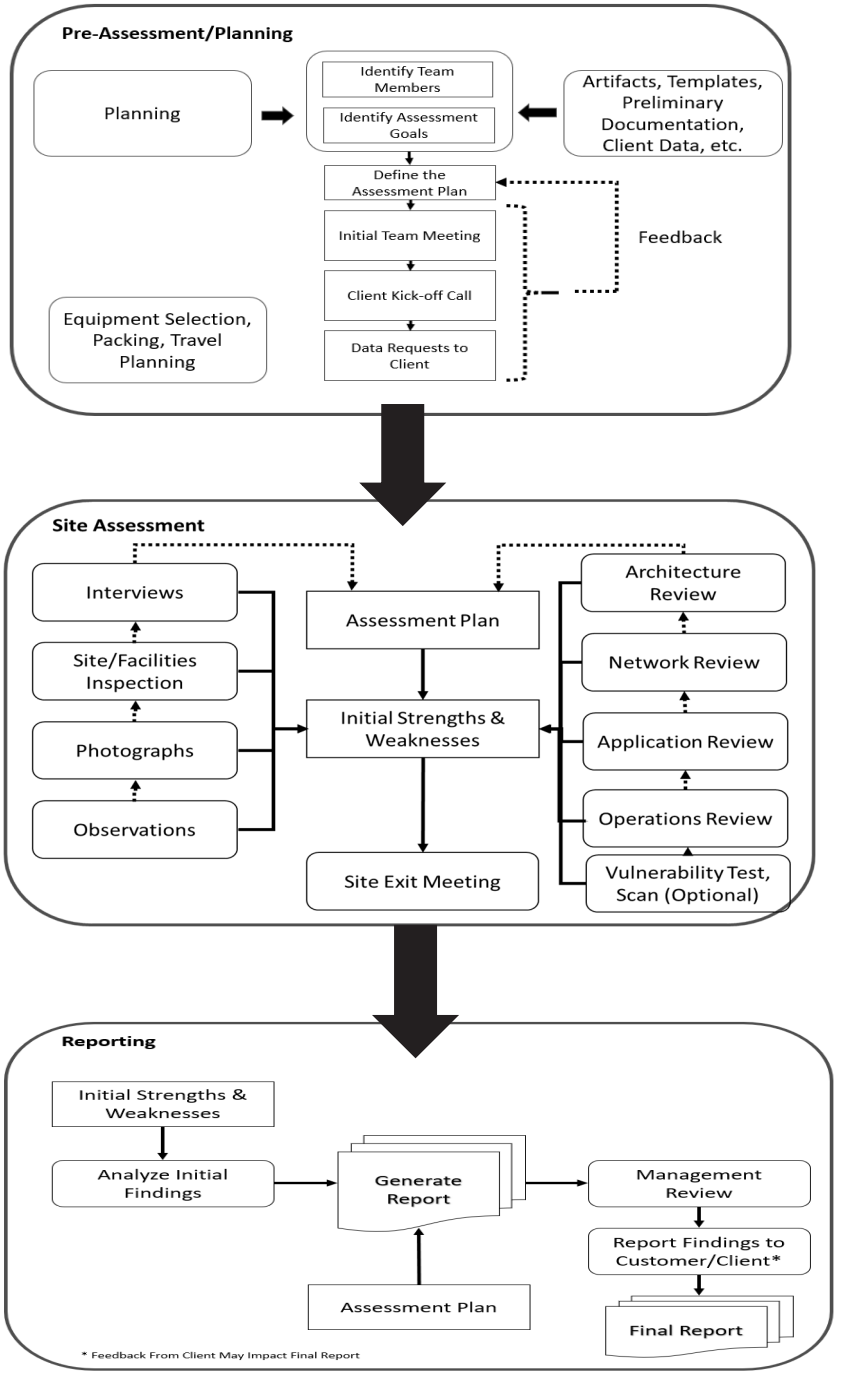


Figure 0-2 Hybrid Facility Risk Analysis Flow Chart

As we proceed with this book, and especially in Chapters 5 through 8, this map will help you understand where in the process we are, and what are the subprocesses in play for each phase.

Your Job

Your job is to jump in and use this handbook to guide you and your teams when you perform risk assessments and other facility analyses. There's a lot going on and I think you'll find this a worthwhile guide. Good Luck! Enjoy your journey as we try to eat the elephant!

REFERENCES

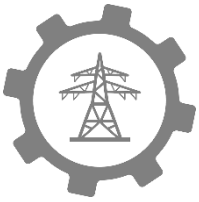
Biss, E. (2020). Eula Biss - Some of the most interesting research that I... Retrieved April 14, 2020, from https://www.brainyquote.com/quotes/eula_biss_724462

Interagency Security Committee. (2013). *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*. Retrieved from https://www.dhs.gov/publication/isc-risk-management-process-aug-2013

Joint Task Force Transformation Initiative. (2012). *Guide for Conducting Risk Assessments (SP 800-30, Rev 1)*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Stewart, J. K. (2019). *The Value of Security Risk Assessments*. Retrieved from https://www.nccllc.net/journal-shift//the-value-of-security-risk-assessments

Tzu, L. (2020). Lao Tzu - Do the difficult things while they are easy and... Retrieved April 14, 2020, from https://www.brainyquote.com/quotes/lao_tzu_398196?src=t_journey



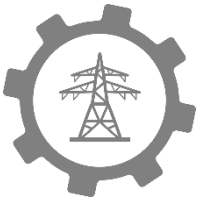
PART I
FOUNDATIONS

Before you can begin to conduct a risk assessment you need to understand a few fundamentals. This section helps you get prepared before you pick up your pen and camera to walk down the site.

Part I includes essential information on the following:

- What constitutes Critical Infrastructure and how is it defined in the US and internationally?
- What is Risk? What are the elements that make up this concept?
- What is a Risk Assessment? What are the different types of risk assessments and their constituent parts?

You should find this an interesting read which will offer the basic information necessary to jump into the risk assessment phase.



Chapter 1

Just What is Critical Infrastructure?

Infrastructure sector is all about building assets for the country. It is part of nation building.[1]

– *Gautam Adani*

This chapter brings you the fundamentals of what constitutes critical infrastructure and the associated government policies from the US and internationally. Since this book will discuss approaches and techniques when performing risk assessments of critical infrastructure, it is important for the executive and the assessment team to understand what critical infrastructure constitutes as a concept, and the history of it becoming a policy idea for government focus. Then, with this knowledge, the assessment process can be more holistic and complete with better understanding of a) what is critical infrastructure, b) what sectors does my

[1] https://www.brainyquote.com/quotes/gautam_adani_680241?src=t_infrastructure

company/institution rely upon, and c) how are the sectors interdependent and what is their effect on my organization's performance and production?

1.1 What is Critical Infrastructure?

So, just what is critical infrastructure?

We are surrounded by it. We use it every day. It keeps our factories running, schools operating, and governments governing.

Infrastructure is very important for the function of a nation as well as an industrial sector.

One of my favorite quotes about infrastructure is from an article in ***The Atlantic*** where the author, Ian Bogost observed[2]:

> *Infrastructure is everything you don't think about. The roads you drive on. The rigs and refineries that turn fossil fuel into the gas that makes your car go. The electricity that powers the streetlights and lamps that guide your way. All these technologies vanish into the oblivion of normalcy*.

To give you a sense of how large this challenge is, the *2003 National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* offered a list of the different sectors and the scope of every way an attacker can penetrate your perimeter digitally and physically. Such a concept of the ways to break into an organization is often referred to as the attack surface.

This updated list is provided in the table below and, upon study, can be not only impressive but overwhelming to national policy makers and defenders.[3]

---

[2] https://www.theatlantic.com/technology/archive/2019/07/manhattan-blackout-reveals-infrastructure-risk/594025/

[3] This list was updated and populated in April 2020 with statistics coming from the US Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) (https://www.cisa.gov/critical-infrastructure-sectors) unless otherwise noted.

Table 1.1 Critical Infrastructure Attack Surface

Agriculture & Food	• 2.1 million farms • 935,000 restaurants • 200,000 registered food manufacturing, processing, and storage facilities • 1/5 of the US economy
Banking & Finance	• 5,177 FDIC Insured Banks[4]
Chemical Industry & Hazardous Materials	• 13,500 Chemical Plants Owned by Over 9,000 Companies[5]

[4] https://www.fdic.gov/bank/statistical/stats/
[5] https://archive.epa.gov/sectors/web/html/chemical.html

Commercial Assets	• Entertainment and Media (e.g., motion picture studios, broadcast media). • Gaming (e.g., casinos). • Lodging (e.g., hotels, motels, conference centers). • Outdoor Events (e.g., theme and amusement parks, fairs, campgrounds, parades). • Public Assembly (e.g., arenas, stadiums, aquariums, zoos, museums, convention centers). • Real Estate (e.g., office and apartment buildings, condominiums, mixed use facilities, self-storage). • Retail (e.g., retail centers and districts, shopping malls). • Sports Leagues (e.g., professional sports leagues and federations).
Dams	• Over 90,000 Dams
Defense Industrial Base	• Over 100,000 Firms

Emergency Services	• Over 50,700 fire stations • Over 120,000 Full-Time Federal Law Enforcement Officers • 787,470 Full-Time State, Local, Tribal, Territorial Law Enforcement Officers • 9,840 Emergency Management Directors • 21,280 Emergency Medical Service Agencies
Energy	• 6,413 Power Plants • 1,100,000 Oil and Natural Gas Production Sites Produced by Over 9,000 Different Companies • 200,000 Miles of High-Voltage Transmission Lines[6] • 5.5 Million Miles of Distributions Lines[7]
Government Facilities	• General Service Administration (GSA) Owns and Leases Over 376.9 Million Square Feet of Space in 9,600 Buildings in > 2,200 Communities[8]
Natural Monuments & Icons	• 62 National Parks[9] • 83 National Monuments[10]

[6] https://www.quora.com/How-many-miles-of-power-lines-are-there-in-the-US
[7] Ibid
[8] https://www.gsa.gov/real-estate/gsa-properties
[9] https://www.nationalparks.org/connect/blog/how-many-national-parks-are-there
[10] ibid

Nuclear Power Plants	• 60 Commercially Operating Nuclear Power Plants with 98 Nuclear Reactors in 30 States
Postal & Shipping	• 137 Million Delivery Sites • 31,324 US Post Offices • 2,000 Federal Express Sites • 5,000 United Parcel Service Sites • 720,000,000 Packages & Letters Shipped Each Day
Public Health	• 6,146 Registered Hospitals[11]
Telecommunications	• 349,344 Cell Towers[12] • 2,668 Internet Service Providers (ISP)[13] • 113,000 Miles of Fiber[14]
Transportation	• 19,700 Public Airports • 4,000,000 Miles of Roadway • 350 Tunnels • 138,000+ Route-Miles of Major Railroads • 600,000+ Highway Bridges • 2,500,000 Miles of Pipelines • 361 Commercial Ports • 25,000 Miles of Waterway • 11,000,000 Containers Enter the US Annually

[11] https://www.aha.org/statistics/fast-facts-us-hospitals
[12] https://www.statista.com/statistics/185854/monthly-number-of-cell-sites-in-the-united-states-since-june-1986/
[13] https://broadbandnow.com/All-Providers
[14] https://www.insider.com/map-long-haul-fiber-optic-cable-network-united-states-internet-2017-7

Water & Wastewater	• 153,000 Public Drinking Water Systems • 16,000 Publicly Owned Wastewater Treatment Facilities

The United States has been a leader in defining critical infrastructure, what it constitutes, and protection policies. However, this is not just an American problem. A *CIPedia*[15] article identified 40 countries that have put forth a definition or at least a list of what constitutes critical national infrastructure. I will provide an in-depth review of the United States and a few other countries and their approach to critical infrastructure definition and protection policy in the discussion which follows.

1.2 Critical Infrastructure Conceptual Development – United States

Infrastructure can be defined as:

> *Basic facilities, services and installations needed for the functioning of a community or society.*

One of the earliest policy reviews identified in my research is from the United States Congressional Budget Office (CBO). The report, *Public Works Infrastructure: Policy Considerations for the 1980's,* was initiated at the request of the Senate Committee on the Budget in order to "…assess the needs of seven infrastructure systems and the costs of meeting those needs." (Bodde, page iii).

In this document, the concept of "critical" infrastructure is not discussed; however, the report identifies the following infrastructure verticals considered for this review.

- Highways
- Public Transit
- Wastewater Treatment
- Water Resources
- Air Traffic Control
- Airports
- Municipal Water Supply.

[15] https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure_Sector

The report did acknowledge that the idea of "infrastructure" can be applied to include social facilities such as schools, hospitals, and prisons as well as industrial capacity. But, the seven systems listed above and reviewed in this policy document "…share common characteristics of capital intensiveness and high public investment at all levels of government. They are, moreover, directly critical to activity in the nation's economy." (Bodde, page 1)

Interestingly enough, even in 1983, this report highlighted challenges with inadequate infrastructure investment resulting in "…deterioration and obsolescence of existing facilities" and insufficient capacity to serve projected growth. (Bodde, page 7)

Overall, this report appears to be the beginning of a policy discussion on infrastructure and subsequent federal investment; however, the concept of "critical" infrastructure is only inferred.

1.2.1 Mid-1990's – Executive Order 13010

In July, 1996, President Bill Clinton issued Executive Order 13010, *Critical Infrastructure Protection.*[16] This appears to be the beginning of policy perspectives identifying selected national infrastructures as "…so vital that their capacity or destruction would have a debilitating impact on the defense or economic security of the United States." (Clinton, Page 3)

The critical infrastructures identified in this Executive Order (EO) included:

- Telecommunications
- Electrical Power Systems
- Gas and Oil Storage and Transportation
- Banking and Finance
- Transportation
- Water Supply Systems
- Emergency Services (including medical, police, fire, and rescue)
- Continuity of Government.

The threats identified in this EO were divided into physical threats to tangible property and threats of "…electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats"). (Clinton, Page 1)

[16] https://www.federalregister.gov/documents/1996/07/17/96-18351/critical-infrastructure-protection

One more key aspect of this EO is the recognition that most critical infrastructure is owned by the private sector and it is imperative that both the federal government and the private sectors work together to develop a strategy for their and the country's mutual protection.

The EO included orders to establish the following:

- President's Commission on Critical Infrastructure Protection (Commission) – This included a Chair as well as representatives from the following departments and agencies:
    - Treasury
    - Justice
    - Defense
    - Commerce
    - Transportation
    - Energy
    - Central Intelligence Agency (CIA)
    - Federal Emergency Management Agency (FEMA)
    - Federal Bureau of Investigation (FBI), and
    - National Security Agency (NSA).
- Principals Committee – This committee was established to review any recommendations or reports regarding critical infrastructure or their threats before submission to the President. The Principals Committee included:
    - Secretary of Treasury
    - Secretary of Defense
    - Attorney General
    - Secretary of Commerce
    - Secretary of Transportation
    - Secretary of Energy
    - Director of the CIA
    - Director of the Office of Management and Budget (OMB)
    - Director of FEMA
    - Assistant to the President for National Security Affairs, and
    - Assistant to the Vice President for National Security Affairs.

The Commission's mission was to identify and consult with public and private sectors that "…conduct, support, or contribute to infrastructure assurance" including owners and operators of critical infrastructure and those with an interest in reliable availability of critical infrastructure.

Additionally, the Commission was charged to perform the following:

- Assess the scope and nature of the threats and vulnerabilities to critical infrastructure.
- Determine legal and policy issues raised in regard to protecting critical infrastructure.
- Recommend a comprehensive national policy and implementation strategy for protecting critical infrastructure.
- Propose legislation, regulations, statutes, etc. as required to implement the recommendations, and
- Produce recommendations and reports to the Steering Committee as they are available.

An interesting and subtle element of the EO is the establishment of the "Infrastructure Protection Task Force" (IPTF) within the Department of Justice. The IPTF was intended to:

- Provide, facilitate, or coordinate the provision of expert guidance to critical infrastructures to "…detect, prevent, halt, or confine an attack and recover and restore service."
- Issue threat and warning notices if advance information is available about a threat.
- Provide training and education on ways to reduce vulnerabilities and respond to attacks on critical infrastructure.
- Conduct after-action analysis to ascertain future threats, targets, or methods of attack, and
- Coordinate with the appropriate law enforcement entities during or following an attack to aid in any criminal investigations.

Of note, EO 13010 was amended by: EO 13025[17], November 13, 1996; EO 13041[18], April 3, 1997; EO 13064[19], October 11, 1997; EO 13077[20], March 10, 1998

In July 1999, Clinton issued Executive Order 13130[21], entitled National Infrastructure Assurance Council. The council is a 30-member panel of private-sector representatives appointed by the President who represent the critical infrastructures identified in EO 13010. The Council was slated to meet periodically in order to:

- Enhance the partnership between public and private sectors.
- Propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes including information and telecommunications systems, and
- Monitor the development of Private Sector Information Sharing and Analysis Centers (PSISACs) and provide recommendations to the National Coordinator and National Economic Council on how these organizations can enhance and support improved cooperation among the PSISACs, the National Infrastructure Protection Center (NIPC – pronounced "NIP-SEA"), and other Federal Government entities.

The council was slated to terminate two years after the EO was issued.

[17] http://www.gpo.gov/fdsys/pkg/FR-1996-11-18/pdf/96-29597.pdf - minor word changes

[18] http://www.gpo.gov/fdsys/pkg/FR-1997-04-08/pdf/97-9200.pdf extended the life of the Commission for an additional 90 days, added the Assistant to the President for Economic Policy and Director of the National Economic Council, and added the Assistant to the President and Director of the Office of Science and Technology Policy.

[19] http://www.gpo.gov/fdsys/pkg/FR-1997-10-16/pdf/97-27644.pdf - designated the Executive Secretary of the National Security Council to exercise the authority to classify information originally as ''Top Secret'' with respect to the work of the Commission staff, the Principals Committee, the Steering Committee, the Advisory Committee, and the Infrastructure Protection Task Force.

[20] http://www.gpo.gov/fdsys/pkg/FR-1998-03-12/pdf/98-6628.pdf - extended some dates from March to September 1998

[21] http://www.gpo.gov/fdsys/pkg/FR-1999-07-19/pdf/99-18476.pdf - establishes the National Infrastructure Assurance Council

Administratively, EO 13130 essentially enhanced the originally proposed Advisory Committee established in EO 13010. Therefore, the Advisory Committee idea of EO 13010 was revoked in Clinton's EO 13138[22].

Apologies to the reader for all these Executive Order references – but, you know how government bureaucracy can be!

1.2.2 1998 – Presidential Decision Directive (PDD) 63

Stemming from recommendations from the President's Commission on Critical Infrastructure Protection established in EO 13010, President Clinton issued PDD 63. Clinton's intent in issuing this directive is included in Section II:

> *It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. I intend that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both the physical and cyber attacks on our critical infrastructures, including especially our cyber systems.* (Clinton 1998, page 2)

[22] http://www.gpo.gov/fdsys/pkg/FR-1999-10-04/pdf/99-25958.pdf - terminated the Advisory Committee to the President's Commission on Critical Infrastructure Protection

CIKR

Around 2009 I was working with my Verizon colleague Mr. Seán McGurk, at a utility in Atlanta. Seán was once a key senior director in the US Department of Homeland Security and often spoke in "gov speak." At this meeting he referred to "CIKR." I asked him later what the term meant

CIKR refers to "Critical Infrastructure and Key Resources" – an umbrella term referring to "…the assets of the United States essential to the nation's security, public health and safety, economic vitality, and way of life."

https://www.dhs.gov/blog/2009/11/19/cikr

The PDD does a few things above and beyond EO 13010. First it includes a definition of "Critical Infrastructure" and secondly, there is raised awareness and focus on the cyber aspects of the country's critical infrastructure and associated vulnerabilities.

The definition of "Critical Infrastructures" included in PDD 63 cites "…those physical and cyber-based systems essential to the minimum operations of the economy and government." (Clinton 1998, page 1)

Although a nice, pristine list of critical infrastructure sectors is not provided per se, Annex A, Structure and Organization, identifies the accountabilities within the US Government for some sectors. The table below summarizes Annex A and the assigned agencies.

Table 1.2 Presidential Decision Directive 63 Lead Agencies and Assigned Sectors

Lead Agencies	Critical Infrastructure Sectors
Commerce	• Information and communications
Treasury	• Banking and finance
Environmental Protection Agency (EPA)	• Water supply
Transportation	• Aviation • Highways (including trucking and intelligent transportation systems) • Mass transit • Pipelines • Rail • Waterborne commerce
Justice/FBI	• Emergency law enforcement services
FEMA	• Emergency fire service • Continuity of government services
Health and Human Services (HHS)	• Public health services, including prevention, surveillance, laboratory services and personal health services
Energy	• Electric power • Oil and gas production and storage

PDD 63 explicitly establishes some organizations and hierarchy to address critical infrastructure threats, vulnerabilities and the associated risks. Key organizations established by the PDD included:

- National Coordinator – focused on critical infrastructure, foreign terrorism and threats of domestic mass destruction including biological weapons.
- National Infrastructure Protection Center (NIPC) was established as a national warning and information center. It was located at the FBI integrating representatives from the FBI, Department of Defense (DOD), United States Secret Service (USSS), Energy, Transportation, CIA and NSA. The private sector was included in this structure which was quite unprecedented! The intent was to improve sharing of threat information.
- Information Sharing and Analysis Centers (ISACs) were encouraged to be set up by the respective private sectors.
- Critical Infrastructure Assurance Office with some emphasis on coordinating national education and awareness programs relative to critical infrastructure protection.

1.2.3 2001 (Post 9/11) Executive Order 13228[23]

Obviously, the events of 9/11 had a profound effect on many defense policies of the US government. President George W. Bush took action to establish the Office of Homeland Security and the Homeland Security Council. He signed the Executive Order on October 8, 2001.

This new office was established to "…develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks." In essence the office's key roles and actions were to:

- Develop and maintain a national strategy for homeland security.
- Detect terrorist threats.
- Prepare for and mitigate consequences of terrorist threats.
- Prevent terrorist attacks on the United States.
- Protect the US and its critical infrastructure from the consequences of terrorist attacks.
- Respond and recover from terrorist threats or attacks.

[23] http://www.gpo.gov/fdsys/pkg/FR-2001-10-10/pdf/01-25677.pdf

- Coordinate domestic response in the event of imminent terrorist threat as well as during and in the immediate aftermath of a terrorist attack within the US.
- Ensure continuity of government (COOG).
- Coordinate communications to the public in the event of a terrorist attack.
- Encourage and invite participation of state and local governments and private entities in carrying out the above functions.

The Homeland Security Council was established to advise and assist the President regarding all aspects of homeland security.

Table 1.3 Executive Order 13228 – Identified Critical Infrastructure Sectors

Sector	New Addition vs. Earlier Executive Orders
Energy Production, Transmission and Distribution Services	
Other Utilities	
Telecommunications	
Facilities that Produce, Use, Store or Dispose of Nuclear Material	X
Privately Owned Information Systems in the US	X (Private Aspect)
Special Events	X
Transportation Systems including Railways, Highways, Shipping, Ports and Waterways, Airports, and Civilian Aircraft	

Sector	New Addition vs. Earlier Executive Orders
Livestock, Agriculture, and Systems for the Provision of Water and Food for Human Use and Consumption	X
Chemical, Biological, Radiological, Nuclear, Explosive, or Other Related Materials that Can be Potentially Used in a Terrorist Attack	X

When compared to the earlier Executive Order lists of CIKR, EO 13228 is exclusively focused on terrorism and the terrorist threats to the US. It does not include or address natural disasters or non-terrorist threats to critical infrastructure. This is later recognized and addressed in subsequent government policy actions.

1.2.4 2001 (Post 9/11) USA PATRIOT Act[24]

Legislatively the USA Patriot Act[25] passed through Congress extremely fast. The legislation was built in response to the attacks of 9/11 and was signed into law on October 26, 2001.

Title X, Miscellaneous, Section 106 of the Act includes a two-page discussion about critical infrastructure protection. On page 401 there is a definition of critical infrastructure:

> *Critical Infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*

[24] https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf
[25] The official title of the USA Patriot Act was *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*.

The only other notable point of discussion here relative to US government review of CIKR is that the policy of the United States was explicitly stated that any physical or virtual disruption of the operation of the critical infrastructures of the United States be:

- rare,
- brief,
- geographically limited in effect,
- manageable, and
- minimally detrimental to the economy, human and government services and national security of the United States (PATRIOT ACT, Page 400).

Otherwise, a specific listing of all defined critical asset categories or sectors was not specifically included in the Act.

1.2.5 2002 National Strategy for Homeland Security[26]

When this strategy evolved, the events of 9/11 were still fresh on everyone's minds and the concerns about terrorist threats were palpable. There was also recognition by the Bush Administration that the US Government was not organized in a way to protect the country effectively from a "non-linear" threat like a terrorist. On July 16, 2002, the ***National Strategy for Homeland Security*** (*Strategy*) was released. As stated in the executive summary:

> *"The purpose of the Strategy is to mobilize and organize our Nation to secure the US homeland from terrorist attacks. This is an exceedingly complex mission that requires coordinated and focused effort from our entire society – the federal government, state and local governments, the private sector and the American people."*

Relative to critical infrastructure and key assets, an entire chapter was devoted to this subject. A new list of 18 Critical Infrastructure Sectors was included on page 32 of the *Strategy*. The *Strategy* modified the list of sectors identified in EO 1338 and included:

[26] https://www.dhs.gov/publication/first-national-strategy-homeland-security

Table 1.4 Critical Infrastructure Sectors from the National Strategy for Homeland Security

Sector	Lead Agency
Agriculture	Department of Agriculture
Food: *Meat and Poultry* *All Other Food Products*	Department of Agriculture Department of Health and Human Services
Water	Environmental Protection Agency
Public Health	Department of Health and Human Services
Emergency Services	Department of Homeland Security
Government: *Continuity of Government* *Continuity of Operations*	Department of Homeland Security All Departments and Agencies
Defense Industrial Base	Department of Defense
Information and Telecommunications	Department of Homeland Security
Energy – Electricity, Oil & Natural Gas	Department of Energy
Transportation	Department of Homeland Security
Banking and Finance	Department of the Treasury
Chemical Industry and Hazardous Materials	Environmental Protection Agency
Postal and Shipping	Department of Homeland Security
National Monuments and Icons	Department of the Interior

This list actually provided the true foundation for future lists of critical infrastructure in subsequent Executive Orders and legislation. Some nuances in this list that may be of interest to the reader include:

- Food is now separate from Agriculture.
- The Defense Industrial Base is cited separately.
- The Chemical Industry is separately identified because it can provide raw materials to the terrorists for bombs and weapons of mass destruction.
- Postal and Shipping is now added.
- National Monuments and Icons are newly included.

That said, in the narrative of the CIKR chapter, the authors also include:

- Individual or localized facilities that deserve special protection because of their destructive potential or value to the local community (However, no examples were provided).
- Certain high-profile events strongly coupled with national symbols or national morale.

Future changes occurred to the designation of critical infrastructure; however, this is and remains the foundation for the future with some relatively minor changes.

1.2.6 2003 National Strategy for Physical Infrastructure Protection

According to the introduction of this new national strategy, there was recognition by the Bush Administration that added focus on the physical aspects of protecting critical infrastructure was necessary. Also, since the Department of Homeland Security (DHS) was now formed[27] and in operation, the Strategy could readily designate DHS as the ultimate owner of this Strategy and the required actions.

This new Strategy was issued in February 2003 and acknowledged the many important steps that public and private entities across the country had taken in response to the September 11, 2001 attacks to improve the security of their critical facilities, systems, and functions. However, the Strategy built upon these efforts and provided direction to the various Federal departments and agencies assigned a role in critical infrastructure and key asset

[27] DHS was created on November 25, 2002.

protection. It also suggested actions state and local governments, private sector entities, and concerned citizens could take regarding critical asset security. (Strategy 2003, page vii)

The Strategy was built upon eight principles which included (Strategy 2003, page ix):

1. Assure public safety, public confidence, and services.
2. Establish responsibility and accountability.
3. Encourage and facilitate partnering among all levels of government and between government and industry.
4. Encourage market solutions wherever possible and compensate for market failure with focused government intervention.
5. Facilitate meaningful information sharing.
6. Foster international cooperation.
7. Develop technologies and expertise to combat terrorist threats, and
8. Safeguard privacy and constitutional freedoms.

Adding to the 2002 Strategy, the 2003 Strategy protecting CIKR added four more key asset "categories" for consideration and action. The four added categories were:

- Nuclear Power Plants
- Dams
- Government Facilities, and
- Commercial Key Assets.

Continuing on a theme, this 2003 Strategy was almost exclusively focused on the terrorist threat and did not raise concerns or suggest actions relative to natural disasters, resilience of the CIKR, etc. This will be addressed in much later Presidential actions.

Overall, the 2003 Strategy is an excellent primer for the critical infrastructure professional or student. The report offers analysis and review of each CIKR sector and the unique challenges each face. For instance, in the Transportation discussion alone, the sector is delineated into:

- Aviation
- Passenger Rail and Railroads
- Highways, Trucking, Bussing
- Pipelines
- Maritime, and
- Mass Transit.

1.2.7 2003 Homeland Security Presidential Directive (HSPD-7)

Homeland Security Presidential Directive 7 was signed on December 17, 2003 and establishes a national policy for Federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks. The directive defines relevant terms and delivers 31 policy statements. These policy statements define what the directive covers, and the roles various federal, state, and local agencies will play in carrying it out.[28]

Essentially, this directive formalized the elements of the 2003 physical security strategy into Presidential orders to the different federal agencies.

The designation of the CIKR sectors and their supporting agencies appears to remain the same as the 2003 physical security strategy discussed above. Also, the only threat against CIKR discussed – again – was terrorism.

1.2.8 2013 Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience (PPD-21)

Almost 10 years after HSPD-7 was issued by the Bush Administration, the Obama Administration promulgated PPD-21[29] along with Executive Order 13636[30] addressing critical infrastructure security *and* resilience with emphasis on both physical and cyber threats. The document also stated:

> *"U.S. efforts shall address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect this infrastructure's interconnectedness and interdependency." (PPD-21)*

These documents were a step change over the directives from the Bush Administration in HSPD-7. PPD-21 does address the physical harm that could affect or destroy CIKR; however, PPD-21 recognizes the doctrine of protecting against "all hazards" rather than terrorism alone.

From the PPD itself the term "all hazards" means a threat or an incident, natural or manmade, that warrants action to protect life, property, the

---

[28] https://www.dhs.gov/homeland-security-presidential-directive-7

[29] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[30] http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

environment, and public health or safety, and to minimize disruptions of government, social, or economic activities.

The hazards considered include:

- natural disasters,
- cyber incidents,
- industrial accidents,
- pandemics,
- acts of terrorism,
- sabotage, and
- destructive criminal activity targeting critical infrastructure.

The PPD still retained the definition of critical infrastructure from the PATRIOT ACT but it modified the number of sectors from 18 to 16; however, some of the sectors were consolidated when compared to HSPD-7. The revised list of sectors is in the table below and is the list in use as of this writing.

Table 1.5 PPD-21 Critical Infrastructure Sectors

Sectors	Sector Specific Agencies (SSAs)
Chemical	Department of Homeland Security
Commercial Facilities	Department of Homeland Security
Communications	Department of Homeland Security
Critical Manufacturing	Department of Homeland Security
Dams	Department of Homeland Security
Defense Industrial Base	Department of Defense
Emergency Services	Department of Homeland Security
Energy	Department of Energy
Financial Services	Department of the Treasury
Food and Agriculture	US Department of Agriculture

Sectors	Sector Specific Agencies (SSAs)
	Department of Health and Human Services
Government Facilities	Department of Homeland Security General Services Administration (GSA)
Healthcare and Public Health	Department of Health and Human Services
Information Technology	Department of Homeland Security
Nuclear Reactors, Materials, and Waste	Department of Homeland Security
Transportation Systems	Department of Homeland Security Department of Transportation
Water and Wastewater Systems	Environmental Protection Agency

PDD-21 included three strategic objectives to be addressed by DHS and the assigned agencies.

1. Refine and clarify functional relationships across the Federal Government and to advance national unity of effort to strengthen critical infrastructure security and resilience.
2. Enable efficient information exchange by identifying baseline data and systems requirements for the Federal Government.
3. Implement an integration and analysis function to inform planning and operational decisions regarding critical infrastructure.

The last strategic objective is interesting because of its planning function. The associated actions here will look at prioritizing assets; anticipating interdependencies and cascading impacts; recommending actions prior to, during, and after an incident or event; and, support incident management and restoration efforts related to CIKR. (PPD-21)

A key deliverable from PPD-21 was an updated *National Infrastructure Protection Plan.*[31] The 57-page plan outlined how government and private sector participants in the CIKR domain community coordinate and interface in order to manage risks and achieve security and resilience.

1.3 International Perspectives on Critical Infrastructure

The United States has been the leader in development of critical infrastructure policies and identification of specific sectors. However, there has been some other effort to designate and delineate CIKR sectors in the remaining Five Eyes[32] countries of Australia, Canada, New Zealand, and the United Kingdom. Let's take a moment and review how these countries address critical infrastructure sectors and some of their unique elements versus the US.[33]

In comparison it appears that the Five Eyes countries have commonly specified the following sectors as critical:

- Communications
- Energy
- Healthcare and Public Health
- Transportation
- Water – Including Wastewater and Storm Water Systems.

[31] https://www.dhs.gov/cisa/national-infrastructure-protection-plan

[32] The Five Eyes, often abbreviated as FVEY, is an intelligence alliance including Australia, Canada, New Zealand, the United Kingdom and the United States. These countries are parties to the multilateral UKUSA Agreement, a treaty for joint cooperation in signals intelligence. For some additional details visit the US National Security Agency web page https://web.archive.org/web/20130613044129/http://www.nsa.gov/public_info/declass/ukusa.shtml

[33] An excellent summary of how the Five Eyes address critical infrastructure is in the Public Safety Canada document *Critical 5 Forging a Common Understanding for Critical Infrastructure* which is included in the References.

1.3.1 United Kingdom

The Centre for the Protection of National Infrastructure (CPNI)[34] is the UK's "Department of Homeland Security. CPNI's role is to support protection of national security against terrorism and other threats. CPNI reports to the Director General of MI5[35], Security Services.

CPNI's charge is to provide assistance and advice to UK entities with responsibility for protecting "…most crucial elements of the UK's national infrastructure from national security threats." (CPNI Web Page)

CPNI's definition of critical infrastructure is a bit varied from the US definition. The UK's characterization of critical infrastructure is:

> *"Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:*
>
> *a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or*
>
> *b) Significant impact on national security, national defence, or the functioning of the state." (CPNI Web Page)*

A table showing the 13 UK-designated national infrastructure sectors is below:

[34] https://www.cpni.gov.uk/about-cpni
[35] https://www.mi5.gov.uk/what-we-do

Table 1.6 UK Critical National Infrastructure Categories

Chemicals
Civil Nuclear Communications
Defence
Emergency Services (Police, Fire, Ambulance Services, and Coast Guard)
Energy
Finance
Food
Government
Health
Space
Transport
Water

Because of the UK's addition of Space to the list of CIKR, perhaps such a category should be included in the US and other global powers delineating their critical infrastructure categories. For instance, in March, 2019, the Indian Government successfully shot down a low earth orbit satellite. Such a weapon could be used in the future to destroy enemy satellites which could disrupt defense, navigation, communication and even agriculture sectors. The US may consider such an attack on its Defense Industrial Base sector; however, designating Space as a CIKR category may make sense after the UK's leadership in this domain.

1.3.2 Canada

The Canadian Government is also in step with the US and UK relative to recognizing that there are critical infrastructure sectors that require focus and attention for protection. Public Safety Canada is the primary agency coordinating critical infrastructure policy and analysis.

The critical infrastructure strategy is included in the National Security Policy and includes three primary areas of focus:

- Cyber Protection
- Physical Protection
- Emergency Management.

The Canadian definition of critical infrastructure is:

> *Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be*

stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence.[36]

The ten Canadian critical infrastructure categories are included.

Table 1.7 List of Canadian Critical Infrastructure Sectors

Health
Food
Finance
Water
Information and Communication Technology
Safety
Energy and utilities
Manufacturing
Government
Transportation

1.3.3 Australia

Australia also has made an effort regarding CIKR. Their definition of critical infrastructure is:

[36] https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx

> *"Critical infrastructure is those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia's ability to conduct national defense and ensure national security."*[37]

It is interesting to observe that the Australians have included the concept of supply chains being part of their critical infrastructure. Also, the Australian approach recognizes that some aspects of CIKR are not physical assets but are in fact networks.

Table 1.8 Australian Critical Infrastructure

Banking and Finance
Communications • Broadcast Media • Postal Services • Telecommunication Networks
Energy • Electricity Systems • Offshore Oil and Gas • Onshore Oil and Gas • Coal Supply
Food Chain
Health • Including supply of blood and blood products

[37] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-frgng-cmmn-ndrstndng-crtcalnfrstrctr/index-en.aspx , Page 8

Transport • Aviation • Land-based Mass Passenger Transit – Including Bridges and Tunnels • Land Freight • Maritime – Shipping and Ports
Water Services
Other Critical Sub-Sectors • Labs Holding High-Risk Biological Agents • Chemical Manufacturing Industry • Defense Industries • Emergency Services

1.3.4 New Zealand

New Zealand has some of the most active earthquake faults on earth. The New Zealand government is taking time to recognize what constitutes critical infrastructure and the associated key sectors.

The New Zealand government has defined critical infrastructure as:

> *"Critical infrastructure is that infrastructure necessary to provide critical services, whose interruption would have a serious adverse effect on New Zealand as a whole or on a large proportion of the population, and which would require immediate reinstatement." (Helm, Page 11)*

The sectors included in the NZ CIKR is limited and are:

Table 1.9 New Zealand's Critical Infrastructure Sectors

Energy
Social Infrastructure
Telecommunications
Transportation
Water

One of the most unique CIKR sectors addressed by the New Zealand Government is the concept of "Social Infrastructure." What does that mean?

The New Zealand Treasury describes "Social Infrastructure" as the features of social organization – such as trust, norms. and networks – that can improve the efficiency of society by facilitating coordinated actions. It also encapsulates the concept of culture such as the values, shared beliefs, customs, behaviors, and identity that underpin the way society works and helps shape and define the New Zealander population. It is similar to the concepts of civil society and social capital. (New Zealand Government, Page 2)

New Zealand appears to be the only country to address the cultural aspects of what is included in the idea of critical infrastructure. This is unique.

1.3.5 European Union

The European Union (EU) has also recognized the need to have a formal program for critical infrastructure protection. Their definitions of critical infrastructure are:

> *European Critical Infrastructures constitute those designated critical infrastructures which are of the highest importance for the Community and which if disrupted or destroyed would affect two or more Member States, or a single Member State if the critical infrastructure is located in another Member State. This includes transboundary effects resulting from interdependencies between*

> *interconnected infrastructures across various sectors. (EU Communication 2006, Page 4)*
>
> *"Critical Infrastructure" means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions. (EU Directive 2008, Page 77)*

In 2008 the Council of the European Union (EU) promulgated Council Directive 2008/114/EC regarding the identification and designation of European critical infrastructures. The document recognizes that the European programme for critical infrastructure protection (EPCIP) is based on an "all hazards" approach versus a single terrorism threat. Hence, natural disasters, man-made, and technological threats are taken into account. However, terrorism is still given priority.

Because of its multi-country environment, the EU explicitly takes into account "interdependencies between interconnected infrastructures." (EU 2008, Page 75) For instance, the Directive also has a definition for "European Critical Infrastructure (ECI)."

> *"European critical infrastructure" or "ECI" means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure. (EU Directive 2008, Page 77)*

The 2008 Directive, Annex I includes a list of ECI Sectors; however, it is incumbent upon each Member State to identify potential ECIs that satisfy both the cross-cutting and sector criteria defined in the Directive. Also, the list of ECI Sectors in Annex I "…does not generate a generic obligation to designate ECI in each sector." (EU Directive 2008, Page 81) Therefore, the EU has not developed precise, all-encompassing lists in a manner such as

the US or the other members of the Five Eyes have as discussed earlier. Instead, there is reliance on each Member State to designate their own critical infrastructure.

Table 1.10 List of European Critical Infrastructure (ECI) Sectors

Sector	Subsector	Additional Notes
Energy	Electricity	Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity
	Oil	Oil production, refining, treatment, storage, and transmission by pipelines
	Gas	Gas production, refining, treatment, storage, and transmission by pipelines. Liquid Natural Gas (LNG) terminals
Transport	Road Transport Rail Transport Air Transport Inland Waterways Transport Ocean and Short-Sea Shipping and Ports	

1.3.6 Germany

Since 2009 Germany has had a formalized critical infrastructure program and strategy overseen by the Federal Ministry of the Interior (Federal MOI).

Of course, the strategy does include a definition of what constitutes critical infrastructure:

> *Critical Infrastructures (CI) are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences. (German Ministry of Interior, Page 4)*

A unique element added to this strategy as compared to the others reviewed above is the inclusion of a definition of the term "criticality." This term aided the German government in determining what sectors are truly important enough to be designated as Critical Infrastructure. The definition of criticality is cited as:

> *Criticality is a relative measure of the importance of a given infrastructure in terms of the impact of its disruption or functional failure on the security of supply, i.e., providing society with important goods and services. (German Ministry of Interior, Page 7)*

The criticality of an infrastructure may be systemic or symbolic in nature or both. For instance, electricity is systemic since it supports so many of the different elements of society from power supply for lighting to electricity for telecommunications and information technology to the operation of the media.

Relative to symbolic infrastructure, such a category of CIKR would be of "…critical significance to its important role in creating a sense of identity, emotionally unsettle a nation's society and psychologically have a lasting unbalancing effect on it." (German Ministry of Interior, Page 7) Although not stated by the Germans, the loss of the Twin Towers on 9/11 can immediately be considered the loss of a "symbolic infrastructure."

Alternatively, loss of a critical national monument due to natural disasters or terrorism would again be an impact on symbolic infrastructure.

The German critical infrastructure protection strategy identified a table of infrastructure sectors and is included below.

Table 1.11 German Critical Infrastructure Sectors

Technical Basic Infrastructure	Socio-economic Services Infrastructure
Power Supply	Public Health; Food
Information and Communications Technology	Emergency and Rescue Services; Disaster Control and Management
Transport and Transportation	Parliament; Government; Public Administration; Law Enforcement Agencies
Drinking Water, Water Supply and Sewage Disposal	Finance; Insurance Business
	Media; Cultural Objects (Cultural Heritage Items)

The German strategy does recognize the terrorist threat to its CIKR but it also acknowledges that natural disasters/events and technical failure and human error also can seriously impact critical infrastructure. I especially liked the unique German approach in the table below regarding the risks they have considered – some of which I've not seen in other national CIKR policies and strategies such as failures of organizations.

Table 1.12 German Strategy for Critical Infrastructure Protection

Natural Events	Technical Failure / Human Error	Terrorism, Crime, War
Extreme Weather Events	System Failure – Insufficient or Excessive Complexity of Planning, Defective Hardware and/or Software Bugs	Terrorism
Forest and Heathland Fires	Negligence	Sabotage
Seismic Events	Accidents and Emergencies	Other Forms of Crime
Epidemics and Pandemics in Man, Animals, and Plants	Failures in an Organization – Shortcomings in Risk and Crisis Management, Inadequate Coordination and Cooperation	Civil Wars and Wars

The German strategy also takes explicit account of the concept of "interdependencies" between the different sectors. Hence, the failure or degradation of one sector could lead to cascading failures that lead to more complex recovery and restitution activities. The concept of critical infrastructure interdependency will be discussed later on in this chapter.

1.3.7 Netherlands

In 2014, the Dutch government reviewed their national critical infrastructure. The driver for this review was that Dutch society had become more dependent on critical infrastructure, for example on IT systems and electricity, and its failure had become less acceptable in society. Furthermore, the interdependencies of critical infrastructures made it

increasingly difficult to predict cascading effects. This review of the national policy on critical infrastructure aimed for an updated, more rigorous approach to protecting Dutch CIKR.

The result of the Dutch analysis and review led them to shift away from critical infrastructure "sectors" to "critical processes." Also, there was a recognition that not all processes in a sector are considered critical.

Additionally, this review resulted in a modified focus on the impact of criticality and the impact of a disruption on critical processes.

The fascinating result in this new and unique approach to critical infrastructure policy led to development of one comprehensive list of critical processes in the Netherlands. Also, critical infrastructure was classified into two categories – A and B – in order to prioritize responses during incidents. The ultimate result was "tailor-made" arrangements for each critical process on the national and regional level.

1.3.8 Japan

The Japanese government defines critical infrastructure as:

> *Critical infrastructure is the backbone of national life and economic activities formed by businesses providing services that are extremely difficult to be substituted; If the function of the services is suspended, deteriorates or becomes unavailable, it could have a significant impact on the national life and economic activities. (Government of Japan, Page 63)*

Japan's national critical infrastructure is categorized by 13 critical sectors:

Table 1.13 Japanese Critical Infrastructure Sectors

Sector	Critical Infrastructure Services
Information and Communication Services	• Electrical Communication Services • Broadcasting Services • Cable TV Services
Financial Services	• Banking Services • Life Insurance Services • General Insurance Services • Securities Services
Aviation Services	• Air Transportation Services for Passengers and Cargo • Reservations, Ticketing, Boarding/Loading Procedures • Flight Maintenance • Flight Plan Creation
Railway Services	• Passenger Transport Services • Ticketing, Entry and Exit Procedures
Electric Power Supply Services	• General Electric Power Transmission and Distribution Services • Electric Power Generation Services
Gas Supply Services	• General Gas Supply Services
Medical Services	• Medical Examination
Water Services	• Supply of Water Through Water Services

Sector	Critical Infrastructure Services
Logistics Services	• Motor Truck Transportation Business • Shipping Business • Port Transportation Business • Warehousing Business
Chemical Industries	• Petrochemical Industries
Credit Card Services	• Credit Card Settlement Services
Petroleum Industries	• Petroleum Products Supply Services

1.4 Critical Infrastructure – A Missing Sector

In 2016 the United States presidential election was marred by Russian interference in the vote and influence on the electorate. In July 2019 The US Senate Intelligence Committee concluded election systems in all 50 states were targeted by hackers linked to the Russian government.[38] However, after reviewing the lists of designated critical infrastructure in the US, the Five Eyes countries, and even in the CIPedia list referred to earlier in this chapter, I did not see election and voting infrastructure highlighted.

In January 2017, after the 2016 election was finalized, then US Secretary of Homeland Security, Jeh Johnson, argued that election infrastructure should be designated as its own, standalone, critical infrastructure sector. He writes:

> *"I have determined that election infrastructure in this country should be designated as a subsector of the existing Government Facilities critical infrastructure sector. Given the vital role elections play in this country, it is clear that certain systems and assets of election*

[38] https://www.theverge.com/2019/7/25/8930985/russia-targeted-election-systems-in-all-50-states-senate-concludes

infrastructure meet the definition of critical infrastructure, in fact and in law.

I have reached this determination so that election infrastructure will, on a more formal and enduring basis, be a priority for cybersecurity assistance and protections that the Department of Homeland Security provides to a range of private and public sector entities. By "election infrastructure," we mean storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments.

... This designation does not mean a federal takeover, regulation, oversight or intrusion concerning elections in this country. This designation does nothing to change the role state and local governments have in administering and running elections."[39]

[39] https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

A contemporary example where the list of critical infrastructure and the associated definitions has been used for state policy is during the Covid19 pandemic of 2020. For instance the Governor of the State of Washington required all non-essential businesses to shut down through April and part of May 2020. However, there was a question as to what an "essential" business was.

Therefore, the state government used the US list of Critical Infrastructure to identify essential services and businesses.

As of this writing the 2020 election activities are rapidly accelerating with the Democratic debates in play. Even at the DefCon conference in Las Vegas in August 2019 there was some added focus on voting machine security and hardening.

The point here is that election infrastructure for any country should be designated critical infrastructure and, as the US 2016 election demonstrated, the election storage facilities, polling places, vote tabulation locations, and the IT that supports all of this should have added protections and oversight by national and regional governments.

1.5 Critical Infrastructure Interdependencies

When the discussion turns to critical infrastructure and interdependencies the seminal paper on this subject is *Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies* by Steven Rinaldi, James Peerenboom, and Terrence Kelly. This white paper was published in December 2001 and continues to be a "textbook" on the subject. Their work is beyond reproach and continues to educate and train the future global critical infrastructure students and defenders.

As examples of critical infrastructure interdependencies, we immediately think of electric power outages and their impact on our cities. But there are other impacts that are more subtle.

1.5.1 Seattle Tacoma Airport Oil Pipeline Interdependencies

For instance, consider the Olympic Pipeline. The pipeline is operated and managed by British Petroleum (BP) and is a 400-mile interstate pipeline system that includes 12-inch, 14-inch, 16-inch, and 20-inch pipelines. The pipeline runs along a 299-mile corridor from Blaine, Washington to Portland, Oregon. The system transports gasoline, diesel, and jet fuel. This fuel originates at four Puget Sound refineries, two in Whatcom County and two in Skagit County, and is delivered to Seattle's Harbor Island, Seattle-Tacoma International Airport, Renton, Tacoma, Vancouver Washington, and Portland, Oregon.[40]

As early as 2001 Seattle-Tacoma International Airport management was concerned about their reliance on and interdependency with Olympic Pipeline to provide jet fuel to the airport. The airport consumes 1.5 million gallons of jet fuel a day and stores about 24 million gallons of jet fuel in tanks at the south end of the airport. The tank capacity has not expanded even though the airport has undergone substantial expansion. The tanks are connected to the Olympic Pipeline and are usually topped off when they are half full.

Because of SeaTac's reliance on the Olympic Pipeline – and because they do not rely on or use truck deliveries, the airport has had several near-misses when it comes to failures on the pipeline reflecting on the airport's operations.

There were instances where the airport came very close to running out of fuel due to an extended shutdown of the Pipeline in 2001 and 2004. In one case the airport avoided complete loss of fuel because of some mandated aircraft inspections at Alaska Airlines (MD-80s) thus lowering fuel consumption. In another case the Nisqually Earthquake of 1999 impacted the pipeline delivery to the airport; however, the airport control tower was out of service due to the earthquake, so fuel consumption was much lower than normal.

Singular reliance on one jet fuel delivery mechanism can be problematic for entities like Seattle-Tacoma airport.

[40] https://www.bp.com/en_us/united-states/home/products-and-services/pipelines/our-pipelines.html#accordion_olympic

1.5.2 Critical Infrastructure Interdependencies with Orbiting Satellites

In his article "What Would Happen If All Our Satellites Were Suddenly Destroyed?"[41] George Dvorsky provides a stark description of how important orbiting satellites are for our economy to function. Dvorsky's title makes you wonder about the probability of such an event where all satellites are destroyed; however, he explains that this is not as outlandish as it seems. Dvorsky argues we could lose a lot of satellites due to a massive geomagnetic solar storm – a natural event and not war-related.

Loss of our satellites could result in loss of geographic positioning system (GPS) signals necessary for navigation and time signals for electric substations, critical facilities, communications, etc. Loss of GPS would also affect air traffic and airline travel/routing.

Loss of the satellites would also result in stressing the ground-based communications systems such as underwater cables and telecommunications lines. All international calls and data traffic would have to be re-routed thus placing substantial pressure on terrestrial and undersea lines. Oversaturation would stretch the capacity of these systems to the limit, preventing many calls from going through. Hundreds of millions of Internet connections would vanish or be severely overloaded. A similar number of cell phones would be rendered useless. In remote areas, people dependent on satellite for television, Internet, and radio would practically lose all service. (Dvorsky, 2015)

Failure of many if not all of the satellites would also severely impact the military and its ability to communicate, launch weapons, etc. Don't forget farmers, TV meteorologists, militaries, air traffic controllers, etc. rely on weather satellites. The US National Oceanic and Atmospheric Administration (NOAA) has estimated that weather satellites save as much as $3 billion in lives and property damage during hurricane season. (Dvorsky, 2015).

[41] https://io9.gizmodo.com/what-would-happen-if-all-our-satellites-were-suddenly-d-1709006681

1.5.3 The Expansive Nature of Interdependencies and Critical Infrastructure

Now, let's better understand how reliant our critical infrastructure is on deliveries and services from other CIKR. In other words, if I break one critical infrastructure, how can it break other systems?

Using the schematic of the petroleum "system," let's dissect the interdependencies.

Figure 1-5: Overview of the Petroleum System

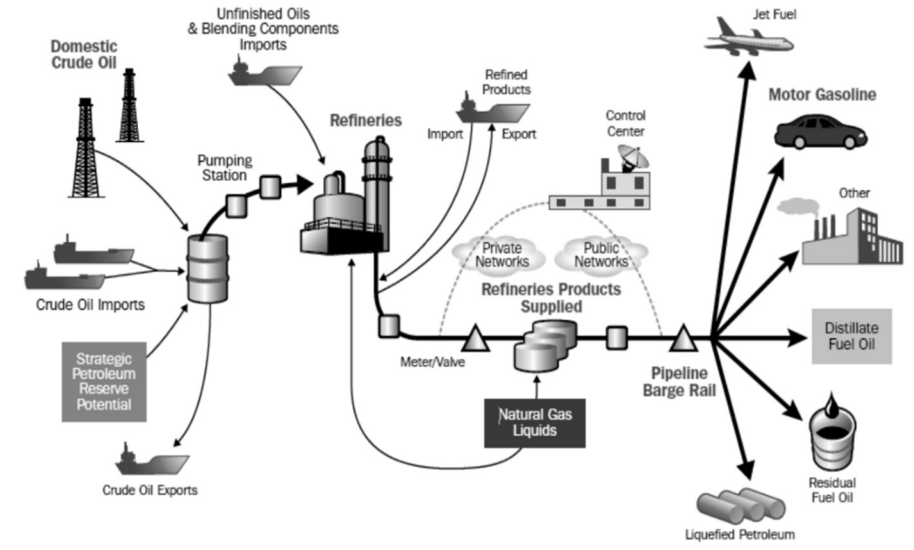


Figure 1-1 Petroleum System Interdependencies (US Department of Energy, 2007 – Page 13)

Table 1.14 Petroleum System Interdependencies

Sectors	Impact or Effect on Petroleum System?
Communications	☑ Communications are important for system status, system control, maintenance and operations crew coordination.

Sectors	Impact or Effect on Petroleum System?
Dams	☑ Failure of a Dam may result in flooding of the refinery, distribution points or failure of electric generation.
Emergency Services	☑ Loss of Emergency Services may require shutdown of refineries, pipelines, storage facilities, etc.
Financial Services	☑ Loss of Financial Services may impact oil trading, petroleum prices.
Information Technology	☑ IT is critical for signal transport and management for industrial control systems, plant and pipeline operation, market communications, inventory management.
Transportation Systems	☑ Transportation impacts the ability to supply the refineries with raw materials but also to transport petroleum products to end users.
Water and Wastewater Systems	☑ Water is used for plant cooling, fire protection, shipping.

Failure of one or more services or capabilities in the petroleum "system" may not necessarily cause failure of the entire system; however, loss of one of these capabilities may be reflected throughout the system in the form of plant shut downs, reduced operations and production, and indirect impacts to the global economy.

In their seminal work, Rinaldi, et al, defined a ***dependency*** as a "…linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other." For instance, electric power is a supported infrastructure. That is, the electric power is supported by natural gas, banking and finance, telecom, transportation, and water critical infrastructures.

They then go on to define ***interdependency*** as "A bidirectional relationship

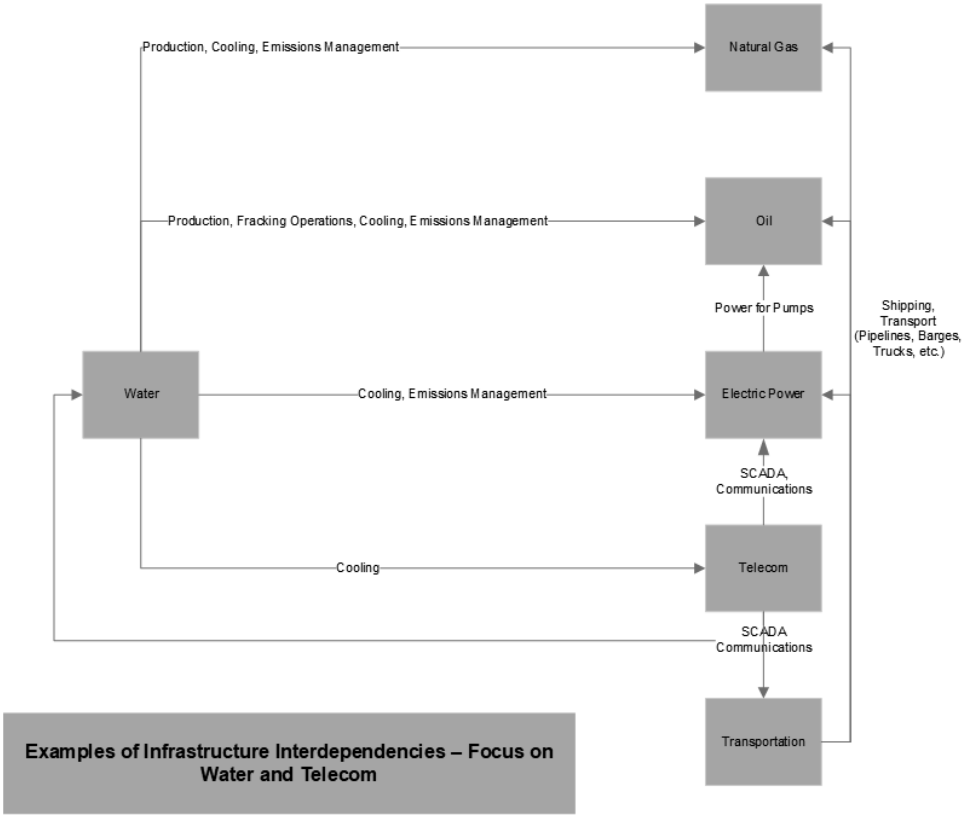


Figure 1-2 Examples of Infrastructure Interdependencies

between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other. More generally, two infrastructures are interdependent when each is dependent on the other." Interdependencies can be shown in the example graphic above (based on Figure 3 of the Rinaldi paper).

What are the types of interdependencies? They include:

- Physical Interdependencies – a physical connection or linkage between the inputs and outputs of the critical infrastructure.
- Cyber Interdependencies – an interconnection due to electronic/digital information exchange and control between critical infrastructures.

- Geographic Interdependencies – an interdependence between critical infrastructures due to their geographic proximity or adjacency.

Rinaldi also cites the Logical Interdependency as a fourth type. Rinaldi observes, "Logical interdependencies may be more closely likened to a control schema that links an agent in one infrastructure to an agent in another infrastructure without any direct physical, cyber, or geographic connection." One example of this "Logical Interdependency" could be the impact of the California power crisis caused by Enron in 2000 and its impact on the financial markets. Another example is when fuel prices are low, there is increased road traffic. Essentially, Logical Interdependencies are predicated on human decision-making.

1.6 Conclusion

This chapter is a foundation for the balance of this book. Our discussions here are intended to assist those performing critical infrastructure risk assessments to not only understand what constitutes critical infrastructure, but it is also intended to aid the inspector in understanding how the CIKR is interconnected with other critical operations and sectors.

As a reminder, critical infrastructure includes those systems and components deemed fundamental to the economy and society to function. Critical infrastructure can be segmented into a variety of sectors to make it simpler to understand and manage.

As the assessment begins and the inspector is evaluating either component or system risk, they need to best understand a) is this part of the critical infrastructure schema, and b) what are the interdependencies I should consider?

Now that we have this understanding, our next chapter will go into detail to educate the risk assessment team on the concept of risk and its fundamental attributes.

1.7 Questions for Further Thought and Discussion

1. What has your country and local government done to designate critical infrastructure sectors? What was their purpose?

2. Does your company consider government critical infrastructure protection policy in its corporate security policies and procedures? Why or why not?
3. When you look at your own company, what critical infrastructure sectors are you dependent upon? What are you doing to ensure these sectors and services are continuously provided and without interruption?
4. After reading this chapter what critical infrastructure sectors are missing? Why?
5. Of the four types of interdependencies – cyber, physical, geographic, and logical – which one is most important to the operations of your company/city/institution? Which one has had the most impact on your entity's performance?

REFERENCES

Bodde, David L., et al. (1983). *Public Works Infrastructure: Policy Considerations for the 1980's*. Washington DC. Retrieved from https://www.cbo.gov/sites/default/files/98th-congress-1983-1984/reports/doc20-entire.pdf

Bogost, I. (2019). Revenge of the Power Grid. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2019/07/manhattan-blackout-reveals-infrastructure-risk/594025/

Clinton, B. (1998). *Presidential Decision Directive/NSC-63 Critical Infrastructure Protection*. Retrieved from https://fas.org/irp/offdocs/pdd/pdd-63.htm

Clinton, B. (1996). *Executive Order 13025: Amendment to Executive Order 13010, the President's Commission on Critical Infrastructure*. Retrieved from https://fas.org/irp/offdocs/eo13025.htm

Clinton, B. (1996). *Executive Order 13010: Critical Infrastructure Protection*. Washington, DC. Retrieved from https://fas.org/irp/offdocs/eo13010.htm

Commission of the European Communities. (2006). *Communication from the Commission on a European Programme for Critical Infrastructure Protection*. Brussels. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN

Council of the European Union. (2008). Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. *Official Journal of the European Union*, 75–80. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

German Federal Ministry of the Interior. (2009). *National Strategy for Critical Infrastructure Protection (CIP Strategy)*. Berlin, Germany. Retrieved from https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.html;jsessionid=0866A3F0C23648DAC59B118CBD0DAF83.2_cid295

Government of Canada. (2014). Forging a Common Understanding for Critical Infrastructure. Retrieved July 29, 2019, from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-frgng-cmmn-ndrstndng-crtcalnfrstrctr/index-en.aspx

Government of Canada. (2004). *Securing an Open Society: Canada's National Security Policy*. Ottawa, Ontario, Canada. Retrieved from http://publications.gc.ca/site/eng/9.686980/publication.html

Government of Canada. (2019). Critical Infrastructure. Retrieved July 29, 2019, from https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx

Helm, P. (2008). Critical Infrastructure Resilience: Perspective from New Zealand. In *International Disaster and Risk Conference*. Davos, Switzerland. Retrieved from http://www.alg.org.nz/publicdownload.ashx?q=q6bLKI8Z6JgNEP%2F8jUVYnvBIX3FUCU5Z9oOTdUN52wXfqaGmaCJnKkP4WJ3o2niXga%2BgX%2BMWZh8PjqpnhiiqlA%3D%3D

Maccaulay, T. (2019). The Danger of Critical Infrastructure Interdependency | Centre for International Governance Innovation. Retrieved August 12, 2019, from https://www.cigionline.org/articles/danger-critical-infrastructure-interdependency

Netherlands National Coordinator for Security and Counterterrorism - Ministry of Justice and Security. (n.d.). Review of policy on critical infrastructure. Retrieved August 12, 2019, from https://english.nctv.nl/topics/critical-infrastructure-protection

New Zealand Government - Treasury. (2013). Living Standards: A Short Guide to "Social Infrastructure." Retrieved from https://treasury.govt.nz/sites/default/files/2017-12/hls-ag-socinfr-jan13.pdf

Rinaldi, S., Peerenboom, J., Kelly, T. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies," Retrieved July 9, 2020 from https://www.researchgate.net/publication/3206740_Identifying_understanding_and_analyzing_critical_infrastructure_interdependencies

Safi, M. (2019). Modi's space weapon announcement struggles for lift-off | World news. Retrieved July 29, 2019, from https://www.theguardian.com/world/2019/mar/27/modi-space-weapon-announcement-struggles-for-lift-off

U S Government. (2003). National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. Retrieved July 24, 2019, from https://georgewbush-whitehouse.archives.gov/pcipb/physical.html

UK Government. (n.d.). Centre for the Protection of National Infrastructure - CPNI. Retrieved July 29, 2019, from https://www.cpni.gov.uk/about-cpni

United States Congress. Public Law 107-56, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001 (2001). United States. Retrieved from https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

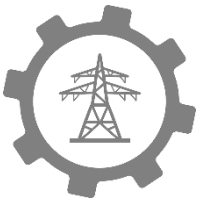
US Department of Homeland Security. (n.d.). CIKR | Homeland Security. Retrieved July 22, 2019, from https://www.dhs.gov/blog/2009/11/19/cikr

US Government. (2013). Federal Register: Improving Critical Infrastructure Cybersecurity. Retrieved July 26, 2019, from https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

US Government. (2013). Presidential Policy Directive -- Critical Infrastructure Security and Resilience | whitehouse.gov. Retrieved July 26, 2019, from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

US Government. (2013). National Infrastructure Protection Plan. Retrieved July 26, 2019, from https://www.dhs.gov/cisa/national-infrastructure-protection-plan

US Government. (2003). Homeland Security Presidential Directive 7 (HSPD-7). Retrieved from https://www.dhs.gov/homeland-security-presidential-directive-7



Chapter 2
Risk and Risk Management

He that will not sail till all dangers are over
must never put to sea.

– *Thomas Fuller, 1608-1661*
Chaplain in Extraordinary to Charles II

Welcome to the chapter on the topic of risk and risk management. Since this book is focused on performing risk assessments of critical infrastructure and industrial facilities, the facility executive and risk assessor need to understand the fundamentals of risk, risk management, and risk assessment. We will be reviewing the concepts of what constitutes risk and how you can manage it in the subsequent sections.

Of note, the topic of risk is not a trivial pursuit. My first introduction to the true depth of the topic was when I read ***Against the Gods – A Remarkable Story of Risk*** by Peter L. Bernstein. Bernstein's book offers a history of risk from the Greeks to Lloyds of London to the end of the 20th Century. This chapter will not go into the same level of Bernstein's book; however, if you want to learn more about this fascinating topic, I'd suggest you read Bernstein's book for starters.

This chapter will help you to:

- Understand what risk is.
- Define the risk equation.
- Explain threats and their categories.
- Explore some nuances of risk.

2.1 What is Risk?

There are multiple definitions for the term "Risk." Here are a few:

- Risk (noun) – A situation involving exposure to danger. (Oxford) [42]
- Risk (verb) – Expose (someone or something valued) to danger, harm, or loss. (Oxford) [43]
- Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. (NIST SP800-30)
- Risk is the expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence. (ISA-62443-1-1)

The last two definitions can be expressed as an equation – something you will find most useful when you perform your risk analyses. The equation is best described in the figure below and should be committed to memory:

Figure 2.1. Classic Risk Equation

As you can observe, the three components of risk – again worthy of memorization – are:

- Threat

[42] https://www.lexico.com/en/definition/risk
[43] ibid

- Vulnerability
- Consequences or Impact

To ensure understanding of each of these elements some added detail is provided in the following text.

2.1.1 Threat

A threat is defined in the National Institute of Standards and Technology (NIST) Special Publication 800-30, ***Guide for Conducting Risk Assessments***, as:

> *Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. (800-30, B-13)*

Threats can be from a variety of sources. The classic threat vectors to consider for a risk assessment include (but are not limited to) the following categories:

Table 2.1. Types of Threat Sources[44]

Type of Threat Source	Description	Characteristics
Man-Made	Individuals, groups, organizations, or states seeking to exploit or disrupt the organization's or facility's dependence upon resources such as other critical infrastructure and supply chains	Capability, intent, targeting Includes terrorism, rioting, product tampering, explosions and bombing, theft, financial crimes, economic espionage, vandalism, etc.
Accidental	Errors committed by individuals in the course of performing their everyday activities and responsibilities	Failure to follow instructions or procedures, failure to pay attention or being distracted, etc. Also, this can include errors or accidents due to erroneous actions performed such as failure to stay in your lane while driving or forgetting to include key elements in cyber code.

[44] This table was developed by using a variety of sources including NIST SP800-30, Page D-2; and Johnathan Tal's article on critical infrastructure threats.

Type of Threat Source	Description	Characteristics
Structural	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances exceeding expected operating parameters	This can include infrastructure and hazardous material failures and accidents, power-grid failures, water-treatment facilities failures, water-mains ruptures, safety-systems failures, bride collapse, etc.
Natural	Natural disasters and failures of critical infrastructure outside the control of the human.	Examples include: earthquakes, tsunamis, land shifting, volcanic eruptions, extreme weather (hurricanes, floods, draught), fires, etc.

Regarding the human threat, first, recognize that the threat can be intentional or unintentional. Secondly, for an intentional threat, the human normally possesses three attributes affecting their success in the attack. These attributes or characteristics are:

- Capacity
- Opportunity
- Intent

When these three characteristics are satisfied, the attack will probably succeed. Therefore, these characteristics and attributes should be part of your mindset when you are looking for threats to the facility or critical infrastructure.

WHAT THREATS ARE UNIQUE TO YOUR FACILITY OR TYPE OF INFRASTRUCTURE?

For instance, if your facility is located next to the ocean you need to worry about extreme high tides, Tsunamis, and ocean rise due to Climate Change.

If your facility is located next to an airport, you need to worry about aircraft crashing on to your facility.

Threats are dictated by many factors. You need to "think out of the box."

When preparing for a risk assessment and you want a complete inventory of threat agents and threat events, I often refer to the very comprehensive lists offered in the Canadian government ***Threat and Risk Assessment Working Guide***. Snapshots of these lists are included below and may be helpful checklists during risk assessments.

Table 2.2. Sample List of Threat Events

Categories of Threat Events	Examples of Sub-Elements
Accidents & Errors	• Power Outage • Water Failure • Omissions • Incomplete Work
Criminal Acts	• Breaking and Entering • Blackmail • Verbal/Physical Assault • Misuse/Abuse of Equipment • Hostile Staff Termination • Impersonation • Tampering • Violation of Privacy
Espionage	• Foreign spying • Commercial/Industrial • News Media • Hacking
Fraud	• Embezzlement • Forgery • Theft of Data or Equipment • Theft of Services • Manipulation of Data

Categories of Threat Events	Examples of Sub-Elements
Interception	• Criminal Activity • Foreign Intelligence • Commercial/Industrial Espionage
Natural Hazards	• Weather • Disease • Earthquakes/Landslides
Sabotage	• Commercial/Industrial Espionage • Foreign Espionage • Criminal Activity • Labor Unrest • Hostile Staff Termination • External Activists (e.g., eco-terrorists)
Subversion	• Misuse/Abuse of Equipment • Impersonation • Tampering
Terrorism	• Foreign • Domestic

Table 2.3. Sample List of Threat Agents

Categories	Elements

Non-Human	• Random
	  o Nature – Acts of God
	  o Information Technology Malfunctions
	• Physical Environment
	  o Electrical
	  o Spontaneous Combustion
	  o Water (e.g., sprinklers, damaged plumbing, condensation, etc.)
	  o Air
	  o Malicious Code
	  o Explosive Devices Arson
	  o False Alarms
	  o Material Fatigue

Human	• Insider
	  o Management
	  o Technical Staff
	  o Users
	  o Security
	  o Courier Services
	  o Business Professionals (e.g., lawyers, accountants, auditors)
	  o Environmental Controls Personnel (e.g., electricians,

Categories	Elements
	plumbers, HVAC[45] technicians, etc.) o Building Maintenance • External/Outsider o Third-party Contractors o News Media o Terrorists o Criminal Elements and Organizations o Computer Hackers o Corporate Raiders/Espionage o Foreign Government Agents

2.1.2 Vulnerability

The next element of the risk equation is vulnerability. A vulnerability can be defined as:

> *Any weakness in a component or system that can be exploited by a threat source.*

One nuance of vulnerability identification is the concept of "a predisposing condition." A predisposing condition is:

> *A condition that exists which affects by either increasing or decreasing the likelihood that threat events, once initiated, result in adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation. (NIST SP 800-30, Page 10)*

An example of a predisposing condition is the location of a facility in an earthquake, tornado, or hurricane-prone area. Another predisposing

[45] HVAC: Heating, ventilation, and air conditioning

condition is the use of outdated technologies that cannot be upgraded or patched (e.g., Windows 2000 operating system), etc.

2.1.3 Probability

In the threat equation the product of Threat times Vulnerability is the probability or likelihood of an event occurring. Thus, the greater the threat, the higher the risk. Also, the more vulnerable the system or component, the higher the risk.

This concept does not always need to be a statistical number or percentage – especially for qualitative risk assessments – which we will discuss in the next chapter.

2.1.4 Consequences or Impact

The final element of the risk equation is consequences or impact. Consequence or impact is related to the magnitude of harm expected to result from the consequences of a particular event.

Examples[46] of adverse impacts include:

- Harm to Operations
- Harm to Assets
- Harm to Individuals
- Harm to Other Organizations
- Harm to the Nation

When evaluating risk, a question usually arises regarding whether an event is High Impact, Medium Impact, or Low Impact. You need boundaries to identify the differences which can appear to be quite arbitrary at times. To guide your risk review in this impact identification, the following table has been very useful for my field work and report preparation:

[46] A detailed table on Examples of Adverse Impacts can be viewed in NIST SP 800-30, Table H-2, Page H-2.

Table 2.4. Guidelines for Risk Impact Levels[47]

Impact Category	Low-Impact	Medium-Impact	High-Impact
Injury	Cuts, bruises requiring first aid	Hospitalization is required	Loss of life or limb
Financial Loss	$1,000	$100,000	Millions
Environmental Release	Temporary damage	Lasting damage	Permanent damage, off-site damage
Interruption of Production	Minutes	Days	Weeks
Public Image	Temporary damage	Lasting damage	Permanent damage

2.1.5 Nuances of Risk

The concept of risk is rather fickle. No matter how hard you try, risk cannot be abolished or eliminated. It is persistent and constantly surrounding the individual, the organization, and the facilities. Because of this, you need to recognize that risk is a perpetual issue you should be aware of and manage.

Is risk a bad thing? Not really unless it becomes a phobia and excessively affects your psychology. But that is a subject for many other books on the subject of anxiety and dread!

Frankly, being aware of risk elements is useful for not only the risk assessor but also for the plant executive and individual employee. Being careful to avoid threats, minimize vulnerabilities, and mitigate consequences is a useful good practice you can apply to your life and your work.

[47] This table is based on Table 6-1, Possible Definitions for ICS Impact Levels Based on ISA99, in NIST SP 800-82 Revision 2, Page 6-3.

Black Swan Event

Another nuance of the risk domain is the concept of a "Black Swan Event." A Black Swan Event is defined as an extreme event that can have the following three characteristics:

a) The probability is low, based on past knowledge and experience.

b) Although the probability is low, when it happens it has a devastating impact.

c) It is impossible to predict the exact nature of the event, but they are retrospectively defined as an event of obvious concern and should or could have been better understood – to some degree – forecast as a potential risk.

Black Swans could be compounded by the simultaneous occurrence of risk events – for example, a tsunami or major hurricane followed by an earthquake.

Because risk is rather capricious, there is always uncertainty present. For instance, you know you can identify most of the threats, vulnerabilities, and consequences; however, can you be 100 percent certain you have identified them all? Not really. Thus, there is uncertainty to contend with. The conclusion here is that uncertainty is another variable the risk assessor should be aware of and consider; however, it is one more element and should not be preventing the risk assessment from being performed. Just recognize that even with the final report not *all* risks are identified, but the assessment team should identify as many reasonable risks to the facility and critical infrastructure and include them in the report.

Another nuance of risk is the contribution of cultural and technical factors. Cultural risk factors correspond to how people and processes interpret risk elements. Cultural risk factors are considered the most important element when developing an effective risk and security program. Essentially, the

cultural risk factors are there because people and their attitudes and reactions towards risk are variable. Hence, one person may believe there are nefarious hackers in the world trying to attack their systems and react accordingly; however, another person may not have any belief they are subject to attack or hacking – for whatever reason.

I witnessed one cultural risk perspective I found fascinating and horrifying at the same time. When I have travelled in Asia and Africa, I've often seen industrial safety practices that are worrisome. For instance bamboo scaffolding is quite common. I saw a bamboo scaffold alongside a 10-story building in Taipei. The scaffold swayed with each worker movement. I'm surprised no one or no tools fell off onto the street below while I was watching. But, this is the cultural norm in that society.

Oh, yes, another cultural factor is the worker who does not follow policies and procedures. Sometimes they are simply lazy or do not believe it is necessary to adhere to the steps in the manual. Also, some people do not pay attention to the procedural requirements because cultural norms do not reward such behavior. These are some of the cultural aspects of risk a risk evaluator must consider.

Technical factors are the largest contributor to risk for complex automated control systems not consistently operated by people. The reasons for this are multifold. Here are some reasons:

- For instance, early technical systems – such as early computer operating systems and industrial control systems – were not built with cybersecurity in mind. Therefore, as the systems age and the attackers become more sophisticated, the risk of failure and/or successful attack increases. This is caused by the technology and not by human error, per se.
- Interconnection between IT and control systems is increasing. This improves the efficiency and effectiveness of these systems; however, this is one more attack vector that was not taken into account when industrial control systems were developed. Such interconnections include remote access capabilities.
- Many older technical systems are still in place. They were installed but are not replaced or updated due to cost or because they are doing the job and there is no compelling need to be replaced. This is good economic news; however, the risks of failure of the system are increased due to age-related failures let alone cyber-attacks.

It is important for the risk assessor to consider both the technical and cultural causes of risk as they are evaluating the critical infrastructure, complex system, or components.

2.1.6 Risk Appetite and Tolerance

A term of art in the risk assessment and management domain is focused on how risk tolerant the institution's executive management and board of directors are. You may hear conversations revolve around whether or not executive management has an "appetite for certain levels of risk." These are not quantitative elements but are important discussions the institution's leadership should undergo. It is important to remember that risk is always present; however, there are levels of risk that should not be accepted and some levels that are allowed.

An excellent perspective on risk appetite and tolerance is from the Institute of Risk Management. Their perspective is that both risk appetite and risk tolerance are inextricably linked to performance over time. While risk appetite is about the pursuit of risk, risk tolerance is about what you can allow the organization to deal with. (IRM 2011, Page 8)

HAVE YOU CONSIDERED WHAT YOUR COMPANY'S RISK APPETITE IS? IS IT EVEN DEFINED IN THE RISK COMMITTEE OF YOUR BOARD OR BY YOUR CEO AND EXECUTIVE LEADERSHIP TEAM?

Since risks and risk opportunities consistently vary some organizations will have a process for risk reviews and approvals. For example, consider a risky operation at a plant that is not normally performed. A risk management technique includes performance of in-depth risk analysis of the planned event followed by written approval of the risks and proposed mitigation activities by management. This would take into account the executive and board-level risk appetite and tolerance in a formal manner. Also, it moves the risk decision from the field worker and supervisor to the officer-level of the company.

My friend and security colleague, Kip Boyle, noted in an email to me that a common error in risk management is allowing one's own personal risk appetite and tolerance to be unknowingly substituted for those of the organization when making decisions. Frankly, it is best for the organization

to ensure a policy on corporate risk appetite is promulgated and followed. Also, the policy should identify who can make corporate risk decisions. For instance, one policy I saw said that only Vice Presidents and senior (i.e., corporate officers) are permitted to make corporate-level risk decisions.

Risk reviews involve a variety of techniques published in many books and guidelines. These reviews can include:

- Auditing and Inspection
- BPEST Analysis (Business, Political, Economic, Social, Technological)
- Brainstorming
- Event Tree Analysis
- Failure Mode and Effect Analysis (FMEA)
- Fault Tree Analysis
- HAZOP (Hazard and Operability Studies)
- Incident Investigations
- Industry Benchmarking
- Questionnaires
- Risk Assessments
- Risk Assessment Workshops
- Scenario Analyses
- Studies
- SWOT Analysis (Strengths, Weaknesses, Opportunities, Threats)

Except for risk assessments, detailing how these analyses are performed is outside the scope of this book; however, they are excellent preparatory resources before performing the risk assessment. Before you arrive on site, ask the company to provide any or all of the above analyses to identify some of the risk concerns and findings you will be observing. This is time well spent.

2.1.7 Risk Velocity

In the risk domain, another concept to consider is that of "risk velocity." Risk velocity is an indication of how soon or how fast the effects of risk will be experienced. From the Qatar Aviation Cyber Security Guidelines is an excellent table summarizing this idea:

Table 2.5. Risk Velocity

Velocity Measure	High	Medium	Low
Time to Impact	Risk impact will be felt in less than a week after occurrence	Risk impact will be felt between a week to a month after occurrence	Risk impact will be felt more than one month after occurrence
Reaction Time	There will be very little or no time for reaction and response planning before serious consequences of the risk hits	There will be limited time for reaction and response planning before serious consequences of the risk hit	There will be time for reaction and response planning before the serious consequences of the risk hit

2.2 Risk Management

The previous section covered the concept of risk and key supporting elements. This new section overviews the concept of Risk Management. Let's start with some definitions.

Risk management can be defined as:

> *Risk management involves understanding, analyzing, and addressing risk to make sure organizations achieve their objectives. It must be proportionate to the complexity and type of organization involved.* (Institute of Risk Management), or

> *The process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment* (ISA-TR62443-1-2, Page 29)
>
> *A strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio. (ASIS, page 6)*

2.2.1 Risk Management Principles

According to the International Organization for Standardization (ISO) 3100, ***Risk Management – Guidelines on principles and implementation of risk management***, the following are principles of risk management:

- Create value – resources spent to mitigate the risk should cost less than the consequences of taking no action
- Be an integral part of the organizational process
- Be part of the decision-making processes
- Explicitly address uncertainty and assumptions
- Be a systematic and structured process
- Be based on the best available information at the time
- Be customizable
- Take human factors into account
- Be transparent and inclusive – integrated with overall project management planning
- Be dynamic, iterative, and responsive to change
- Be capable of continued improvement and enhancement
- Be continually or periodically re-assessed.

In addition to the above principles, risk management must be holistic. It must have a global perspective and views the activities in question within the larger system of systems. Additionally, risk management activities

should not be exclusively focused on the past but should be forward-looking and consider potential outcomes.

Risk management involves planning, followed by organizing, directing, and controlling resources to ensure risk remains within acceptable bounds. It is expensive to safeguard critical infrastructure and key assets from all threats; the risk management process allows for a process to identify and manage obvious risks and then identify mitigating action to reduce or even eliminate the risk.

US Coast Guard STAAR Model

The US Coast Guard uses a memory aid for strategies to control or mitigate risk. They use the initials STAAR to stand for:

S – Spread Out
T – Transfer
A – Avoid
A – Accept
R – Reduce

Ref: USCG General Assessment of Risk Tool (GAR 2.0)

2.2.2 Addressing Risk

Part of the risk management process includes answers to the question, "What do I do when I identify a risk?" The five actions you can take include:

- Accepting the risk.
- Avoiding the risk.
- Reducing or Mitigating the risk.
- Transferring the risk – buy insurance.
- Spreading the risk – joining a risk management pool.

The last element – spreading the risk – is relatively new to this list of risk management actions. But, with the advent of risk management pools[48] formed by insurance companies, spreading risk within a group of asset owners – such as water utilities – helps spread the risk.

By the way, some people will argue you can also "ignore the risk." Unfortunately, this is not an acceptable perspective and should never be considered.

To add to this argument why one should not "ignore the risk" is the perspective of ensuring "due care" and its execution – a/k/a "due diligence." Essentially, if an organization is not taking due care to ensure its operations are safe and secure it could be found negligent in the event of an accident or injury or death. Due care should be a fundamental reasoning for all executive decisions.

2.2.3 Risk Management Process

Risk management is a program and process with the intent to manage risk to organizational operations including mission, functions, image, reputation, organizational assets, and individuals. Risk management has an associated process.

Essentially risk management is intended to answer four primary questions: (Cribbs)

- What can be done about identified risks?
- What options are available?
- What are the associated tradeoffs of the options?
- What are the impacts of current management decisions on future options?

[48] In a risk pool, insurance companies come together to form a risk pool, which can provide protection to insurance companies against catastrophic risks such as floods or earthquakes. One definition of risk pooling could be "a group formed by insurance companies to provide catastrophic coverage by sharing costs and potential exposure." Risk pools help insurance companies offer coverage to both high- and low-risk customers. They also lessen the risk borne by any single insurance company by spreading it among many. (Bizfluent)

The industry standard risk management process flow chart is in ISO 31000 and is presented below:

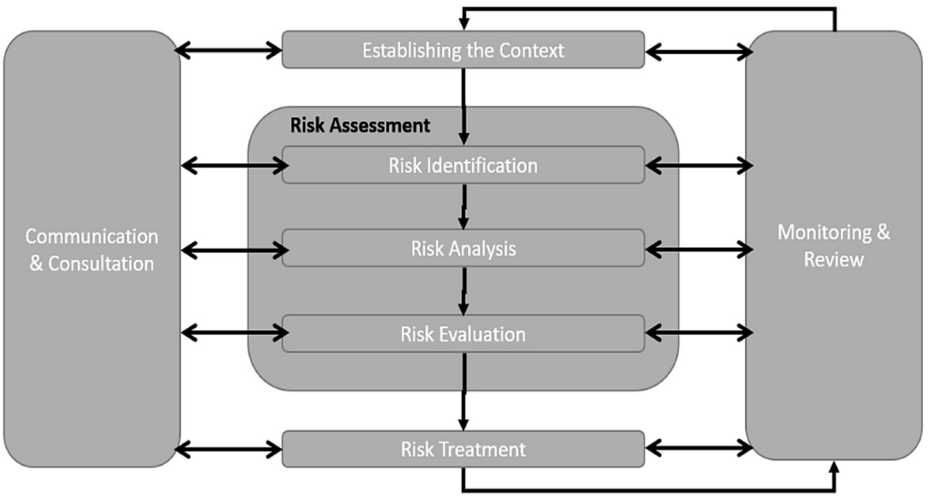


Figure 2.2. Risk Management Process Diagram Per ISO 31000

The risk management process shown above revolves around the Risk Assessment processes which we will discuss later in this book.

The first element in this process stack is Establishing the Context. This means that the risk management process should be consistent with the enterprise's structure, processes, and culture. The context should be predicated on both internal and external constraints or parameters relevant to the organization. Also, the context provides a basis for risk evaluation.

The external context is anything outside the organization influencing organizational objectives. This can include: (ISO 31000-2007, page 9)

- Cultural, political, legal, regulatory, financial, economic, and competitive environment whether local, regional, national, or international.
- Drivers and trends impacting the objectives of the organization
- Perceptions and values of external stakeholders[49]

[49] The external stakeholders can include the shareholders, the media, the public at large. These entities have an interest in the organization. The shareholders are worried about

The internal context are those things within the organization influencing the way the organization manages risks. For instance, the risk appetite of the board of directors and executive leadership is an internal context. The internal context is influenced by such key drivers as:

- Decision-making processes
- Governance processes and structures
- Information and communication flows and processes
- Internal perceptions, values, culture, and norms
- Organizational capabilities relative to capital, people, capabilities, expertise, processes, systems, and technologies
- Organizational structure – formal and informal
- Policies, standards, procedures, and guidelines

Besides the internal and external drivers affecting the risk management process, you need to structure the processes and procedures accordingly. Per ISO 31000 the risk management process should address the following:

- Define responsibilities
- Define the depth and breadth of risk management activities to be performed to include specific exclusions and inclusions
- Define the extent of the project, process, function, activity and its associated goals and objectives
- Define the relationships between a particular activity and other projects and activities of the enterprise
- Define the risk assessment methodologies and practices
- Define the way risk management performance is evaluated
- Identify and specify the necessary decisions to be made
- Identify necessary scope and framing studies to be performed including their extent, objectives, and necessary resources

---

financial performance and the media and public are monitoring the company to ensure it is a good citizen and not negatively impacting their lives or health.

2.2.4 Risk Management Focus – Component or System

One perspective on risk management is relative to the focus one can take. You can focus on components – which is a quite common approach – or you can focus on systems. The component-driven risk management approach focuses on technical components and the risks they face. Alternatively, the system-driven risk management analyses systems and their risk.

Component-driven risk management looks at individual components within systems. This approach mandates you determine the function you are analyzing then look at the components included within the associated system. Essentially you develop an asset list or asset register to use for your risk management and subsequent risk assessment.

What about those components where you have no control, but your system relies upon them? They are called "dependencies." You should include these dependencies as part of your asset register to demonstrate how the outside systems affect your internal system being reviewed. For example, you may be looking at the compressed air system of a factory or power plant. You first identify the components – compressors, receivers, filters, valves, etc. – but also realize that electric power is a "dependency" for the compressed air system. Hence, you have your asset list and list of dependencies for the risk assessment and subsequent risk management approach.

For information technology component-driven risk management a primary framework to rely upon is from the US National Institute of Standards and Technology (NIST) Special Publication 800-30, ***Security and Privacy Controls for Federal Information Systems and Organizations***.[50]

The system-driven risk analysis is more complex and not as intuitive as the component-driven risk management approach. The UK National Cyber Security Centre (NCSC) has a helpful description of system-driven risk management.[51] They observe that the systems-driven approach is resource intensive and time-consuming.

The system-driven risk management approach tries to look at the system as a whole and identify system-level risks and dependencies. Such an approach may be appropriate for reviews of critical infrastructure and key resources;

---

[50] https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

[51] https://www.ncsc.gov.uk/collection/risk-management-collection/component-system-driven-approaches/understanding-system-driven-risk-management

however, it gets very complex very fast. I have personally not performed a system-driven risk assessment and normally – and comfortably – use the component-driven risk approach because it is simple and allows for more targeted risk mitigation. Also, the findings are more intuitive and easier to correct.

Should you want to learn more about system-driven risk management consider spending time to review the Systems-Theoretic Accident Model and Process (STAMP), The Open Group Architectural Framework (TOGAF)[52], and SABSA[53].

A summary comparison of component-driven risk versus system-driven risk methods is in the table below:

[52] https://www.opengroup.org/togaf
[53] https://sabsa.org/sabsa-executive-summary/

Table 2.6. Component vs System Driven Analyses (UK NCSC, 2019)

Type	Useful For:
Component-driven	• Analyzing the risks faced by individual technical components • Deconstructing less complex systems and identifying connections between component parts • Working at levels of abstraction where a system's physical function is understood and agreed upon
System-driven	• Exploring risk issues and security failures which surface out of the complex interaction of many parts of the system • Establishing system security requirements before you have decided upon the system's exact physical design • Bringing together multiple stakeholder's views of what a system should and should not do (e.g., safety, security, legal views, etc.) • Analyzing security breaches which cannot be tracked back to a single point of failure.

2.2.5 Risk Management Focus – Defensive and Offensive

In his article on defensive risk management, Brian Schwartz observes that defensive risk management is an approach where you establish a proactive risk program. The defensive risk program includes the following elements:

- Setting up a risk appetite statement and framework approved by the board of directors and executive suite
- Aggregating the risks across the enterprise and map them against the risk appetite along with risk tolerances and limits
- Developing a set of key risk indicators (KRIs)
- Establishing a solid business continuity/disaster recovery strategy to quickly return the business to normal following a risk event

Schwartz also continues with his view on offensive risk management. Here you leverage your risk program as part of your corporate strategy and growth planning. In this offensive risk program, you first align your risk management process with strategic planning so you can drive those priorities forward in light of all the risks faced by the company. Additionally, another offensive tactic involves giving some of the risk management activities back to the individual business units so they can run faster and drive risk-adjusted decisions and revenue plans. (Schwartz, 2016)

2.2.6 Risk Management Focus – Checklist Approach

Conducting risk management actions simply for compliance purposes can lead to risk being managed in a "tick-box" fashion with unintended negative consequences. Sadly, such an approach prevents organizations from looking broadly across the enterprise for all risks and instead there is more concern whether the right boxes have been checked – not how well the risks are being managed. Similarly, the compliance-focused team can have an unrealistic view of what the rest of the organization is doing regarding risk management thus leading to incorrect decisions. (NCIS, 2019)

There is an adage that I personally have believed in in this regard. Basically, compliance does not equal risk management and risk management does not equal compliance. You can satisfy all the check boxes, but you may be missing a key vulnerability or threat. Hence, you need a balanced risk management program that does take into account the compliance requirements of the frameworks you are following, and you do ask the question, "What can go wrong."

Compliance ≠ Risk Management

Figure 2.3. Compliance Does Not Equal Risk Management

2.2.7 Risk Management – Convenience vs Liability or Risk

Years ago, my friend and security mentor, Mr. Kirk Bailey[54], developed a convenience vs risk model – literally on a napkin at our favorite breakfast hang out. The premise of our model is that risk is predicated on whether a process/system/asset is conveniently available or restricted from general use. Yes, this is fairly obvious, but we've not seen a similar model in risk literature.

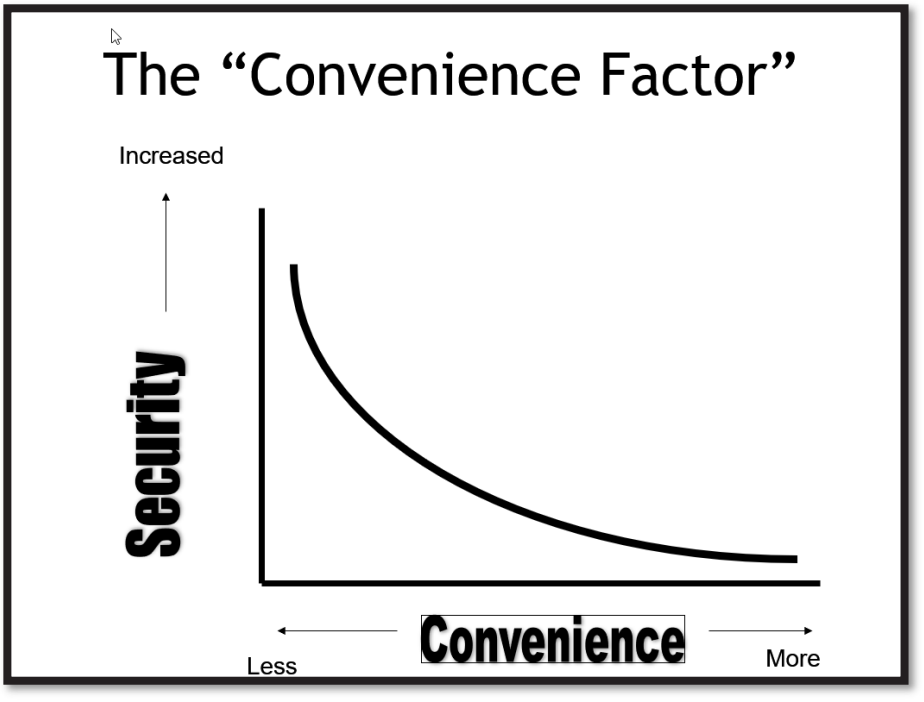


Figure 2.4. Convenience vs Security

[54] Kirk Bailey retired recently as the Chief Information Security Officer at the University of Washington in Seattle, Washington USA

In the figure above, consider how convenience affects security or associated risk. For instance, if you leave your keys in the car so you always know where they are, it is very convenient but there is essentially no security for the vehicle and the risk of it being stolen is very high. Alternatively, consider a high-security military facility. With multiple layers of physical and cyber security it is very inconvenient to the individual (or hacker) and the risk of penetration and damage or theft is greatly reduced.

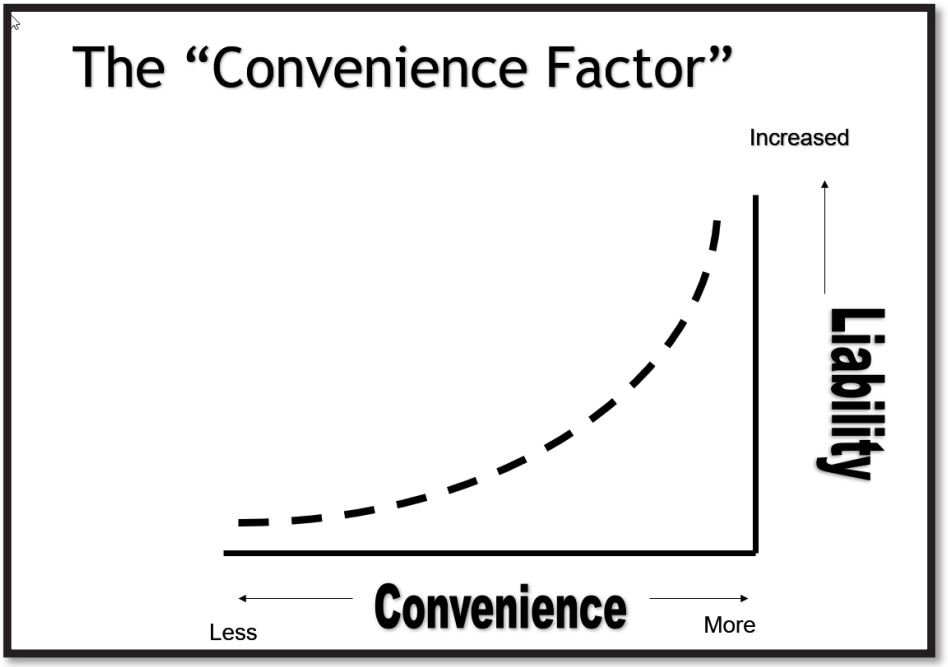


Figure 2.5. Convenience vs Liability

Now, let's look at how the level of convenience impacts the risk of liability to the enterprise or individual. Again, when leaving your keys in the car, yes, it is convenient; however, your liability for being sued or arrested due to a thief stealing the car and killing a pedestrian is very high (i.e., you did not practice very good due care or due diligence). Your personal risk is extremely high. So, when looking at the high-security military facility again, the government's liability is quite low because they have spent the resources to protect the facility and its assets.

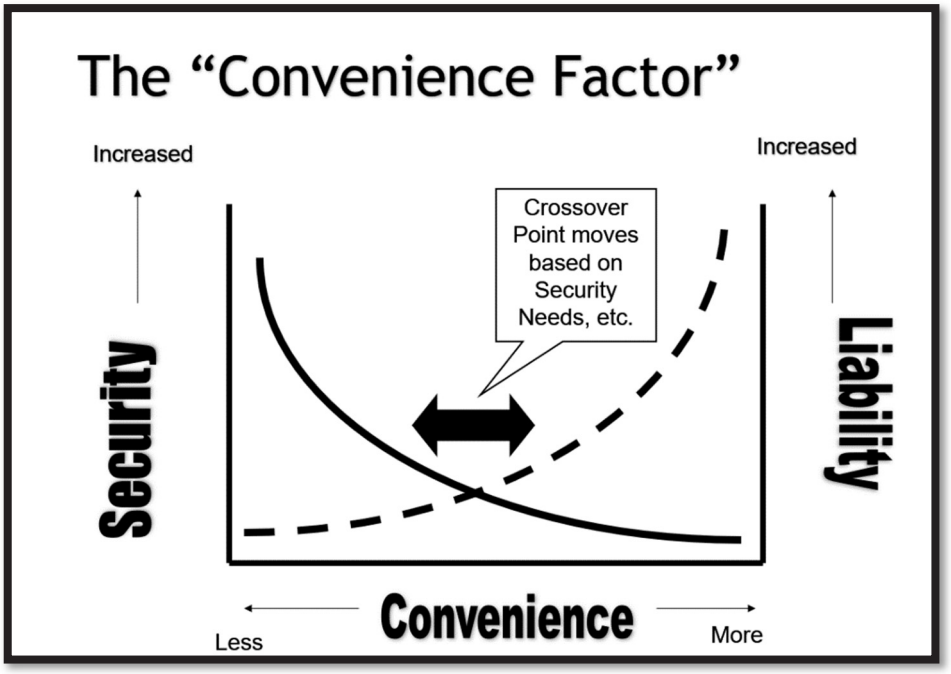


Figure 2.6. Security, Liability, and Convenience

Overlaying these curves allows for some qualitative analysis of the risk. At the crossover point you can get a sense of how increasing or reducing your security affects your risk of liability.

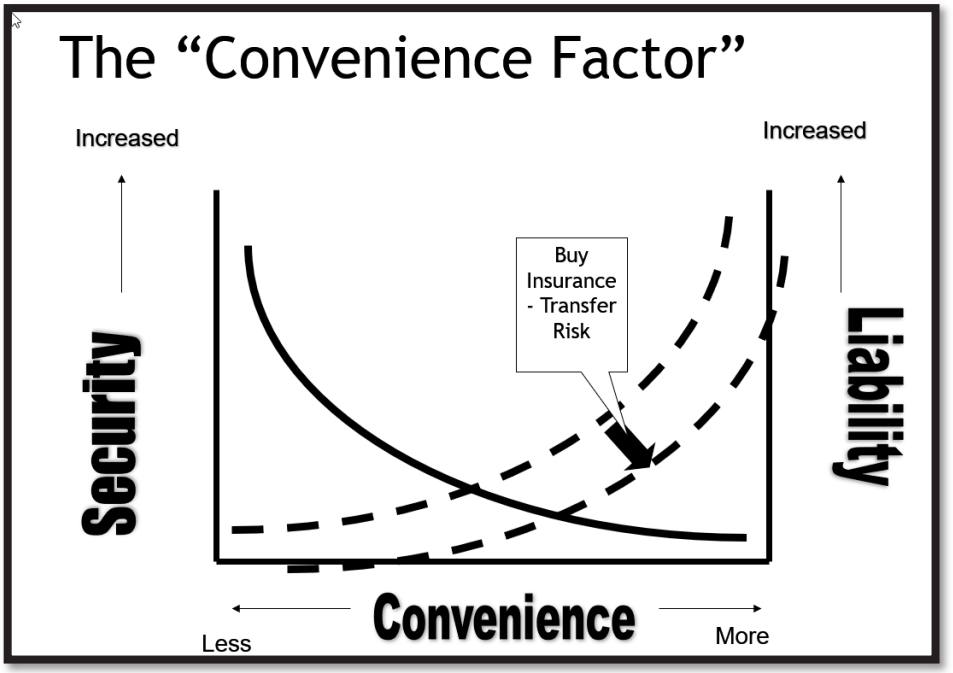


Figure 2.7. Risk Transfer and the Convenience Factor

Finally, in the graphic above, we can use this model to help us better understand how we handle our risk. For instance, by buying insurance – i.e., transferring the risk – you shift the curve thus allowing you to make access to the asset a bit more convenient – within reason.

Like most models, this one is not perfect; however, it can help when analyzing the risk to the enterprise and its current practices regarding access control, perimeter protection, etc.

2.2.8 Risk Management – Summary Guidance

The UK National Cyber Security Centre offers an excellent summary of risk management principles[55]. I've included a modified list here to summarize risk management ideas to include before moving to the core of this book, Risk Assessments:

[55] https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics/get-basics-right-risk-management-principles-cyber-security

- Start with a security baseline.
- All organizations face risks, no matter the size.
- Understand what you care about and ***why.***
- Think about situations in which you could have a component or system failure.
- Accept ***some*** risk.
- Balance risks against other types of risks – some security measures can reduce one type of risk but increase risk somewhere else.
- Learn from risk management solutions used by other organizations.
- Keep an eye out for risk management myths.
- Be aware of the strengths and weaknesses of risk management techniques.
- Ensure you have some variety in risk information.
- Always ask: What can go wrong?

2.3 The Next Chapter – Risk Assessment

Because the core concept of this book is risk assessment, the next chapter will be devoted entirely to risk assessment fundamentals. However, the concepts we've discussed above regarding risk and risk management are important and help the risk assessor better understand how to "look" for risks and review risk management programs.

2.4 Questions for Further Thought and Discussion

1. Why should we worry about risk? Risk is constantly with us and we can't eliminate it?
2. Describe the risk equation and its components. Of the equation, which element do you think is the most difficult to identify? Why?
3. What are the five ways of addressing risk? What practice do you see being used the most at your institution or company?

4. What are the most common threat sources as we become more technologically centered with artificial intelligence, internet of things, reliance on our smart phones?
5. Describe risk appetite. Does your management team understand such a concept?

REFERENCES

Anderson, R., Aujla, B., Clatworthy, G., Garrini, R., Hopkin, P., Shackleford, S., … Williams, C. (2011). *Risk Appetite & Tolerance Guidance Paper*. London. Retrieved from https://www.theirm.org/media/7239/64355_riskapp_a4_web.pdf

ASIS International. (2015). *Risk Assessment*. Alexandria, VA: ASIS International. Retrieved from https://www.asisonline.org/publications/sg-risk-assessment-standard/

Bernstein, P. L. (1996). *Against the Gods - The Remarkable Story of Risk*. New York: Wiley.

Commandant United States Coast Guard. (2018). *Risk Management (RM)*. Washington, DC.

Cribbs, D. (2018). Security Principles and Practices Presentation. Houston.

Endicott-Popovsky, B. (n.d.). *Information Security Risk Assessment and Management (Lecture Notes)*. Seattle, Washington.

Government of Canada Communications Security Establishment. (1999). *Threat and Risk Assessment Working Guide*. Ottawa. Retrieved from http://www.iwar.org.uk/comsec/resources/risks/ITSG4e.htm

Institute of Risk Management. (2002). *A Risk Management Standard*. London. Retrieved from https://www.theirm.org/media/4709/arms_2002_irm.pdf

International Organization for Standardization. (2007). Committee Draft of ISO 31000 Risk Management. Retrieved August 23, 2019, from https://web.archive.org/web/20090325160441/http://www.nsai.ie/uploads/file/N047_Committee_Draft_of_ISO_31000.pdf

ISA Working Group 3. (2013). *Security for industrial automation and control systems - Master Glossary (TR62443-1-2)*.

Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments*. Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-30r1

Leveson, N. (2004). A New Accident Model for Engineering Safer Systems. *Safety Science*, *42*(4), 237–270. Retrieved from https://www.sciencedirect.com/science/article/pii/S092575350300047X?via%3Dihub

Lexico - Powered by Oxford. (n.d.). risk | Definition of risk in English by Lexico Dictionaries. Retrieved August 15, 2019, from https://www.lexico.com/en/definition/risk

National Cyber Security Centre. (2019). Risk Management Guidance. Retrieved August 26, 2019, from https://www.ncsc.gov.uk/collection/risk-management-collection

Qatar Civil Aviation Authority, & Communications, Q. M. of T. &. (2019). *Aviation Cyber Security Guidelines*. Retrieved from https://www.caa.gov.qa/en-us/PrintedPublications/Pages/Aviation-Cyber-Security-Guidelines.aspx

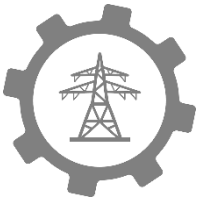
Sisk, A. (2018). What Is Risk Pooling in Insurance? | Bizfluent. Retrieved August 23, 2019, from https://bizfluent.com/about-6521384-risk-pooling-insurance-.html

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security*. Gaithersburg, MD USA. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Tal, J. (2018). America's Critical Infrastructure: Threats, Vulnerabilities and Solutions. Retrieved August 16, 2019, from https://www.securityinfowatch.com/access-identity/access-control/article/12427447/americas-critical-infrastructure-threats-vulnerabilities-and-solutions

US Department of Homeland Security. (n.d.). 210W-05 Cybersecurity for Industrial Control Systems - Cybersecurity Risk. (Password required) Retrieved August 20, 2019, from https://ics-cert-training.inl.gov/learn/course/external/view/elearning/17/210W-05CybersecurityforIndustrialControlSystems-CybersecurityRisk

US National Institute of Standards and Technology. (2006). *Minimum security requirements for federal information and information systems*. Gaithersburg, MD. https://doi.org/10.6028/NIST.FIPS.200



Chapter 3
Risk Assessment

Some of the most interesting research that I did was about risk assessment and how ordinary citizens like me handle risk assessment and how irregular our risk assessments are.[56]

– *Eula Bliss*

Welcome to the chapter on Risk Assessment! Although the remainder of the book is on practical aspects of risk assessment preparation, onsite performance, and writing the report, this chapter is intended to revolve more around theory and risk assessment models.

In this chapter you will:

- Learn the definitions of risk assessment,
- Understand different types of risk assessments, and
- View some different risk assessment models as revealed in some international and national standards.

[56] https://www.brainyquote.com/quotes/eula_biss_724462?src=t_assessment

What is the function of a risk assessment? Risk assessments attempt to identify answers to three primary questions (Cribbs, 2018):

1. What can go wrong?
2. What is the likelihood of it going wrong?
3. What is the impact of it going wrong?

Risk assessments are just an element of risk management. Risk management is more of a comprehensive process to identify what can be done about identified risks. Specifically, the risk assessment process intentionally focuses on raising awareness as to what risks exist in the enterprise.

Secondly, risk management takes advantage of the risks identified during risk assessments and guides the organization on how to handle the risks. As observed in Chapter 3, risk can be handled by a) accepting the risk, b) avoiding the risk, c) reducing or mitigating the risk, d) transferring the risk, or e) spreading the risk. Recognize, however, that is not the function of risk assessments – they are primarily intended to identify the risks for treatment by the organization's risk management team and executive leadership.

Overall, risk assessment identifies internal and external threats and vulnerabilities and offers "on site" perspective on the probability and impact of an event surfacing from such threats or vulnerabilities.

In summary, the best security methodology is one that yields the highest risk awareness at the lowest cost in time and money. Overall, the benefit is first becoming aware of the vulnerabilities faced by your systems and components. Secondly, the security assessment is of no value unless actions are taken by the enterprise leadership or plant owner/operator to mitigate and correct the vulnerabilities and risks identified. Therefore, the risk assessment is a team effort with assessment team members highlighting the vulnerabilities, identifying the level of risk (critical, high, medium, low), and offering suggestions to the enterprise leadership and risk managers on ways to mitigate the risks in order of priority from highest to lowest risk.

3.1 Definitions of Risk Assessment

The term "risk assessment" is definitely a term of art you can observe across multiple industries. Risk assessment models, methodologies and checklists can be found across such industries as:

- Auditing (e.g., assessing the risks of material misstatement)

- Environmental protection
- General project management and "megaprojects"
- Health care and public health
- Information security
- Maritime industry
- Underwater diving.

The risk assessment concept was developed in the insurance industry. (ASIS, 2012)

"A risk assessment is not about creating huge amounts of paperwork, but rather about identifying sensible measures to control risks in your work place."

"Risk Assessment," UK Health and Safety Executive

Here are some definitions of risk assessment:

> *A risk assessment is the overall and systematic process of evaluating the effects of uncertainty on achieving objectives. A risk assessment includes risk identification, risk analysis, and risk evaluation. Risk assessment helps identify threats, assets, and vulnerabilities through a systematic, defensible process.* (ASIS, 2015)
>
> *Risk assessment is the overall process of risk identification, risk analysis, risk evaluation. Note: Risk assessment involves the process of identifying internal and external threats and vulnerabilities, identifying the probability and impact of an event arising from such threats and vulnerabilities, defining critical functions necessary to continue the organization's operations, defining controls in place necessary to reduce exposure, and evaluating the costs of such controls. (ASIS, 2012)*
>
> *An evaluation of risk based on threat assessment information, the effectiveness of existing and proposed security safeguards, the likelihood of system vulnerabilities being*

> *exploited, and the consequences of the associated compromise to system assets.* (Government of Canada, 1999)
>
> *The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system.* (NIST 800-30, Page B-9)
>
> *A methodology to determine the nature and extent of risk by analyzing potential hazards and evaluating existing conditions of vulnerability that could pose a potential threat or harm to people, livelihoods, and the environment on which they depend.* (UNDRR, 2017)
>
> *Risk assessment is a formal and systematic analysis to identify or quantify frequencies or probabilities and magnitude of losses to recipients due to exposure to hazards (physical, chemical, or microbial agents) from failures involving natural events and failures of hardware, software, and human systems.* (Modarres, 2006)

The key points to consider for what a risk assessment entails are: a) risk assessment is an action; b) risk assessment is a systematic process; c) risk assessment requires identification of threats, vulnerabilities and consequences to the systems or components; and, d) it requires an evaluation of the results to identify and prioritize the risks and risk levels (critical, high, medium, low). Basically, effective and properly performed risk assessments are a lot of hard work, require focused attention-to-detail, and take time. They cannot be glossed over or done in a day.

3.2 Assessment Foundational Principles, Scope, and Applicability

Of the books I've read on the subject on risk assessment, I find NIST Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, contains the best discussion on the fundamental elements of risk assessments. The book is information technology-centric; however, the focus and key points provide an excellent foundational summary of what constitutes a risk assessment. These key principles are repeated below since they are so profound:

- Risk assessments are a key part of effective risk management and facilitate decision making at all tiers in the risk management hierarchy including the organization level, mission/business process level, and information system level.
- There are no specific requirements with regard to: a) the formality, rigor, or level of detail that characterizes any particular risk assessment; b) the methodologies, tools and techniques used to conduct such risk assessments; or c) the format and content of assessment results and any associated reporting mechanisms.
- The leadership of organizations receiving risk assessments are advised that risk assessments are often not precise instruments of measurement and reflect a) the limitations of the specific assessment methodologies, tools, and techniques employed; b) the subjectivity, quality, and trustworthiness of the data used; c) the interpretation of assessment results; and d) the skills and expertise of those individuals or groups conducting the assessments.
- Since cost, timeliness, and ease-of-use are a few of the many important factors in the application of risk assessments, organizations receiving risk assessments should attempt to reduce the level of effort for risk assessments by sharing risk-related information, whenever possible, and before the risk assessment begins.
- Risk assessments should consider the entire threat spectrum such as physical, man-made, natural, electronic, digital, etc.

3.3 Application of Risk Assessments

As observed earlier, performing risk assessments is a primary activity supporting risk management. Risk assessments – if done thoroughly and well – support risk-response decisions throughout the company. They can help aid management decisions on ways to mitigate risks through capital improvements, new facility designs, training, etc. Also, even if a risk is identified separate from any risk assessments, the risk assessment response discipline helps management best remediate threats and vulnerabilities as they surface. For instance, a formal risk assessment does not need to be performed to realize a storm will be impacting the local area; however, the risk management approaches to respond to threats and vulnerabilities may be "practiced" with risk assessment response development.

Risk assessments can be performed in a variety of environments ranging from in-the-field, hands on, plant and system walkdowns, to tabletop reviews of policies, procedures, and guidelines. Simply holding a strategic discussion at the executive risk committee on the board can sometimes be considered a risk assessment. At least there is a formal approach to identifying threats and vulnerabilities and subsequently taking action to mitigate, reduce, or eliminate same. But, having a formal risk assessment methodology – which this book attempts to demonstrate – is a useful foundational process an entity should rely upon and practice.

What risks do formal risk assessments consider? They look for threats and vulnerabilities in different domains. They can include reviews of the following:

- Digital risk
- Financial risk
- Obsolescence risk
- Operational risk
- Partnership risk
- Physical plant risk
- Regulatory and compliance risk
- Reputation risk
- Supply chain risk
- Etc.

The risk assessments and their derivative works can impact organization-wide risk management and security programs, policies, procedures, guidelines, and other controls. And, as noted above, risk assessments can guide risk management decisions on risk responses such as acceptance, avoidance, sharing, transferring, or mitigating threats and vulnerabilities.

Risk assessments have a financial impact on the enterprise. The results of risk assessments can affect investment decisions for capital equipment and consumables. The risk assessments can affect the approaches to purchasing and supply chain management including selection of contractors, vendors, and suppliers. (Of note, during the Covid19 pandemic going on as I write this book, there were multiple examples of supply chain failures that could have been avoided if pandemic risk assessments and tabletop exercises had been performed earlier.)

System and facility architecture – both physical and digital – can be impacted by risk assessments. Also, training for employees, contractors, and vendors can be affected by risk assessment results and risk mitigation activities.

Of course, risk assessments can – and should – affect business continuity/disaster recovery planning decisions for the enterprise.

3.4 Risk Assessment Techniques

There are generally four types of risk assessment "techniques." They include a) ad-hoc risk assessments, b) deductive risk assessments, c) inductive risk assessments, and d) targeted risk assessments.

3.4.1 Ad-hoc Risk Assessment

An ad-hoc risk assessment is any approach to evaluating threats and vulnerabilities employing a practical method not guaranteed to be optimal or perfect but may be sufficient to achieve the immediate risk management goals. Essentially, an ad-hoc risk assessment can be a simple, unstructured response to a demand to identify threats and vulnerabilities resulting in some educated guesses on the current risk profile. Using common sense is one of these approaches – it may identify threats and vulnerabilities but may not be complete and is definitely not in-depth. Such a technique may be incomplete and include substantial bias affecting the results.

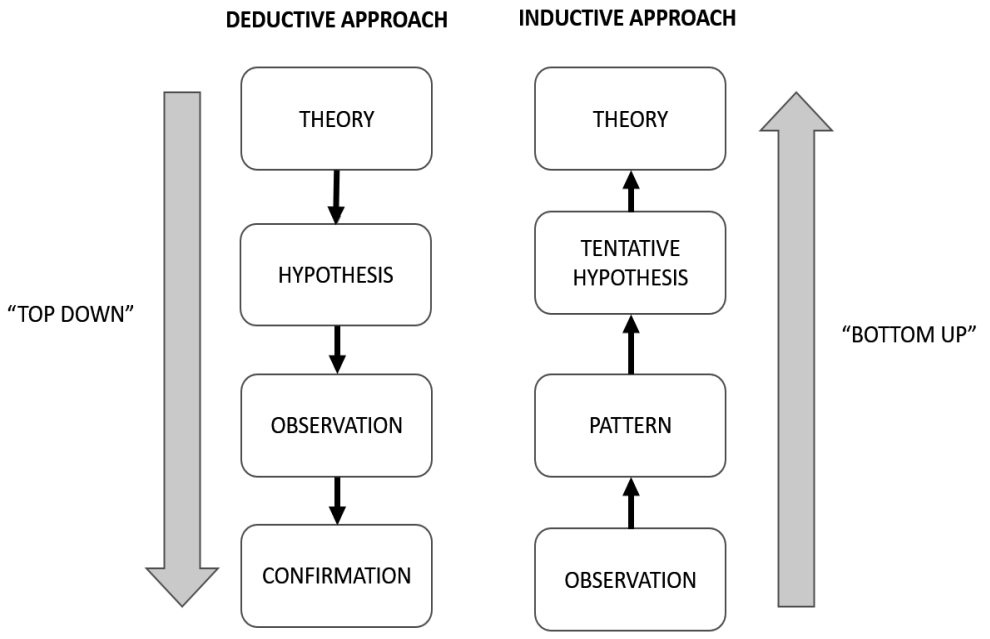


Figure 3-1 Deductive vs Inductive Assessment Approaches (Based on Burney & Saleem, 2008)

3.4.2 Deductive Risk Assessment

A deductive risk assessment would be a "top-down" methodology. Figure 3-1 demonstrates such a concept.

Here you first establish a theory based on more general perspective, then you dig down to collect more specifics. The conclusion is drawn after looking at the available facts. Arguments based on laws, rules, and accepted principles are generally used for deductive reasoning. (Burney & Saleem, 2008)

According to ASIS, *Protection of Assets: Physical Security*, a deductive risk assessment uses logic diagrams or fault trees to determine how a particular undesired event may occur.

As an experienced field risk assessor, I normally do not use the deductive approach, but instead, use the inductive methodology.

3.4.3 Inductive Risk Assessment

The inductive risk assessment is a "bottom up" approach. By using observations, you can soon identify patterns to help you identify potential root causes of the vulnerabilities and threats identified.

This is an approach I have used for many years. I find it especially useful since it allows me to perform a holistic, all-risks or all-hazards view of the facility or system being inspected, rather than being constrained by an initial theory or hypothesis. However, some would argue that this approach involves a degree of uncertainty since you still cannot see "everything."

3.4.4 Targeted Risk Assessment

Targeted risk assessments are another tool in the risk assessor's kit. According to the US National Institute of Standards and Technology (NIST), Special Publication 800-30, *Guide for Conducting Risk Assessments*, a targeted risk assessment is used when the scope of the assessment is narrowly defined to produce answers to specific questions (e.g., What is the risk associated with relying on a given technology? How should prior risk assessments be revised based on incidents that have occurred? What new risks can be identified based on knowledge about a newly discovered threat or vulnerability? etc.)

3.5 Assessment Approaches – Qualitative vs Quantitative

There are generally two types of assessment approaches. First, there is qualitative followed by quantitative which includes a "semi-quantitative" sub-methodology.

Qualitative risk assessments use a set of methods and approaches that ultimately assess risk characteristics in non-quantitative terms. You may see qualitative risk assessment results in terms of critical, high, medium, or low risk. Some would argue qualitative risk assessments are predicated on "feel," or predictions, or the experience of the assessor.

Quantitative risk assessments are based on hard numbers such as historical events, statistics, actuarial tables, etc. usually possessed by the insurance industry. Unfortunately, when assessing an industrial environment, large facility, or critical infrastructure, such data and statistics are simply not

available. This is especially the case when performing a cyber security assessment.

Of note, there are semi-quantitative risk assessment approaches. Here, a set of methods, principles, or rules for assessing risk ultimately use scales, bins, or representative numbers whose values and meanings are not maintained in other contexts. The bins (e.g., 0-15, 16-35, 36-70, 71-85, 86-100) or scales (e.g., 1-10) translate easily into qualitative terms supporting risk communications for executive management. For instance, a score of "95" is more readily understood as very high or critical risk. (NIST, 2012)

In the security industry, risk assessments typically rely on qualitative, not quantitative approaches. (Cribbs, 2018) Also, qualitative risk assessments are faster to execute and normally easier to communicate and explain to executive management and the board of directors.

From my own experience, quantitative risk assessments are simply not an option. Obtaining statistics and probabilities on large facility, system, or critical infrastructure is simply not available or would be very dated and not reflect the current state of threats and vulnerabilities.

> *"We sought out consultant help and found that we didn't always assess ourselves correctly. Once we assessed properly… we created a list of prioritized system improvements. As a result, the utility was able to reduce its attack surface and limit opportunities for hackers to do harm."*
>
> *David Paul*
> *Vice President and Director of Engineering*
> *Aqua Engineers, Hawaii*
>
> *(WaterWorld, 2018)*

3.6 Dynamic Risk Assessment

A dynamic risk assessment is primarily performed when emphasizing industrial safety or emergency response. It is the process of observing and identifying risks and hazards in the workplace that are difficult to predict

due to changing conditions. It is performed by persons in charge who can implement control measures and mitigate dynamic risks. (Anear, 2019)

The British Government appears to have developed the concept of "Dynamic Risk Assessment" to apply to firefighters responding to emergencies. In their book, *GRAs - Generic Risk Assessments Introduction – Fire and Rescue Service Operational Guidance*, (Page 7) a step-by-step approach to dynamic risk assessments is offered as follows:

1. Identify the hazards.
2 Decide who might be harmed and how.
3 Evaluate the risks and decide on precautions.
4 Record the findings and implement them.
5 Review the assessment and update if necessary.

Dynamic risks are those that are difficult to predict and can result from organizational and environmental changes, such as slip hazards caused by bad weather. Performing dynamic risk assessments can help businesses identify, connect, and visualize clusters of critical risks present in the workplace. This can help reduce the risk of workplace accidents and injuries caused by difficult-to-predict threats or hazards.

Dynamic risk assessments tend to be more checklist-based and focused on industrial safety assessment and response. According to Anear, a dynamic risk assessment helps when risks and hazards arise from such circumstances as:

- Introduction of new equipment/resources.
- Change of supervision approach.
- Opening a new line of business.
- Reallocation of work.
- When there are threats to safety and security.

One could argue this is a "Targeted" risk assessment.

Of note, I do find the five-step approach listed above to be very useful and consistent with my approach to field assessments; however, the concept of the "Dynamic Risk Assessment" is primarily for emergency response and very dynamic, changing circumstances versus a factory risk assessment that takes a week to complete.

3.7 Difference Between Assessment and Audit[57]

It is becoming more common that an industrial customer is increasing their concern for and awareness of cyber and physical security threats to their factories, large buildings, industrial control systems (ICS) and enterprise IT – especially in light of attacks such as WannaCry, Petya, etc. One of the customer's initial actions is to evaluate their options for system security and they often ask for a "risk or security inspection." These "inspections" are often viewed as an "audit" by the customer; however, the customer is better off with an "assessment" instead.

What is the difference between an "audit" and an "assessment?"

Well, the differences are pretty substantial, and each will yield a different level of scrutiny and different sets of actionable results. Also, each will give the management a different sense of how serious their risk is – or is not.

If you look at the differences between an audit and an assessment, consider the following:

- The purpose of an audit is to compare current circumstances against a specific standard or set of standards and find specific gaps where the standard is not being met or achieved. An audit has the inspector comparing the customer's activities against a particular list of requirements in an industry standard. Basically, the audit is identifying whether or not the customer is "complying" with these requirements, but not necessarily exceeding. The problem with this approach is a) the customer needs to identify the standard they expect to follow, and b) the auditor needs to have knowledge and capability to identify if the standard requirement is truly being satisfied or not. Unfortunately, the customer may not have any idea as to the applicable standards and the auditor will tend to not look beyond the standard's requirements for areas needing attention. The audit is looking for "minimum achievement."
    - Of note, it has been my own experience where those industrial customers outside the North American Electric Power and Transmission industry and oil/gas industries

[57] I have written previously about this subject at TechTarget/Search Security. To learn more, please check our https://searchsecurity.techtarget.com/tip/The-difference-between-security-assessments-and-security-audits.

normally don't know what "standard" they should "comply." Therefore, the audit may not even be meaningful since the customer has never been working towards a standard anyway.

- Assessments are about understanding the customer's security posture. The goal of the assessment is to allow for the inspectors to use their experience and practical knowledge in conjunction with other recognized standards/guidelines for cyber and physical risk to look for ways the customer can achieve a higher level of performance and not simply meet minimum compliance. The assessment is not a strictly pass-fail approach but instead intended to give the customer a sense of the current "risk reality." The assessment will also normally provide different gradients of risk to the facility and its operations. For instance, an assessment may categorize the findings as Critical Impact, High Impact, Medium Impact, or Low Impact. The assessment should also nominally provide feedback to the customer on identified strengths as well as informational findings that are outside the scope of the risk assessment. Basically, the assessment will give the customer a list of actions to take to mitigate issues and achieve a more ideal situation rather than simply satisfy a minimum requirement in a standard.
- Industry standards can be used or cited during an assessment; however, for an assessment, the experience of the assessor will also be able to identify the quality of achievement of a standard. This is beneficial to the customer so they can gauge the amount of effort and resources necessary to correct a problem.

Do I use references when performing an assessment? Of course, audits are against a specific standard or set of standards – but that doesn't mean to imply that assessments are not permitted to use any type of standards or guidelines. On the contrary, the more knowledge and experience an assessor has in the area of risk and cyber and physical controls, the better off for the customer. Therefore, in my role as an assessor I still often rely on selected documents to help me with my assessment performance depending upon the client, the facility, the reasons for the risk assessments, the regulatory environment, etc. We will discuss this more in later chapters.

Kip Boyle reminded me of a difference between audits and assessments: audits often become adversarial when conducted by outsiders which in turn encourages insiders to withhold or obscure the real situation if they feel

threatened. This psychology is useful information for the executive management when choosing between an audit and assessment.

3.8 Assessment Models

A risk assessment methodology normally encompasses: a) a risk assessment process, b) an explicit risk model defining key terms and assessable risk factors and the relationships among the factors, c) an assessment approach – qualitative, semi-qualitative, or quantitative, d) an analysis approach (e.g., threat-oriented, asset/impact oriented, or vulnerability oriented). (NIST SP800-30, pages 6-7). In this section of the chapter I would like to offer a survey of different risk assessment models I've referred to over my career. Each model has its strengths that I have implemented in my approach.

3.8.1 ISO 31000

ISO 31000, *Risk Management - Guidelines*, provides principles, framework, and a process for managing risk. ISO 31010, *Risk Management – Risk assessment techniques*, is another document within the ISO 31000 family of publications focused on risk management. The ISO 31000 series risk assessment model is shown below.

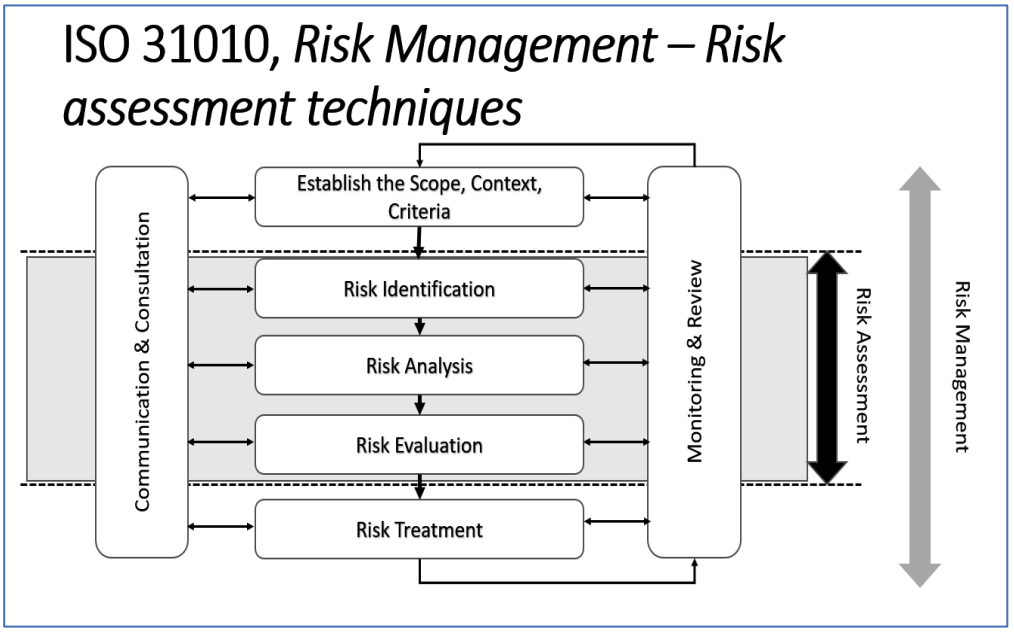


Figure 3-2 ISO 31000 Risk Assessment Model

To reiterate, the ISO 31010 document observes, "Risk assessment provides decision-makers and responsible parties with an improved understanding of risks that could affect achievement of objectives, and the adequacy and effectiveness of controls already in place. This provides a basis for decisions about the most appropriate approach to be used to treat the risks. The output of risk assessment is an input to the decision-making processes of the organization."

This model is simple, easy to follow, and gives the assessor some general guidance on how to start performing a risk assessment; however, step-by-step details on the contents of each element are not easily collected from the ISO document. The contents of each element are summarized below.

Risk Identification

Risk identification is the process of finding, recognizing, and recording risks – including hardware and software events, and human and organizational factors. ISO 31010 observes that risk identification methods can include:

- Evidence-based methods – for me, these are primarily field observations, document reviews, interviews, and inspections.
- Systematic team approaches where a team follows a systematic process to identify risks using a structured set of questions or prompts.
- Inductive reasoning approaches and techniques such as Hazard and Operability Study (HAZOP)[58] .
- Using supportive techniques such as brainstorming and/or the Delphi methodology.

Risk Analysis

Simply stated, risk analysis is about developing and understanding of the risks identified in the Risk Identification phase. Risk analysis activities

[58] From the American Institute of Chemical Engineers (AIChE), Center for Chemical Process Safety, A HAZOP is a systematic qualitative technique to identify process hazards and potential operating problems using a series of guide words to study process deviations. A HAZOP is used to question every part of a process to discover what deviations from the intention of the design can occur and what their causes and consequences may be. This is done systematically by applying suitable guidewords. This is a systematic detailed review technique, for both batch and continuous plants, which can be applied to new or existing processes to identify hazards.

determine the consequences and likelihood of identified risk events, taking into account the presence of any existing technical or process controls.

The supporting activities within this phase include:

- Controls assessment.
- Consequence analysis – determine the nature and type of impact.
- Likelihood analysis and probability estimation.
- Sensitivity analysis – involving the determination of the size and significance of the risk.
- Uncertainty identification and documentation.

Risk Evaluation

Risk evaluation includes comparing estimated levels of risk with risk criteria defined in the Context phase. This helps the organization get a sense of the significance level and type of risks.

Risk evaluation also uses ethical, legal, financial, and "perceptions of risk" as inputs to this phase. The decisions that are made during this review could include whether a risk needs any treatment (e.g., a tsunami threat in Kansas). Also, the decisions consider the priorities for taking any action on the risks and whether an activity should even be performed.

The ISO 31010 document suggests dividing risks into three bands:

- Upper Band – Level of risk is considered intolerable, whatever benefits the activity brings, and risk treatment is essential whatever the cost.
- Middle Band (a/k/a "grey" area) – Level of risk where costs and benefits are accounted for and balanced against possible consequences.
- Lower Band – Level of risk is regarded as negligible or so small that risk treatment measures are not necessary.

3.8.2 NIST SP 800-30, R1 – Guide for Conducting Risk Assessments

The US National Institute of Standards and Technology (NIST) has published a guide for performing risk assessments. Although the guide is

primarily focused on information technology organizations and systems, the guide offers a risk assessment flow similar to ISO 31010.

The general scheme included in NIST SP 800-30, Revision 1, is shown below:

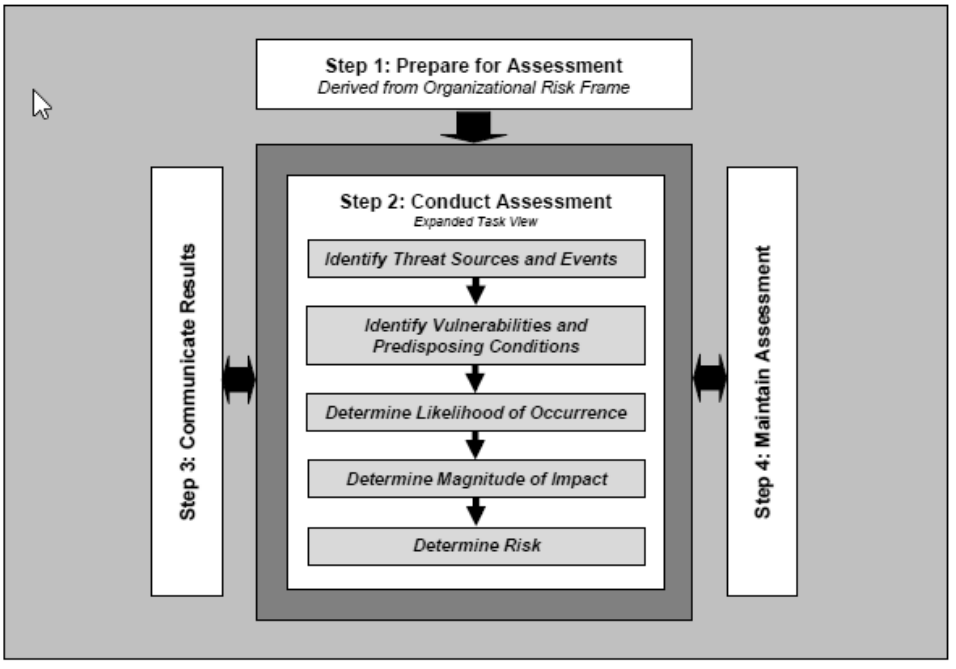


Figure 3-3 NIST SP 800-30 R1, Figure 5, Page 23

Although this does look very similar to the ISO 31010 flow chart, it breaks down the "Risk Identification" into the components of risk.

Previously I included the risk equation and how its fundamental elements include "threats," "vulnerabilities," and "consequence/impact." Well, the NIST SP 800-30 R1 breaks down the assessment into first, identifying the threat sources and events. This is followed by identifying vulnerabilities and predisposing conditions.

The consequence/impact aspect is broken up into determining the likelihood of occurrence and then the magnitude of the impact.

Essentially the SP 800-30 R1 approach is encouraging the assessment team to build the risk case element by element.

Intuitively, I like the approach, but it still doesn't offer much detail on *how* to perform the steps.

3.8.3 NIST SP 800-30, R0 – Risk Management Guide for Information Technology Systems

NIST SP 800-30, R0 was issued in 2002 and withdrawn in 2012 when NIST SP 800-30, R1 was published. This particular product from NIST is one of my favorites due to the level of detail offered in the risk assessment methodology included in Figure 3-1, Page 9, of this work.

This section of the chapter will be a more detailed review of the contents of this standard because it has been withdrawn from publication and does contain some excellent guidance I have used for my assessments of large industrial facilities.

The flowchart and its details are included below:

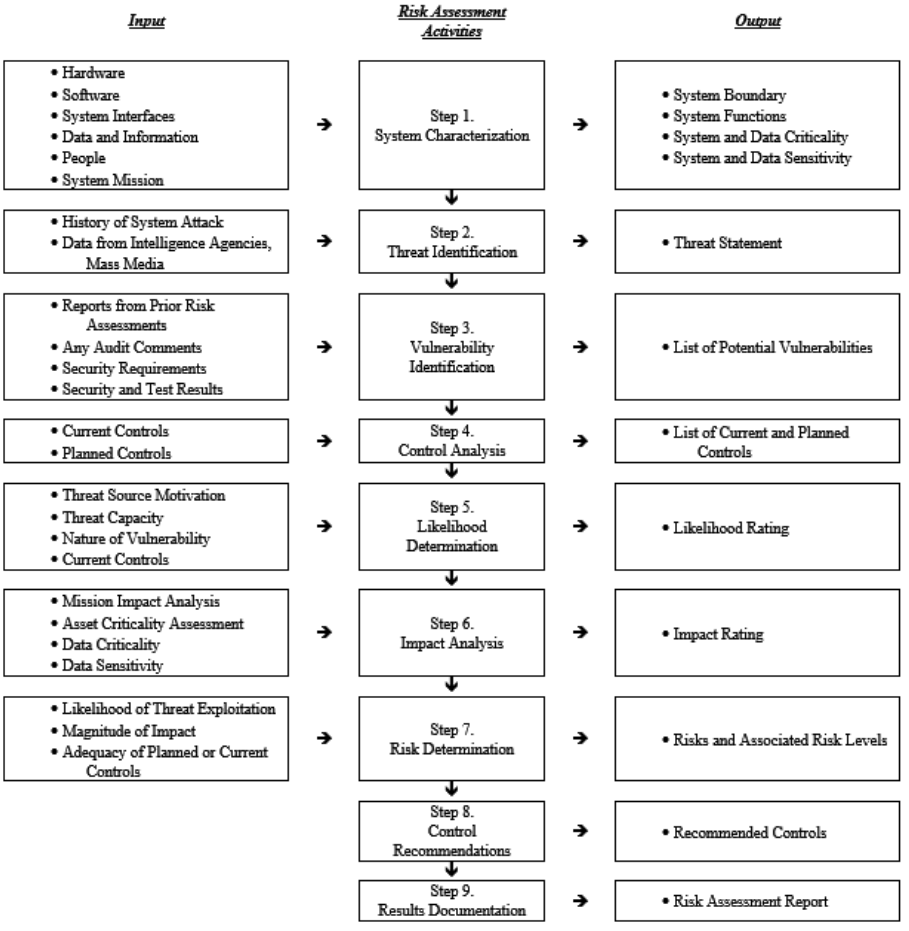


Figure 3-4 NIST SP 800-30, R0, Risk Assessment Methodology Flowchart

Admittedly, the process flow is similar to NIST SP 800-30, R1; however, this is more of a checklist approach for the assessment leader which I will address below.

Step 1: System Characterization:

This step is essentially determining the context of the risk assessment. Here the assessment team needs to collect system and plant-related information. Some items to include – which I'll cover in more detail later on when discussing preparing for a risk assessment –are:

- Physical buildings to be evaluated – Physical security environment.
- Systems to be reviewed.
- Hardware.
- Software.
- System interfaces – both internal and external connections.
- Data and information used and collected by the systems and hardware/software.
- Persons who support the plant, systems, hardware, software.
- System and data criticality – or importance to the enterprise/overall organization and/or country.
- System and data sensitivity.

As observed the output of this step includes a collection of information extremely useful for the assessment. The assessment team will have collected drawings and lists associated with the operation of the facility and its mission. The team needs to remember this information is extremely sensitive and, if in the hands of an outsider or attacker, could be detrimental to plant security, operations, or community perception and corporate reputation. Therefore, the team needs to treat this information carefully and protect it as if it were plant or corporate confidential information.

Step 2: Threat Identification

In Chapter 3 the definition of threats and their consideration in the risk equation was discussed. The NIST document suggests the assessment team identify the potential "threat sources."

A “Threat Source” is defined as either 1) intent and method targeted at the intentional exploitation of a vulnerability, or 2) a situation and method that may trigger a vulnerability. Common threat sources per NIST SP 800-30, R0, are categorized as natural, human, or environmental.

- Natural threat examples: Earthquakes, tornadoes, landslides, floods, avalanches, electrical storms, etc.
- Human threats: Events that are enabled by or caused by human beings such as unintentional actions (e.g., errors, omissions) or deliberate actions (e.g., insider threat). Don’t forget to ask about how terminated employees are handled relative to their plant physical and computer access.
- Environmental threats: Events such as long-term power outages; air, water, and soil pollution; chemicals; liquid leakage (e.g., leaking fire protection sprinkler head), etc.

So, how do you obtain this information? Consider looking at plant security history (physical and cyber), violation reports and operations incident reports. Perform an open source intelligence (OSINT) review of the industry sector, company, and plant on the internet to identify threats and threat sources. Look at such agencies for threat information as the US Cybersecurity and Infrastructure Security Agency (CSIA) (https://www.us-cert.gov/about-us), the UK Centre for the Protection of National Infrastructure (CPNI) (https://www.cpni.gov.uk/), industry Information Sharing and Analysis Centers (ISACs) related to the company/plant to be assessed. Even looking at news items online related to the company/plant and the surrounding area may be helpful to identify the threats of concern.

The output of this step is a “threat statement” identifying a list of threat sources that could exploit the company and plant.

Step 3: Vulnerability Identification

Admittedly, when performing Step 2, you will also uncover potential vulnerabilities that could be triggered or taken advantage of resulting in a corporate/plant event.

Again, we will go into more detail on this subject in the later chapters when preparing for and conducting a site assessment. But, before you head off to the field to perform the assessment, be sure to review such documents as:

- Previous risk assessments of the corporation, plant, sister plants, and internal systems (if available).
- Any previously performed audits.
- Vulnerability lists associated with corporate and plant hardware and software to be assessed.
- Previously performed security assessments such as penetration tests, cyber vulnerability tests, etc.

The output of this step is a list of corporate/plant/system vulnerabilities that could be exercised by a threat source.

Step 4: Control Analysis

This step is intended to prepare the assessment team to understand the types of controls that have been implemented or planned for by the corporation/plant management.

When you consider controls, the first categories to evaluate are:

- Management
- Operational, and
- Technical.

Additionally, controls can be divided into both preventive or detective. A preventive control is intended to inhibit attempts to violate security and include activities such as access control enforcement, authentication for physical and cyber access, etc. Even encryption is considered a preventive control.

Detective controls are those controls reviewed *after* an event occurs. For example, violation of a fence perimeter monitoring system will result in an alarm but does not prevent the intruder (that is the job of the fence).

The output of this step is a list of current or planned controls used by the corporation/plant to mitigate the likelihood of a vulnerability being exploited by a threat source.

Step 5: Likelihood Determination

Now that we have identified the context of the assessment, made lists of the threats, vulnerabilities, and controls, the next step is to consider the likelihood a vulnerability can be exploited by a threat.

In theory the likelihood is usually broken down into high, medium, and low gradients and is the probability of the event occurring.

The table from NIST SP 800-30, R0, for likelihood is included below and is used when developing your output or assessment product:

Table 3-1 NIST SP 800-30, R0 Likelihood Definitions

Likelihood Level	Likelihood Definition
High	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Step 6: Impact Analysis

When performing this step, you will require additional information. First, you will require a Business Impact Analysis (BIA) which is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency. (Rouse, 2019)

According to Margaret Rouse in her TechTarget SearchSecurity article regarding BIA, business impact analysis and risk assessment are two important steps in a business continuity plan. A BIA often takes place prior to a risk assessment. The BIA focuses on the effects or consequences of the interruption to critical business functions and attempts to quantify the financial and non-financial costs associated with a disaster. The business impact assessment looks at the parts of the organization that are most crucial. A BIA can serve as a starting point for a disaster recovery strategy and examine recovery time objectives (RTOs) and recovery point objectives (RPOs), and resources and materials needed for business continuance. (Rouse, 2019)

A second element to review as part of the impact analysis is an asset criticality assessment which identifies and prioritizes corporate and/or plant assets supporting the organization's critical missions.

Similar to Step 5, the magnitude of the impact can be ascertained using the table from NIST SP 800-30, R0, page 23 shown below:

In the world of business continuity and disaster recovery the phrases Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) are professional terms of art.

An RTO is the overall length of time a system or process can be in recovery phase before negatively impacting the enterprise's mission and/or business functions. This would be for a critical process necessary to assure the survival of the enterprise. (e.g., the email system can only be out of service for no more than four hours).

An RPO is the point in time in which data or a system must be recovered after an outage. (e.g, the water treatment system must be up and running at 50% capacity within seven calendar days after a 5.0 earthquake).

Table 3-2 NIST SP 800-30, R0, Magnitude of Impact Definitions

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerabilities (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources; or (2) may noticeably affect an organization's mission, reputation, or interest.

The result of this step is identification of the magnitude of impact of the identified risks.

Steps 7, 8, and 9: Risk Determination, Control Recommendations and Results Documentation

In the process identified in NIST SP 800-30, R0, the risk determination is the culmination of steps 1 through 6. Normally, when performing a site risk assessment, I normally do not perform the ultimate risk declaration until I have departed the site and re-reviewed the collected information.

The risk determination process will be reviewed in a later chapter but does rely upon many elements and definitions in NIST SP 800-30, revisions 0 and 1.

Similarly, the control recommendations tend to be developed once the risk is identified for each vulnerability identified. These control recommendations are usually reflected as recommendations to the corporate/plant management on ways to respond to the finding and its associated risk(s).

Of course, documentation is the final element of the risk assessment and will be discussed in substantial detail later in this book.

Overall, NIST SP 800-30, R0, is an excellent "how-to" guide and many of its elements will be woven into the later discussions on ***how*** to perform a risk assessment of critical infrastructure and industrial facilities.

3.8.4 Cyber Security Assessments of Industrial Control Systems – Good Practice Guide

This document was jointly prepared in 2010 by the US Department of Homeland Security (DHS) and the UK Centre for Protection of National Infrastructure (CPNI). The guide provides their vision and overview of the assessment process to aid users in understanding how to execute an ICS cyber security assessment. This guide also covers the process of planning an ICS cyber security assessment, including how to select testing areas.

This is another guide I have relied upon when planning and conducting my field risk assessments. Unfortunately, the guide has been withdrawn from both DHS and CPNI but is available at the Water Information Sharing and Analysis Center (WaterISAC) website (https://www.waterisac.org/).

Figure 4 of this document is replicated below and is the true gem in this document. It offers the reader and assessment leader the opportunity to get an overview of the risk assessment process.

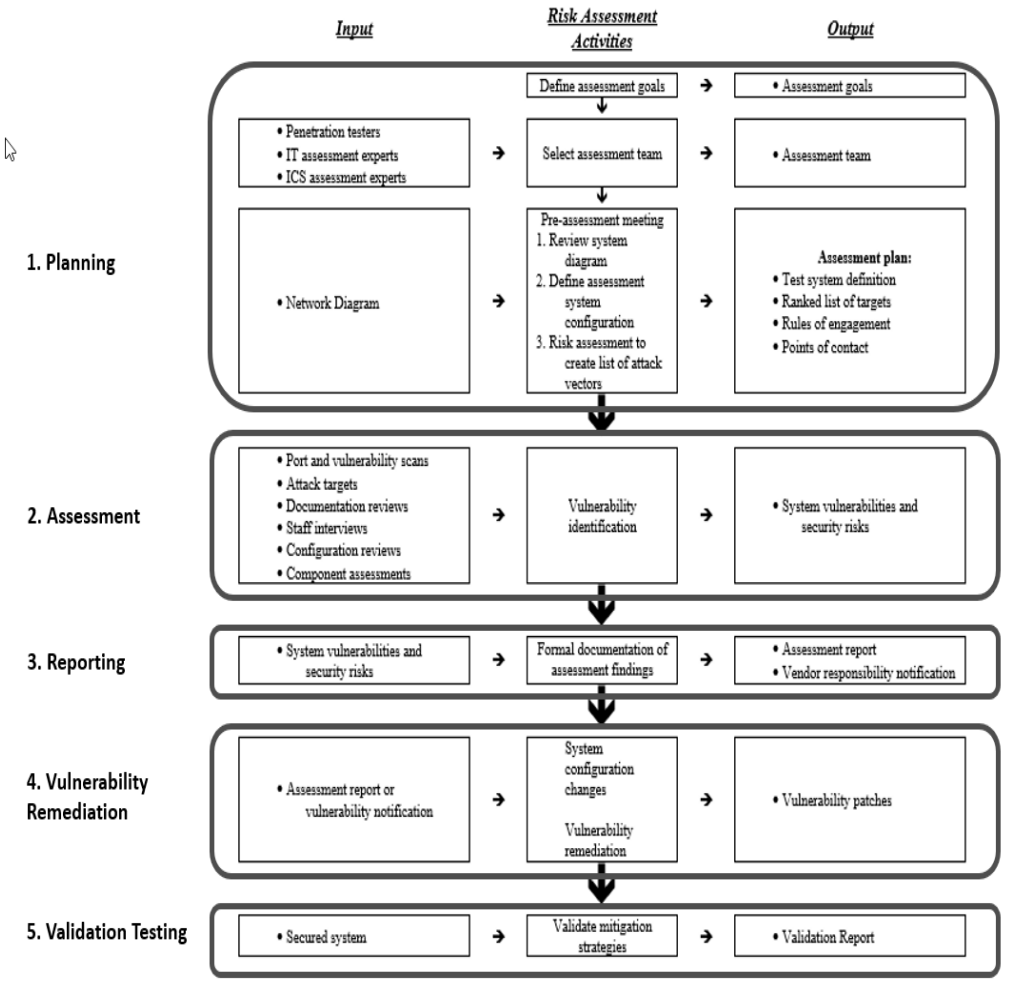


Figure 3-5 DHS-CPNI Assessment Process Flow Chart

When you examine the process flow chart, it does provide some excellent flow on activities and results – similar to the NIST SP 800-30, R0 – however, it is very focused on a cyber assessment process known as a "vulnerability test." Vulnerability tests are an element of an organization/facility risk assessment but should not be the only activity. That said, this still gives the user a recipe on how to perform a cyber risk assessment.

One new element in this process – when compared to earlier models cited in this chapter – includes the practical aspects of assessment team selection.

This will be discussed later on in the book when reviewing the preparation phases.

It should also be observed that this process flow goes beyond the activities normally performed in a risk assessment. For instance, vulnerability remediation and validation testing typically is categorized as a risk management activity.

Overall, though, I found this assessment model a refreshing way to look at the assessment process and it offers some practical considerations when performing the organization/facility risk assessment.

3.8.5 Hybrid Risk Assessment Flow Chart

Having conducted numerous risk assessments at industrial facilities, and using the above references as guides and assistance, I have developed a "hybrid" assessment process which captures the strengths of the systems I've highlighted and made it more "user friendly.

The suggested hybrid approach is shown in the figure below and will be the basis for the remaining chapters in this book.

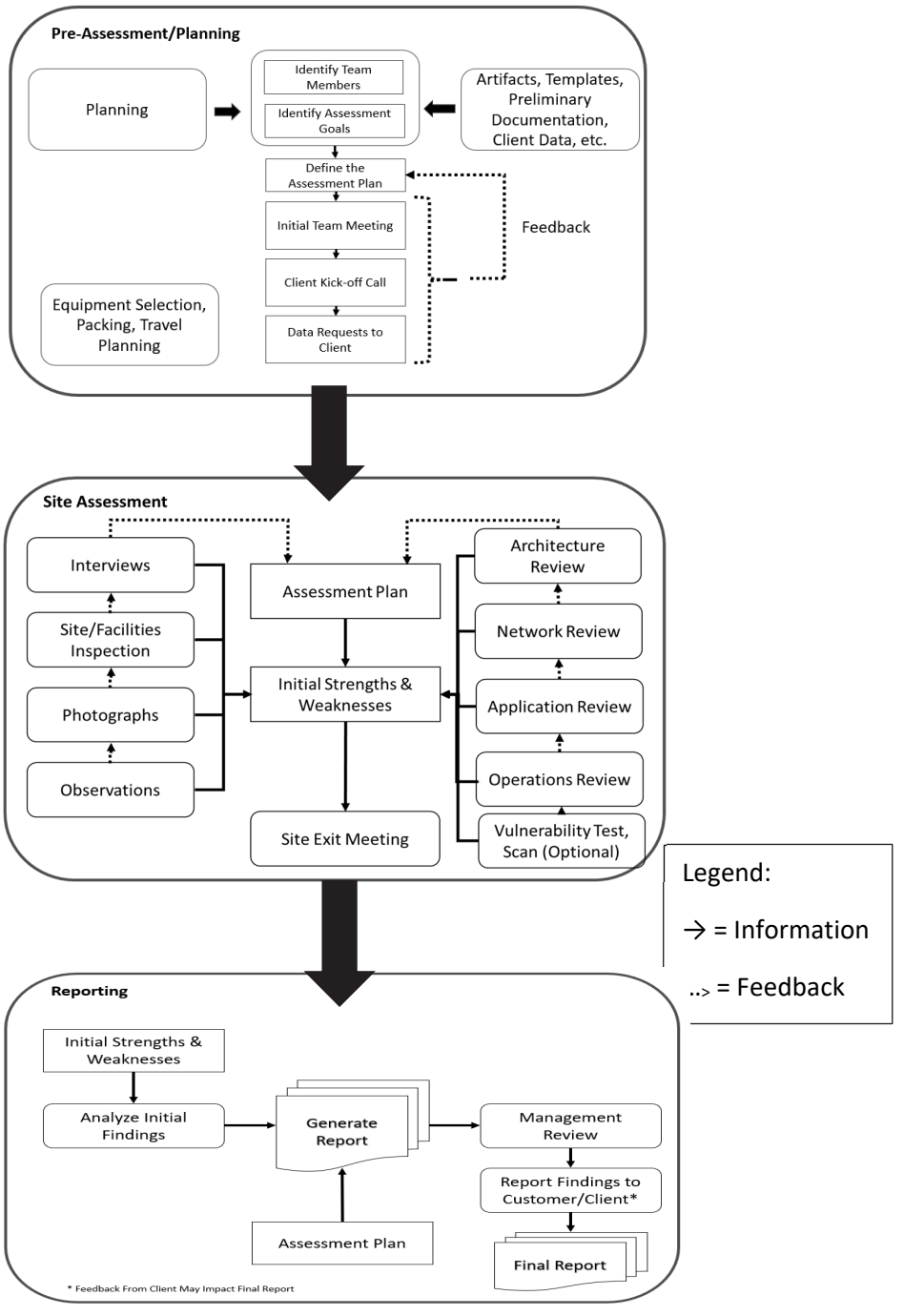


Figure 3-6 Hybrid Facility Risk Analysis Flow Chart

Note that this flow chart does include some of the practical activities normally excluded from the NIST and ISO assessment processes.

You may want to take some time to review and study this flow chart and I'll be sure to include the appropriate sections in each chapter as we proceed.

3.9 Assessment Process

The process of conducting a large facility risk assessment is a fairly simple and logical methodology. As for most projects the first steps are to prepare for the work, do the work, then report on the results. So, as we prepare for the next chapters, I'd like to offer a high-level view of each of the primary sections of the assessment.

On a side note, this process can be used for a week-long risk assessment of a large facility or even a single day at a site. For example, I performed a one-day, very fast risk assessment of a 30-story business building in a Canadian city. I used the same approach shown in the flow chart; however, many of the activities were quick surveys rather than long, deep inspections. Admittedly, this quick approach is not desired; however, it can still be a Pareto approximation just to see the "low-hanging fruit."

As a rule of thumb, for a one-week site assessment you can assume the work nominally requires the following:

- Pre-Assessment – 2 Calendar Weeks.
- On Site Assessment – 1 to 2 Calendar Weeks.
- Reporting – 1 to 3 Calendar Weeks.

3.9.1 Pre-assessment/Planning

As noted in the ISO and NIST approaches to risk assessment, you need to understand and set the context for the review. What is the purpose of this risk assessment? What are the drivers for the performance of the assessment? Is this a preparatory review before an audit or is this a risk assessment after a major site event or accident?

The reason for the assessment will certainly dictate your approach and the areas where you spend the most time.

Besides the scope, a useful element to consider is the scope of the assessment. That is, the "who, what, where, when, how, why, and if." For

instance, is this an assessment of a single site or even a single building or is it of multiple sites located in multiple jurisdictions?

In one instance I was hired by a major global corporation to perform risk assessments at multiple locations. The locations ranged from the United States to Egypt, Nigeria, China, and Indonesia. Each site was different from the standpoint of culture and local laws and regulations; however, each site still needed to be evaluated for the same risk elements – i.e., cyber, physical security, manufacturing risks, industrial safety, etc. Regardless, these reviews each had a unique context and scope.

Don't forget the client's risk tolerance and risk appetite as you prepare for and conduct the risk assessment. There may be some very sensitive areas that could impact the assessment performance. For instance, the client may not have very good relations with the union. Therefore, field assessments need to take this into account to ensure grievances are not generated.

Another risk tolerance/appetite element could be the client's recent history with any regulators. Regulatory reviews may have raised some serious concerns and, as an assessor, you need to be aware of these to ensure the facts of the assessment are couched with some context.

The pre-assessment planning requires selecting a team of capable and skilled individuals who can contribute positively to the assessment plan and approach.

Planning will also include reviewing multiple documents about the client site and history. Some of this information will be provided by the client and some will be generated through open source intelligence reviews (OSINT) on the internet. We will discuss in detail the type of information you will want to collect and review before departing for the site.

The documentation you need to collect and develop for the assessment varies based on context and the purpose of the assessment itself. You will still need to generate and record the assessment goals and assessment plan.

Again, there will be more details on this provided in the Pre-Assessment section of this book.

3.9.2 Conducting the Assessment

Using the assessment goals and plan, the site assessment is primarily for information collection. The effort begins with an entrance meeting with the site management and concludes with an exit meeting before departing to write the assessment report.

During the site assessment, activities will normally include:

- Interviews.
- Observations of work, documentation, and systems/components/buildings, etc.
- Inspections.
- Photography of key strengths and concerns.
- Reviews of architecture, network infrastructure, and applications in use.
- Etc.

Each of these activities will be discussed in detail in the Site Assessment section of this book.

It is paramount that the client and site management are committed to the assessment effort and support it accordingly. If they do not or will not, the assessment could fail, and the results may be for naught. Make sure this particular aspect is addressed even before your team arrives onsite. Ensure management is fully supportive during your pre-assessment calls, entrance meeting, and even during the exit meeting before you begin to write the report.

The team needs to perform a daily end of the day debrief on their discoveries. This entails a face-to-face meeting of the team where strengths and weaknesses identified that day and activities for the next day are reviewed. Also, any documentation collected needs to be reported to the team should other team members find the information germane to their focus areas.

Remember, the documentation you write and collect is sensitive and essentially confidential to the client. Handling and disposal should be performed properly.

On the last day of the site effort an exit meeting is held with the site management team. This could simply be a meeting only with the plant manager or it could be a review of the preliminary assessment strengths and weaknesses with the site staff. That is the plant manager's decision.

Note how I've stated the review is of strengths and weaknesses. It is *not* appropriate for the team to develop any findings or good practices at the site. This declaration is normally performed in the Reporting Phase where the assessment team's management has time to review the strengths and weaknesses before they become cited as good practices and findings respectively.

3.9.3 Reporting

Remember the adage, "The job isn't finished until the paperwork is done." Yes, that is the reporting phase.

In this phase the team will review all the collected information, observations, photographs, site documents, reviews conducted onsite, etc. and identify the following:

- Strengths → That may become "Good Practices."
- Weaknesses → That may become "Findings" or "Documented Concerns."
- Risk levels of the findings (usually qualitative – Critical, High, Medium, Low).
- Recommended actions to resolve the findings/documented concerns.

Once the decisions are made regarding the Good Practices, Findings, and Risk Levels, the report is written and reviewed by the assessment team management. The draft report is then sent to the client for initial review and feedback including requested changes, deletions, etc.

Following the iterative review, the report is declared Final.

The next chapter is focused on the Pre-Assessment activities.

3.10 Questions for Further Thought and Discussion

1. Of the risk assessment models discussed in this chapter, which one is the most intuitive? Which one is the most complicated? Why?
2. Describe when you would use a Deductive Risk Assessment. Describe when you would use an Inductive Risk Assessment.
3. Why do you think it is difficult to perform a qualitative risk assessment?
4. For your company, what would be the focus of your first risk assessment? Why?
5. Describe when you would use a Targeted Risk Assessment.

REFERENCES

101 Computing. (2018). *Heuristic Approaches to Problem Solving*. 101 Computing. https://www.101computing.net/heuristic-approaches-to-problem-solving/

American Institute of Chemical Engineers (AIChE). (n.d.). *Hazard and Operability Study (HAZOP)*. Center for Chemical Process Safety. Retrieved November 4, 2019, from https://www.aiche.org/ccps/resources/glossary/process-safety-glossary/hazard-and-operability-study-hazop

American Society of Safety Professionals (ASSP). (2019). *Conducting a Risk Assessment*. American Society of Safety Professionals. https://www.assp.org/news-and-articles/2019/02/12/conducting-a-risk-assessment

Anear, L. (2019). *Dynamic Risk Assessment Templates*. Safety Culture IAuditor. https://safetyculture.com/checklists/dynamic-risk-assessment/

ASIS International. (2015). *Risk Assessment*. ASIS International. https://www.asisonline.org/publications/sg-risk-assessment-standard/

ASIS International. (2003). *General Security Risk Assessment Guideline*. ASIS International. https://www.asisonline.org/publications/sg-asis-general-security-risk-assessment-guideline/

Bliss, E. (2019). *Eula Biss - Some of the most interesting research that I...* BrainyQuote. https://www.brainyquote.com/quotes/eula_biss_724462?src=t_assessment

Burney, S. M. ., & Saleem, H. (2008). *Inductive & Deductive Research Approach*. https://www.researchgate.net/publication/330350434_Inductive_and_Deductive_Research_Approach

CPNI - Centre for Protection of National Infrastructure (UK), & DHS - Department of Homeland Security (US). (2011). *Cyber Security Assessments of Industrial Control Systems*. https://www.waterisac.org/portal/library/2001dhs-cpni-cyber-security-assessments-industrial-control-systems-good-practice

Cribbs, D. (2018). *Security Principles and Practices Presentation*.

Department for Communities and Local Government (UK). (2009). *GRAs - Generic Risk Assessments Introduction -- Fire and Rescue Service Operational Guidance*. https://www.gov.uk/government/publications/generic-risk-assessments-introduction

European Committee for Electrotechical Standardization. (2010). *BS EN 31010:2010 Risk management. Risk assessment techniques*. https://shop.bsigroup.com/ProductDetail/?pid=000000000030183975

Hayden, E. (2017). *The difference between security assessments and security audits*. Tech Target - Search Security. https://searchsecurity.techtarget.com/tip/The-difference-between-security-assessments-and-security-audits

ISO. (2019). *ISO - IEC 31010:2019 - Risk management — Risk assessment techniques*. https://www.iso.org/standard/72140.html

ISO. (2019). *ISO - ISO 31000 Risk management*. https://www.iso.org/iso-31000-risk-management.html

Joint Task Force Transformation Initiative. (2012). *Guide for Conducting Risk Assessments SP 800-30 R1*. https://doi.org/10.6028/NIST.SP.800-30r1

Krzemien, A. (2019). *Contribution of risk assessment to the risk management process. Based... | Download Scientific Diagram*. ResearchGate. https://www.researchgate.net/figure/Contribution-of-risk-assessment-to-the-risk-management-process-Based-on-ISO-IEC-31010_fig2_290237628

Modarres, M. (2006). *Risk Analysis in Engineering: Techniques, Tools, and Trends*. CRC Press.

Murphy, J. (2016). *What is a Risk Assessment. Read Our Free Guide*. HS Direct Ltd. https://www.hsdirect.co.uk/free-info/risk-assessment.html

Peterson, O. (2019). *What Is ISO 31000? Getting Started with Risk Management | Process Street | Checklist, Workflow and SOP Software*. Process.St. https://www.process.st/iso-31000/

Rausand, M. (2011). *Risk Assessment: Theory, Methods, and Applications*. John Wiley & Sons, Inc. https://books.google.com/books?id=9EHeLmbUVh8C&pg=PT21#v=onepage&q&f=false

Rouse, M., & Sliwa, C. (2019). *What is a business impact analysis (BIA)? Definition from WhatIs.com*. TechTarget - SearchStorage. https://searchstorage.techtarget.com/definition/business-impact-analysis

Steel, W. (2018). *Cybersecurity for Water Utilities | WaterWorld*. WaterWorld. https://www.waterworld.com/municipal/water-utility-management/article/16190093/cybersecurity-for-water-utilities

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for information technology systems :(Withdrawn)*. https://doi.org/10.6028/NIST.SP.800-30

UK Health and Safety Executive. (n.d.). *Risk management: Health and safety in the workplace*. Retrieved September 12, 2019, from http://www.hse.gov.uk/risk/

UK Health and Safety Executive (HSE). (2014). *Risk assessment - A brief guide to controlling risks in the workplace*. http://www.hse.gov.uk/pubns/indg163.htm

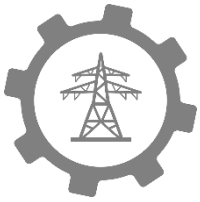
UK Health and Safety Executive (HSE). (2019). *What are the five steps to risk assessment? | WorkSmart: The career coach that works for everyone*. Worksmart. https://worksmart.org.uk/health-advice/health-and-safety/hazards-and-risks/what-are-five-steps-risk-assessment

US Department of Defense Civilion Personnel Advisory Service. (2016). *DOD Mentoring Resource Portal CRITICAL THINKING AND PROBLEM Information for Supervisors Portfolio*. *April*. https://www.dcpas.osd.mil/Content/Documents/CTD/DCPASCriticalThinkingandProblemSolvingLesson.pdf

US Department of Homeland Security, & CPNI - Centre for Protection of National Infrastructure (UK). (2010). *DHS / CPNI - Cyber Security Assessments of Industrial Control Systems Good Practice Guide | WaterISAC*. https://www.waterisac.org/portal/library/2001dhs-cpni-cyber-security-assessments-industrial-control-systems-good-practice

Valis, D., & Koucky, M. (2009). Selected Overview of Risk Assessment Techniques. *Problemy Eksploatacji*. http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-article-BAR0-0046-0019/c/httpwww_bg_utp_edu_plartpe42009pe42009019032.pdf

Walsh, T., & Healy, R. (2012). *Protection of Assets: Physical Security* (T. L. Williams, M. E. Knoke, & M. L. Garcia (Eds.)). ASIS International.

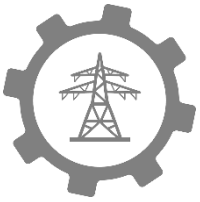


PART II
HANDBOOK

Part II of this book is the true “handbook” for conducting a risk assessment. It includes key and detailed discussions on:

- Getting ready for the assessment.
- Understanding the foundational concept of the Observation and how it fits into the risk assessment process.
- Performing the risk assessment at the client site.
- Putting together the final report.
- Remediating the findings and prioritizing/mitigating the identified risks.

The appendix – which is part of Part II – is an example risk assessment representative of the reports I’ve written over the years.



Chapter 4
Pre-Assessment

"A prudent man foresees the difficulties ahead and prepares for them; the simpleton goes blindly on and suffers the consequences."

– Proverbs 22:3 (Bible)

Or

By failing to prepare, you are preparing to fail.

– Ben Franklin (Brainy Quote)

We are finally beginning a discussion on the practical elements of performing a risk assessment! Hooray!

In this chapter you will discover:

- An overview of how to prepare for the site/customer visit.
- The key items to consider when selecting the assessment team.
- The processes to be followed prior to departing for the customer site.

Where are we in the overall process? We are focused on ***"Pre-Assessment and Planning"*** as depicted in the graphic below from Chapter 3.

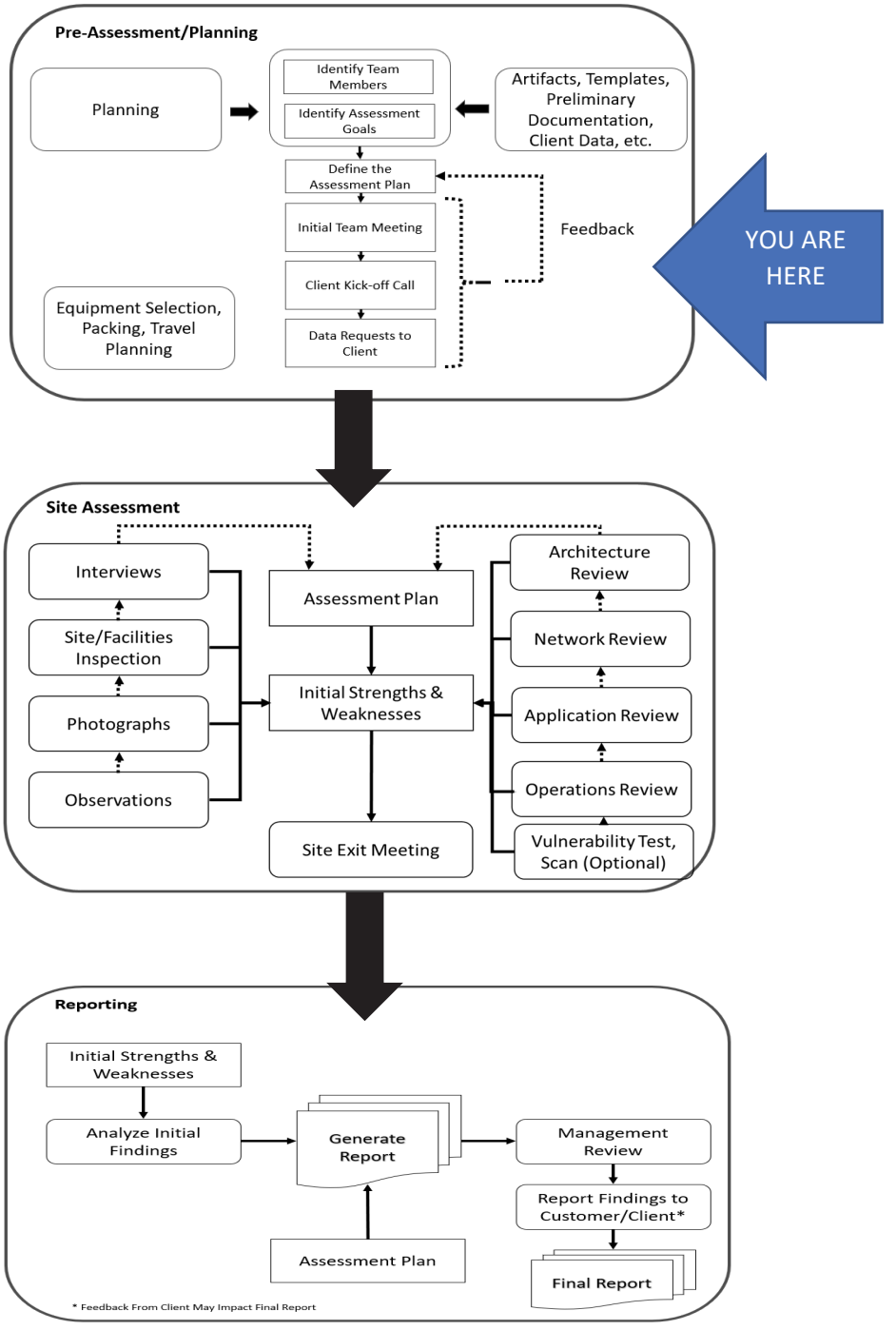


Figure 4-1 Hybrid Facility Risk Analysis Flow Chart

4.1 Planning

What do you think would prompt a risk assessment of a large industrial facility or critical infrastructure? It could be a number of things from regulatory drivers, insurance inspections, accident investigations, legal issues, or disconcerting events at your competitor sites. The assessment could be required for political reasons. Each reason or category of driver will affect how you plan for the risk assessment performance.

Let's look at the example of a disconcerting event at your competitor. Your boss may have heard of this event or accident and decided a risk assessment of your company's facilities is appropriate to ensure the company is not at risk to the same issue. Thus, the risk assessment may be fairly focused to ensure that the event impacting your competitor cannot occur at your site. Hence, the focus will be fairly narrow and may be a "vertical look" at the site processes and procedures that address the specific event or accident.

For regulatory assessments, the primary preparatory focus will be on defining the regulations to be assessed and even audited. This could be a very broad perspective for the assessment team, but it is still moderately defined and bounded by the regulations to be assessed – such as the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. Other examples of regulatory-driven assessments could be due to the US Federal Food and Drug Administration (FDA), US Environmental Protection Agency (EPA), etc.

Insurance assessments may be more interesting since the inspections will be closest to looking for true risk to the facility and organization. An insurance assessment will be focused on risks to the facility – possibly industrial safety or process oriented. Preparation for the assessment will still have some boundaries or "guard rails" for the scope due to the reason for the assessment.

Regarding the assessment plan, it is beneficial to the assessment team and the client to create an assessment plan *before* commencing the review to ensure that all entities are aware of how the assessment will operate. This planning will include the rules of engagement, whether or not any cyber scans are to be performed, key points of contact, "no-touch" zones, etc. Also, now is a good time to ensure site management supports the risk assessment effort.

The level of effort will be dictated by several factors. The first factor to consider is why the assessment is being performed. As highlighted above, the assessment could be due to an accident, cyber event, or regulatory driver.

The level of effort will also be fine-tuned after your first conversation with the client being assessed. Details on current plant events, outages, turnarounds, etc. will be helpful to again guide the assessment team and its plan.

The most important part of planning the assessment is the plan should not constrain the assessment team to a singular approach to a problem. The plan should allow the assessment team the ability to look above, around, under, and at the problem being assessed. The team may gain substantial perspective on the root cause of an event if they are permitted to examine other extenuating circumstances, cause and effect, etc.

The assessment plan should loosely define the scope of the assessment; however, it should not constrain the assessment team on ***how*** to conduct the review. This permits the assessment team to use all their skills and experiences to accomplish the goals of the risk assessment. After all, a potential attacker is not going to follow any precise rules of engagement.

4.2 Identify Team Members

The assessment team makeup and especially the team leader will determine the success or failure of the risk assessment. The team member roster is affected by multiple circumstances but should include the following considerations.

- **Team Leader:** The team leader should be an excellent oral and written communicator. They should have strong interpersonal skills and handle conflict professionally. They should be technically competent – especially relative to the reason for the assessment. The leader will need to have both the capability to look at the "big picture" the assessment is identifying, but also can possess an attention to detail. Finally, the team leader needs to be adept at asking "WHY" as issues surface and looks for cause and effect – perhaps even "root cause."

  A background in risk and security (cyber and physical) are an operational necessity for the successful leadership of the team.

Optimally the team leader will understand and be qualified to implement event and causal factor charting, root cause analysis, and capture of the "fundamental overall problem" (a/k/a FOP) when looking at a list of what appears to be disparate findings and issues.

The team leader should be an experienced and titled manager or supervisor by title and can communicate with senior management without hinderance.

Finally, internal candidates may prove to be more valuable for this role since they typically have an existing understanding of the business and relationships with leaders across the organization. (Miller, 2013) However, internal candidates could be negatively impacted by their concern for "not rocking the boat" as findings and issues are raised by the team. Therefore, an objective leader is needed.

The other team members are selected based on availability and on the reasons and goals of the risk assessment. Consider the following types of individuals to include on the assessment team:

- Regulatory or compliance experts (as necessary for the risk assessment).
- Physical security expert(s).
- Cyber security experts.
- Process or facility engineers.
- Maintenance staff.
- Contractors or suppliers involved with the areas the risk assessment will focus.
- Supply chain and logistics experts.
- Project management – especially for large and complex risk assessments.

The intent is to build a team with a broad range of expertise and experience in both technical capabilities and business knowledge. The team members should also be considered for their own personal networks where they can draw upon expertise of peers and integrate that with their own experiences and knowledge. (Miller, 2013)

According to Tony Miller in his article "How to Build an Effective Threat Assessment Team," the best potential candidates should demonstrate a great deal of creativity. Risk assessment is not a task that can be performed simply by following a checklist. Rather, the assessor needs to be capable of seeing relationships between many pieces of information at a highly abstract level. An inquisitive nature can also be a great asset in a potential candidate. Look for the "tinkerers," the types of people who like to take things apart to understand how they work. This curious nature is valuable when it comes to developing a deeper understanding of potential vulnerabilities and identifying how they may be exploited by potential threats. (Miller, 2013)

4.3 Identify Assessment Goals

The foundation of the assessment goals is the reason for the risk assessment itself. If the assessment is being driven by a regulatory or compliance issue (e.g., NERC CIP), the assessment goals will not include analysis of industrial safety compliance per se. That does not exclude industrial safety reviews; however, the focus of the assessment should answer the questions raised by the regulatory issues.

The objectives of the assessment may include achievement of the following:

- Documentation reviews.
- Staff interviews.
- Component assessments.
- Configuration reviews (component and system-level).
- Observations of work performed by the client staff.
- Physical security inspections and walk-downs.
- Cyber vulnerability scans and penetration tests.

Added guidance for the risk assessment goals may include (Rovins):

- Extent and type of risks that are tolerable and how unacceptable risks are treated.
- Responsibility and authority for undertaking the risk assessment.
- Resources available to carry out the risk assessment.
- How the risk assessment will be reported and reviewed.

It is also important to recognize the stakeholders in the risk assessment and its results in the assessment planning efforts. The stakeholders can include:

- Plant/facility owner/operator.
- Employees and contractors at the site.
- Shareholders.
- Government agencies – Local, State, Regional, National, International.
- Media.
- Outside groups such as environmentalists, intervenors, etc.

Each one of these stakeholders may have a different interest in the results of the risk assessment – even if the results are not intended for public consumption. The assessment plans must take this into account.

4.4 Collect Artifacts, Templates, Preliminary Documentation

As the assessment team is being built, this is the time to implement a secure digital and hardcopy library of information and data for the team's examination and reference. Basically, any current information regarding the client, the client site, and other industry information that can be useful to the assessment team should be included in this library.

Information to include in the library includes:

- Past risk assessment reports.
- Current open source intelligence (OSINT) regarding the client, client's company, etc.
    - Annual Reports.
    - 10Q Financial Reports.
- Industry information that could be helpful for the risk assessment (e.g., reviewing outstanding security or safety events in the same industrial or critical infrastructure sector).
- Any drawings, technical information currently available for the client site to be examined.

A tool like Microsoft SharePoint may be helpful to ensure adequate cybersecurity is maintained on the documents, provision of access control lists, and allows for check-in/check-out of documents.

Remember, this information may be very helpful in developing the assessment plan and could be used as a reference in the assessment report later on. Thus, keeping an organized documentation scheme is to the team's and client's benefit.

By the way, this documentation library will be used throughout the assessment process. We will discuss the types of documents to be collected. Overall, be sure to track your documents and track their version.

4.5 Define the Assessment Plan

The assessment plan is a dynamic document. It is often changing based on such elements as:

- The purpose of the assessment.
- The assessment results recipients.
- Expected deliverables.
- Anticipated constraints.

The plan is useful for both the assessment team as well as the client. This will aid in communicating how the assessment will operate, including rules of engagement, whether or not cyber scans will be performed and their parameters, key points of contact, etc.

Admittedly, the level of effort detailed in the plan may be undefined until the first customer meeting is held. However, the assessment team does not require a great deal of detail in this planning document except for the rules of engagement. In fact, it may be a hinderance to the assessment team should the assessment plan include an excessive number of details. Too much detail may restrict the team from evaluating "low hanging fruit" and cause the team to spend time on less than target-worthy efforts.

The scope of the assessment can be impacted by the level of analysis required by the client and by corporate expectations. The scope can also be impacted by any physical barriers and constraints, logical system boundaries, etc. In this case, take site plan drawings and system drawings and draw "red lines" around the areas to be inspected/assessed and those which are off limits.

The most important part of planning an assessment is that the plan should not constrain the assessment team yet allows the team to approach a problem from any direction. The assessment plan should loosely define what to examine but not detail how to do the inspection or test. This allows the assessment team to use their skills and experience to accomplish the goals of the assessment. After all, by definition, a potential attacker is not going to follow any set rules of engagement.

4.6 Hold the Initial Team Meeting

Ideally, the initial assessment team meeting should be held one or two weeks before the assessment start date. The attendees of this meeting should include the entire assessment team if possible. However, at a minimum the team meeting should include the assessment team leader, the corporate manager overseeing the assessment process (e.g., Risk Manager), and internal stakeholders with an interest in the client site assessment.

The purpose of this meeting is to conduct a high-level review of the tasks outlined in the Assessment Plan and, if appropriate, Statement of Work (SOW).The meeting will also include reviews of any client-specific training or background investigations that need to be completed prior to the team arriving at the client's site.

The initial team meeting is also intended to assign roles and responsibilities to team members such as logistics coordinator, lunch coordinator, document management, etc.

Examples of information reviewed during the internal kick off meeting include:

- Project schedule (draft or final form) including confirmation of dates.
- Location(s) and address(es) of sites to be visited and assessed.
- Expected duration at each site (if applicable).
- On-site contacts such as:
    - Primary Point of Contact (PPOC).
    - Administrative Point of Contact (APOC).
    - Technical Point of Contact (TPOC).
- Start time and location for the first day onsite.

- Personal Protective Equipment (PPE) requirements.
- Identify nearby hotels, airports, transportation options, etc.
    - Determine if the hotel offers corporate rates available to the assessment team.
- Conduct a high-level review of the tasks outlined in the SOW and assessment plan.
- Answer questions regarding the SOW and assessment plan.
- Discuss the above defined elements – especially the assessment plan and goals.
- Discuss and plan any customer-specific training or background investigations that need to be completed prior to arriving onsite.
    - For example, some industrial sites require pre-training by all visitors to ensure they understand the appropriate alarms, safety systems, and safety practices, etc.
- Review assigned roles and responsibilities necessary to complete the assessment.
- Identify which team members will be responsible for:
    - Administrative coordination.
    - Documentation coordination.
    - Lunch/meals coordination.
    - Travel coordination.

The initial kick off documentation shall include the following:

- Meeting minutes.
- Completion of any project checklists.
- Identified revisions to the assessment plan.
- Etc.

4.7 Client Kick Off Call

This is the first formal meeting between the assessment team leadership and the client. Nominally this call is scheduled one to two weeks before the assessment start date but after the initial team meeting.

Attendees for this call should include – at a minimum – the assessment team leader and key client points of contact such as the plant or site manager.

The meeting can be performed via telephone, Skype, WebEx, Zoom, or even face-to-face if budget and time allow.

The client kick off meeting is intended to serve two purposes: 1) show the assessment team's understanding of the assessment scope and plan in terms of goals, deliverables, roles, schedules, resources, etc.; 2) to request specific information from the client related to their organization and business; and 3) identify and confirm assessment goals, objectives, schedules and anticipated challenges in preparation for the assessment activity.

Examples of information exchanged with the client during the kick-off meeting include:

- Assessment schedule (draft or final form) including confirmation of dates and times.
- Locations and addresses of sites to be visited.
- On-site contacts such as:
    - Primary Point of Contact (PPOC).
    - Administrative Point of Contact (APOC).
    - Technical Point of Contact (TPOC).
    - Others.
- Verify the start time and location for the first day.
- Identify any Personal Protective Equipment (PPE) requirements.
- Confirm the presence of onsite technical staff necessary to conduct interviews.
- Identify nearby airports, hotels, and ground transportation options.
    - Determine if the hotel offers a corporate rate.

- Review actions to be performed by the assessment team to include interviews, documentation reviews, inspections, observations of work, taking photographs, etc.
    - Regarding photographs, identify if any special permissions are required to take photos and obtain this permission before the assessment team arrives on site.
- The client should identify the types of information and level of detail desired in the final report. This information should include the desired level of formality of the report contents.
- Describe any particular rules of engagement – both for the assessment team and for the client. These rules essentially describe the constraints affecting the assessment teams' actions. These rules ensure the safety of all personnel involved during the assessment, the security of sensitive information used or generated during the assessment process, and the integrity of the production environment during the assessment.
    - One rule of engagement I have encouraged is that the assessment team will not touch or operate any equipment, systems, machines, etc. without the client's explicit permission and oversight.
    - Another rule of engagement highly recommended is that any serious safety or operational hazards observed by the assessment team will be immediately communicated to the client Primary Point of Contact and will not be delayed until the end of the assessment. This action is intended to ensure the safety of the plant, site personnel, and assessment team members.
- The assessment team manager should inform the client that the assessment team will require a considerable amount of information not only before the assessment team arrives on site, but also when they are at the facility. The data request is usually included as separate email or transmittal to the client

Types of Documents

When you are asking for documents from clients it is important to realize the difference between policies, standards, procedures, and guidelines.

There is a simple hierarchy associated with these four types of documents. They can be described as follows:

- ***Policy –*** *a formal, brief, high-level document that outlines management's beliefs, goals, expectations, and philosophy for a specific subject area. The policy does not offer specific details on how to implement the expectations but it should be followed without exception by site management and personnel (i.e., mandatory). Policies are further defined by standards, procedures, and guidelines.*
- ***Standard*** *– usually written to document how particular technologies are configured. They are mandatory and support the implementation of a policy.*
- ***Procedure*** *– a procedure supports a policy and is written to provide step-by-step instructions, precautions, and prerequisites for the performance of a particular task. The procedure normally is mandatory and often requires "verbatim compliance."*
- ***Guideline or Best Practice –*** *a guideline offers general statements, recommendations, administrative instructions, hints, suggested approaches, etc. to achieve a policy and/or procedure. A guideline does not require mandatory adherence but is primarily a suggestion.*

following the completion of the kick-off meeting. I will be going into more detail on the data requests in the next section.

The documentation maintained following this kick-off meeting includes:

- Meeting minutes including list of attendees (name, title, phone number, email address).
- Project checklists and updates.
- Copy of the kickoff meeting presentation.

4.8 Data Requests to Client

At any time prior to the assessment – but earlier the better – specific client data should be obtained thus allowing the assessment team to be better prepared for their visit. The information should be used to help the assessment team members make more precise plans for the site visit, areas to investigate, etc. The data will also reveal any areas potentially needing improvement.

For instance, shallow or inadequate policies and procedures may indicate an area needing improvement for the client and their organization.

The following information should be requested from the client *before* the assessment begins:

- List of site names and locations including mailing and physical addresses, phone numbers, latitude/longitude (if appropriate), web site URLs, LinkedIn and Facebook pages, other social networking coordinates, etc.
- Corporate and site organization charts.
- High-level plan views of the site, facilities, manufacturing plant lines, floor-by-floor plans for multi-story buildings, etc.
    - Include hardware floor plans.
- Lists of client-identified threats and vulnerabilities.
- Description of system architecture including cyber network diagrams.

    - Be sure both the enterprise network (e.g., email, databases, cloud interface, etc.) and the operational technology network (e.g., plant production controls, industrial control systems, etc.) are provided.
    - Include security zones as appropriate.
- Description of computer applications used on the enterprise and operational technology networks.
- Disaster planning and recovery plans.
- Security and risk-related policies, standards, procedures, and guidelines used by the facility personnel (e.g., employees, vendors, contractors, visitors, etc.)
- Copies of previous risk and security assessments performed at the site – intended to identify repetitive issues.
- Description of the physical plant and interface with critical infrastructure (e.g., rail spurs, highways, airports, telecommunications, internet, water services (potable and fire protection, natural gas, electricity, etc.)
- List of computer and industrial control systems and assets such as:
    - List of systems by criticality to production (e.g., High, Medium, or Low criticality).
    - Assets with device identification.
    - Host names.
    - Manufacturer and model numbers.
    - Internet Protocol (IP) address ranges (both internet-facing and for internal routing).
    - List of approved ports and services for all devices – if available.
    - List of approved firewall rule sets and Access Control Lists (ACLs).

4.9 Packing & Travel Planning

Assessment preparation includes team member actions involving packing, travel planning, etc. Normally it is each team member's individual responsibility to collect and bring the required equipment, forms, documentation, etc. to the client site for the assessment.

Types of equipment and materials to bring along to the assessment include the following:

- ☐ Two USB sticks, each greater than 8GB storage, verified and checked with anti-virus prior to arriving at the client site.
- ☐ A pocket flashlight and holster.
    - I recommend the flashlight have an LED bulb and can be turned on/off with one hand.
    - The holster is important to allow for safe and handy storage of the flashlight while climbing ladders, etc.
- Pen, pencil, and highlighter
    - Note: some facilities prohibit use of blue ink for official records. Be certain to check with the site Point of Contact to ensure the team understands any nuances associated with ink color.
- Notepad or 3"x5" notecards
    - A "Steno" pad is highly recommended to allow for easier handling when climbing ladders, etc.
    - An example of the nominal steno pad is included in the photo below:

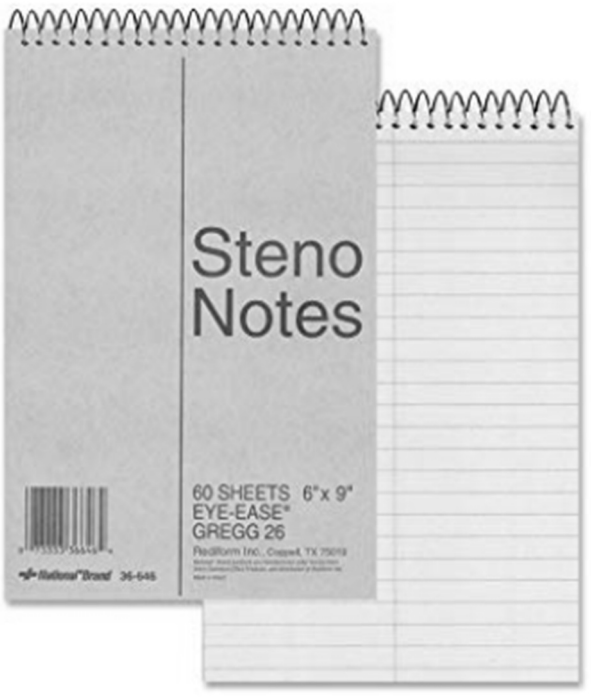


Figure 4-2 Steno Pad

- If you are wondering, I often carry the steno pad between my lower back and belt-line of my work trousers when climbing ladders or when I need to keep my hands free when in some potentially dangerous situations. Here is a photo this mode of carry:

Figure 4-3 Steno Pad Carry Technique

- Personal Protective Equipment (PPE) as required by the client and your company. This can include:
    - Hard hat
    - Steel-toed boots
    - Eye protection
    - Hearing protection
    - Nomex coveralls or shirts (fire retardant)
- Fire retardant or cotton clothing – no synthetic fibers.
    - Note: this is normally required for electric utilities and facilities where polyester clothing could be extremely hazardous if it caught on fire. Polyester melts onto the skin and causes more serious injury than natural fibers.
    - This is normally dictated by the client and your company safety policies.
- Laptop and power supply.
- Digital camera or Smart Phone Camera
    - First, use of a digital camera normally requires explicit approval by the client. In fact, some of my clients have required a written/issued Camera Permit on site.

    - I use the camera to take photos of particularly good demonstrations of facility performance and material condition/cleanliness or to document negative issues identified during the site visit.
    - My preferred camera is a small digital camera that is lightweight, has a zoom, and the memory card is readily available when you want to download the pictures. . A smart phone camera may be adequate; however, some clients do not want smart phones in play because they include location and GPS information in the photo metadata. Again, check with the client.
    - When you do select a camera, consider its weight, ease of use, and zoom. The zoom will allow you to get close up shots on specific equipment concerns such as leaks, etc. Also consider its functionality in low-light environments.
    - Lastly, a camera may not be permitted in some explosive environments.
- Digital camera batteries and charger.
    - Ensure you have spare batteries for your camera. I have a fairly simple process of sorting my camera batteries on their state-of-electric charge using a plastic business card sheet. Please see the photograph below:

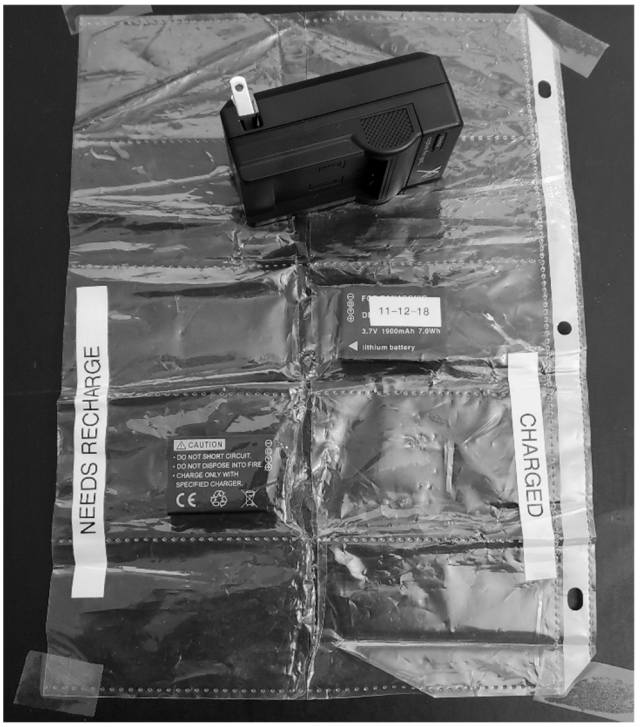


Figure 4-4 Camera Batteries, Charger - Battery Storage Sleeve

- GPS device for your car/rental car – Most now use Google Maps on their smartphones.
- Business cards.
- Software.
    - My favorite software to use for my field documentation includes:
        - SnagIT® – Sold by TechSmith (https://www.techsmith.com/screen-capture.html). $50 for a single seat license. SnagIT is an extremely useful tool for computer screen capture and image manipulation. I use it when inserting photos into my documentation as well as computer screen shots. Like it is said, a picture is worth a thousand words, and SnagIT is tool to help make a point to a client in the risk assessment documentation.
        - Microsoft Word/Word Processing.

    - Microsoft PowerPoint – especially useful for team and client meetings.
    - Photo Editor – Even the photo editor in the Microsoft and SnagIT products above is adequate.
    - Google Earth (https://earth.google.com/web/) or Google Maps (https://www.google.com/maps/) with Satellite View — I use Google Earth or other satellite view depictions to help conduct pre-assessment information gathering regarding the physical layout of a site, factory, etc. I find it especially helpful to gain a sense of the adjacent risks such as a railroad track, residential or business park, highway, etc. You can even use these views to compare your raw visual capture to the client drawings and plan views of their facilities.
- Download available information for any uncommon vendor equipment viewed on the customer equipment lists. This is useful for preparation before arriving on site in order to understand the features and functions of the equipment, any security requirements and default passwords, etc.
- Have access to either hard-copy or digital versions of any relevant standards that may apply to the risk assessment. For example, if you are doing a NERC CIP assessment of an electric utility, then be sure to have hard and soft copies of the NERC CIP standards from www.nerc.com.
- Clothing – consider the weather at the client site as well as the working environment in the client facility. This may dictate the types of clothing you pack.

4.10 Devising the Work Plan

As we are receiving the client documentation the team – and each team member – needs to develop the assessment plan. It is preferred the plan be a formal, written one; however, a simple outline is an option for urgent or rushed departure to the client site (e.g., post-accident or -event).

4.10.1 Example Site Risk Assessment Visit Plan

The following is an example format for a site risk assessment visit plan. It is based on an actual site visit but with the particulars changed to anonymize the client. Regardless, this is strictly a guide but your company risk assessment manual may provide added details on the contents for the plan form and format.

Beginning of Proposed Memorandum/Plan/Report

1. **Introduction**

   The XXX risk assessment team will be on site at the QRS facility to _____(explain)_____. The purpose of this letter/report is to summarize the plan to be used and followed during the course of the on-site risk assessment.

2. **Personnel**

   The risk assessment team personnel who will be on site for the risk assessment are:

   - Team Lead: (Name, Title, Job, Email, Phone)
   - Specialty X: (Name, Title, Job, Email, Phone)
   - Specialty Y: (Name, Title, Job, Email, Phone)

   The XXX risk assessment team personnel will be accompanied by authorized personnel from QRS site throughout the duration of the risk assessment.

   QRS personnel expected to provide escort and support include:

   - Name, Title, Job, Email, Phone
   - Etc.

3. **Objectives**

   The site work activities are intended to support/validate _____(complete this information)_____. After these site activities are complete, the risk level will be assigned to each identified finding or gap thus helping to produce the risk-based remediation plan at the end of the risk assessment.

   The objectives specific to this site assessment are:

   - (Objective 1)
   - (Objective 2)
   - (Objective 3)
   - Etc.

4. **Assessment Methodology**

   In order to successfully achieve the objectives of the site risk assessment, the following must normally be reviewed, examined and inspected (Here the plan contains a checklist of the actions to be performed during the risk assessment):

   - Site material condition.
   - Asset management and classification.
   - Logical and physical access control.
   - Cyber and physical security awareness and training.
   - Information protection.
   - Configuration change management.
   - Cyber and physical security incident response planning.
   - _____.
   - _____.

   The onsite assessment activities will include:

   - Conducting Entry and Exit meetings.

- Interviewing site personnel, vendors, contractors.
- Reviewing client documentation.
- Conducting a physical plant inspection.
- Performing observations documenting reviews performed.

The ultimate product of this effort is the Risk Assessment Report.

5. Approach to the Risk Assessment

Optimally a flow chart will be included here showing the work flow for the XXX site risk assessment.

One example could include the following:

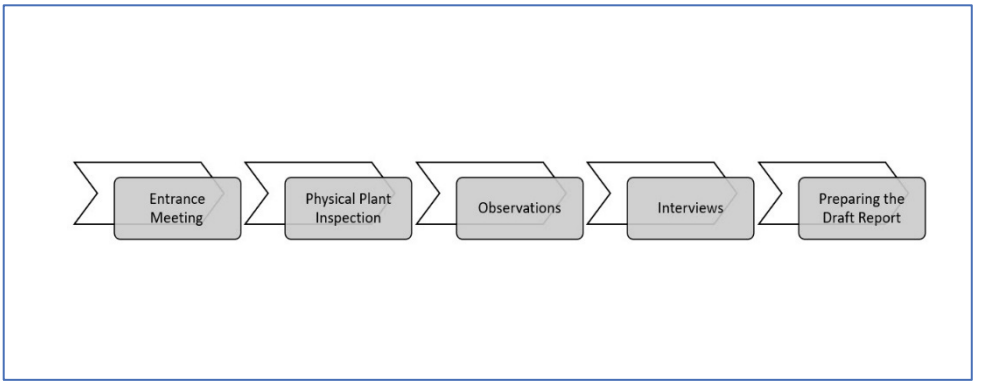


Figure 4-5 Example Approach to XXX Risk Assessment

A second example could include the following type of flow chart:

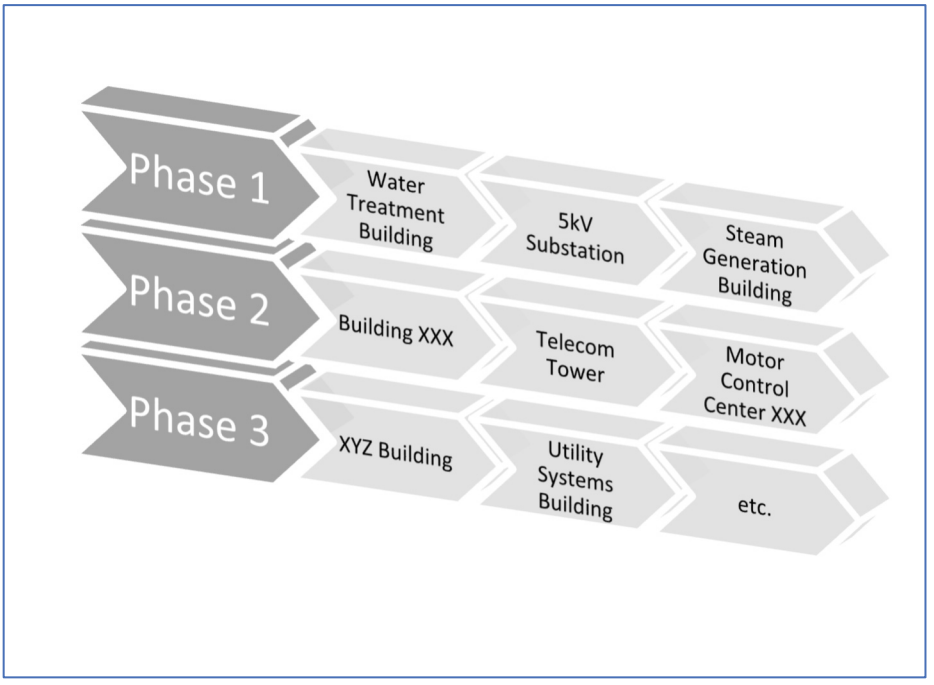


Figure 4-6 A Building-Specific Risk Assessment Flow Chart Example

6. Schedule Overview for the XXX Risk Assessment

The table below provides a tentative schedule overview to facilitate preparation and planning for the risk assessment. This can be used to show scheduled items with firm dates and times, place holders, and open items awaiting schedule. Color coding is probably the easiest way to depict the status of the individual time activities.

Date	Mon, 1st	Tue, 2nd	Wed, 3rd
7:00 AM	Site Orientation	Review of Metrics	Open as Required
8:00 AM	Site Orientation	Review of XXX Documentation	Open as Required
9:00 AM	Entry Meeting	Tour QRS Buildings	Open as Required

Date	Mon, 1st	Tue, 2nd	Wed, 3rd
10:00 AM	Tour of Plant	Tour QRS Buildings	Open as Required
11:00 AM	Tour of Plant	Tour QRS Buildings	Open as Required
12:00 PM	Lunch	Lunch	Lunch
1:00 PM	Admin Building	Interview: Maintenance	Exit Briefing
2:00 PM	Admin Building	Interview: Maintenance	Exit Briefing
3:00 PM	Interview: Physical Security	Inspect Warehouse	Depart for Airport
4:00 PM	Interview Physical Security	Interview: Health & Safety	Offsite
5:00 PM	End of Day	End of Day	Offsite

7. Systems/Subsystems to be Inspected

Based on the statement of work, the following systems are in scope for this risk assessment; however, it is important to understand that due to time and geography, not all of these systems/subsystems/components will be observed or inspected. The focus will be on those systems or assets considered critical or of high important for maintaining availability and integrity of the plant/facility.

7.1 Systems

- Identify systems as appropriate such as distributed control systems, third-party systems, cyber systems, physical access control systems, etc.
- _____
- _____

8. Out of Scope Activities

In this section of the assessment plan, those actions that are specifically out-of-scope for the assessment team members are delineated. For instance, active or passive cyber scanning of selected network components may not be in scope for the risk assessment. Hence, such a prohibition should be listed here.

Additionally, XXX risk assessment team members will not be operating or touching any equipment; however, verification of workstation operating systems, patch levels, etc. may be performed by authorized client personnel at the risk team member's request if approved by the site management.

Again, this section is intended to itemize those activities that are explicitly out of scope for the assessment team and consistent with the scope of work and associated contracts, etc.

End of Example Assessment Plan

4.10.2 Preparing Your Steno Pad

The Steno Pad is my go-to resource for the site activities. It is portable and a ready notepad for my lists of observations, perceptions, etc. as well as a way to capture my questions for future interviews and follow-up activities.

Before I depart for the site assessment, I prepare the Steno Pad with a copy of my business card pasted on the outside cover and reference materials pasted inside of the notebook.

For instance, in the early sections of the Steno Pad I will normally include the following general information:

- Copy of team member contact information (usually a matrix).
- Site/client contact information (again, a matrix).
- Top critical controls in place at the client site (i.e., “critical infrastructure and systems”).
    - I use this as a reminder to ensure I review and inspect all of the critical systems and components.
- Plant network/system topology and plan layouts.
- List of areas of focus based on the Statement of Work and the Assessment Plan. An example list of areas of focus from one of my previous risk assessments is in the table below:

Table 4-1 Example Risk Assessment Areas of Focus

Areas of Focus (Example)
1. Password Management – Storage, Change, Shared, Default, Complexity
2. Network Management – Open IP Ports, USB Ports, Segmentation
3. User Management – Auto Expire Accounts, Employee Exit Strategy, Employee Roles
4. Software Management – Patches, Authorized Installers, Automatic Software Updates
5. Vulnerability Management
6. Remote Access – VPN, No Access to Enterprise

4.10.3 Pre-Checking Control System Assets for Vulnerabilities

The risk assessment may include reviewing selected control system assets for security vulnerabilities. Although there may be cyber and physical vulnerability assessments and scans performed on site after the risk assessment begins, there is merit to cross check on any known control system vulnerabilities at the United States Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) web site[59].

At the CISA web site there are lists of Alerts and Advisories identifying vulnerabilities for multiple control systems and components. You can find these lists at: https://www.us-cert.gov/ics

The suggested preparation before departing for a risk assessment is to take the list of identified control systems submitted by the client. Then, using this list, check the CISA Alerts and Advisories to determine if the components and systems in question and installed at the site have any known vulnerabilities to be checked onsite.

For instance, assume the client has installed Schneider Electric Modicon M340 Programmable Logic Controller (PLC) Station P34 Modules in their control system. This is a supervisory control and data acquisition/programmable logic controller (SCADA/PLC) interface product used in factory and utility control systems. According to multiple reports, the vulnerabilities consist of both remote and local weaknesses and affect the modules supporting an important communications protocol – the Factory Cast Modbus feature. The US Department of Homeland Security CISA/Industrial Control Systems (ICS) Computer Emergency Response Center (ICS-CERT) released the follow-up advisory titled ICSA-15-246-02 Schneider Electric Modicon PLC Vulnerabilities on September 3, 2015, on the ICS-CERT web site.[60]

[59] https://www.us-cert.gov/

[60] ICSA-15-246-02 Schneider Electric Modicon PLC Vulnerabilities, https://ics-cert.us-cert.gov/advisories/ICSA-15-246-02 , web site last accessed September 3, 2015.

As one of the risk assessment team members, you should use this preparatory knowledge to do onsite checks to identify if the client has patched or mitigated the vulnerabilities for applicable client-owned controls as identified by the ICS-CERT using the information and mitigation guidance in ICS Alert (ICS-ALERT-15-224-02), Schneider Electric Modicon M340 PLC Station P34 Module Vulnerabilities, which includes the following from the Alert:

Critical Building Controls and Cyber Security.

I was performing a risk assessment of a large public arena. During the course of my assessment I checked on the status of the current building controls system. Of note, the building controls system manages the building heating, ventilation, and air conditioning; building lighting; etc.

During the examination of the building controls I verified the software brand and software version installed. Then, using this information I cross compared the software configuration with the CISA ICS-CERT Alerts and Advisories at https://www.us-cert.gov/ics.

This review revealed that the current building controls installation was at least two versions behind the current and more secure version. Also, the CISA ICS-CERT site advisories included recommended mitigations to ensure the building controls were quickly brought up to date.

With this knowledge, subsequent interviews with the client led to recognition that the software was not being properly updated by the vendor and that the client was not verifying their building controls were secured based on freely available CISA ICS-CERT alerts and advisories.

- *ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:*
    - *Minimize network exposure for all control system devices and/or systems and ensure that they are not accessible from the Internet.*
    - *Locate control system networks and devices behind firewalls and isolate them from the business network.*
- *When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.*
- *ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.*
- *ICS-CERT also provides a recommended practices section for control systems on the ICS-CERT web site (http://ics-cert.us-cert.gov). Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*

Overall, such analysis before arriving on site is important to both the assessment team members and to the client. This action will ensure the assessment team is familiar with the types of devices installed at the site (assuming the client has provided an accurate list). Also, this will prepare the assessment team on the vulnerabilities to look for and to ascertain what mitigating activities should have been performed by the client.

4.11 Excited to Start the Assessment

With all this pre-assessment preparation, you should be ready to depart for the site and have your questions and follow-up lists prepared and documented. Your Steno Pad should be labeled and ready for field use, and your knowledge of the site and client is on the verge of being "expert." Now we are ready to head to the airport and begin the heavy lifting known as the risk assessment.

Bon Voyage!

REFERENCES

Franklin, B. (1750). By failing to prepare, you are... Retrieved December 19, 2019, from https://www.brainyquote.com/quotes/benjamin_franklin_138217

Guel, M. D. (2007). *A Short Primer for Developing Security Policies*. Retrieved January 16, 2020, from https://pdfs.semanticscholar.org/231b/c2ca1c556cb7b46bc46dd49e86f0e6ab8050.pdf

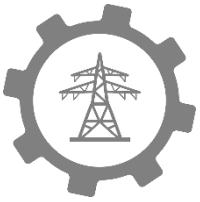
Miller, T. (2013). How to Build an Effective Threat Assessment Team | 2013-02-01 | Security Magazine. Retrieved December 19, 2019, from https://www.securitymagazine.com/articles/83982-how-to-build-an-effective-threat-assessment-team

Mulla, C. (2019). Guidance on Threat Assessment Teams. Retrieved December 19, 2019, from https://www.asisonline.org/security-management-magazine/articles/2019/01/guidance-on-threat-assessment-teams/

Port of Long Beach. (2014). *Risk Assessment Manual*. Long Beach. Retrieved from https://thehelm.polb.com/download/430/2019-applications/8538/risk-assessment-manual.pdf

Rovins, J. E. (Jane E. ., Wilson, T. M. (Thomas M., Hayes, J. (Joshua), Jensen, S. J. (Steven J., Dohaney, J. (Jacqueline), Mitchell, J., … GNS Science (N.Z.). (n.d.). *Risk assessment handbook.*

US Department of Homeland Security, & CPNI - Centre for Protection of National Infrastructure (UK). (2010). *DHS / CPNI - Cyber Security Assessments of Industrial Control Systems Good Practice Guide | WaterISAC*. Retrieved from https://www.waterisac.org/portal/library/2001dhs-cpni-cyber-security-assessments-industrial-control-systems-good-practice



Chapter 5
The Power of the Observation

"To acquire knowledge, one must study; but to acquire wisdom, one must observe."

– *Marilyn vos Savant*

or

"What is important is not what you hear said, it's what you observe."

– *Michael Connelly, Trunk Music*

Before we move forward into the discussions regarding the actual on-site work, I want to take time to provide a chapter entirely focused on the "observation." The observation is very key for the risk assessment process and, as such, I want to provide some detailed review of this important anchor point.

In this chapter you will discover:

- An overview of the concept of an "observation."
- The primary elements included in the observation as well as its format.
- Fundamental considerations when performing and documenting the observation including the power of one's influence on the actions being observed, the need for critical thinking, and considerations on how the observation supports the risk assessment.

Where are we in the overall process? We are focused on ***"Site Assessment – Observations"*** as depicted in the graphic below from Chapter 3.

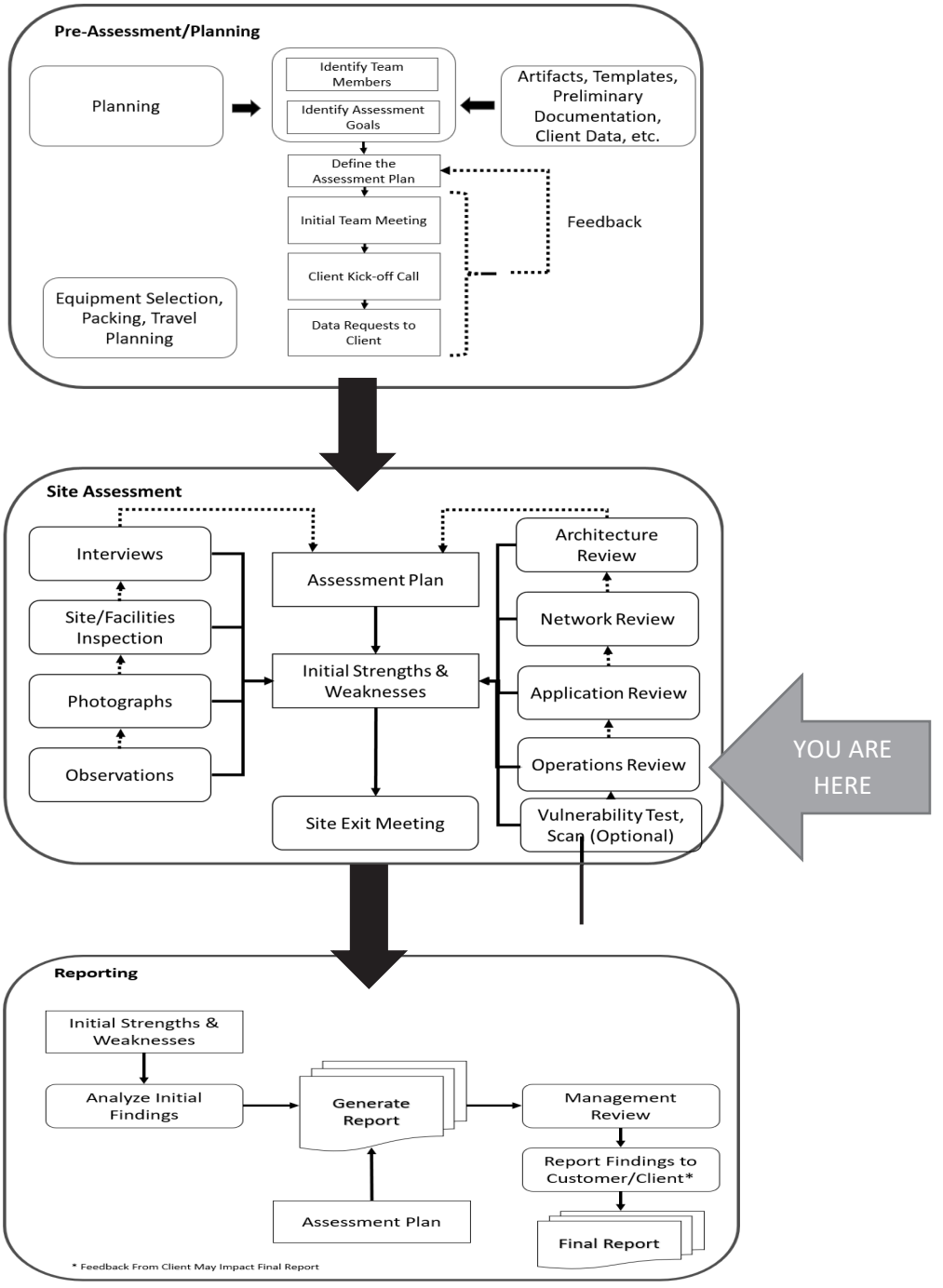


Figure 5-1 Hybrid Facility Risk Analysis Flow Chart

5.1 An Introduction to the History of Observations

From 1986 to 1993 I worked at the Institute of Nuclear Power Operations, also known as INPO. Overall, it was an excellent experience where I traveled to over 40 nuclear power plants in the US, South Korea, and Taiwan performing both risk assessments and supporting assistance visits to the nuclear plant and corporate management. My roles at INPO ranged from being a Maintenance Evaluator to Engineering Evaluator and ultimately qualifying as a risk assessment Team Manager. I departed INPO in 1993 to return to the commercial nuclear industry after serving as the Secretary of the Corporation and Assistant to the President.

INPO's mission is to promote the highest levels of safety and reliability – to promote excellence – in the operation of commercial nuclear power plants. INPO was formed in response to the nuclear accident at Three Mile Island which occurred in 1979. Key activities performed by INPO include:

- establishing performance objectives, criteria, and guidelines for the nuclear power industry,
- conducting regular detailed evaluations of nuclear power plants, and
- providing assistance to help nuclear power plants continually improve their performance

INPO's formation and early risk assessments were primarily influenced by the successful practices and procedures developed in the United States Nuclear Navy. In fact, the first CEO of INPO was former Vice Admiral Dennis Wilkinson, USN, who was also the first commanding officer of the world's first nuclear powered submarine – the USS Nautilus. Of course, Admiral Wilkinson and his initial supporting management team of former Navy nuclear officers brought to bear some ideas on how to assess nuclear safety risk.

One concept the Navy nuclear program used was the use of Operational Reactor Safeguard Examinations – known as ORSE Boards. An ORSE Board is an examination conducted by United States Navy personnel on board US Navy nuclear-powered ships. The purpose of an ORSE is to ensure that the Engineering (submarines) or Reactor (aircraft carriers) department of a nuclear-powered vessel are operating their reactors in a safe manner. The exam also ensures the readiness of the engineering department to safely respond to nuclear power plant casualties and unusual events. Of

note, I've had the opportunity to witness and be involved in ORSE exams as a nuclear officer on the USS Texas CGN-39 and USS South Carolina CGN-37.

The ORSE board is made up of three Junior Board Members, usually prior Engineers, and a Senior Board Member (a prior Commanding Officer).

An ORSE is scheduled during an underway period. There are a few surprise ORSEs when the boat or ship is given only a few days of notice. The first task of an ORSE board is to review all of the ship's records from the date of the most recent ORSE. After the review, a battery of intense simulation drills will begin. Additionally, oral interviews test the department's level of knowledge. Additionally, there are monitored evaluations to address the department's ability to perform selected maintenance items. A typical ORSE lasts for 3 days.

A fundamental aspect of the ORSE Board is the collection of information in the form of narratives that summarized "observations" and findings raised when reviewing logs, conducting interviews, and observing the performance of the ship's crew during simulated drills and when performing maintenance.

Another driving influence for INPO and its approach to performing nuclear power plant risk assessments is from the Office of Naval Reactors.

Naval Reactors or NRO is an umbrella term for the U.S. government office that has comprehensive responsibility for safe and reliable operation of the United States Navy's nuclear propulsion program. A single entity, it has authority and reporting responsibilities within both the United States Department of the Navy (Chief of Naval Operations and the Naval Sea Systems Command, NAVSEA), and the United States Department of Energy (National Nuclear Security Administration).

Many books and articles have been written about core NRO management principles such as attention to detail and adherence to rigidly-defined standards and specifications, as well as the organization's unique personnel practices. NR staff and alumni (including Admiral Rickover himself) have often been called by Congress, the President and other government agencies to provide expert opinion and management support to other important government programs, most notably the large-scale reviews following the destruction of the Space Shuttles Columbia and Challenger. NRO alumni have also joined numerous corporate and industrial organizations founded by three of Admiral Rickover's leading technical managers in NRO's early

Admiral Rickover (1900-1986) was a giant in the US Navy and commercial nuclear industry. As an Admiral in the US Navy, Rickover began and directed the original development of naval nuclear propulsion. He controlled their operations for over 30 years as director of Naval Reactors. He even served as an officer for 63 years – longer than any other naval officer in US history.

I had the chance to meet Admiral Rickover twice – first in 1974 when I was interviewed for selection as a Navy Nuclear Officer. The second time was in 1978 when Rickover joined us on USS Texas (CGN-39) for our initial underway cruise after new construction. I will agree he was rather eccentric during both meetings.

Overall, Rickover possessed an aura of power and had no patience with excuses or weak leadership. He attacked Naval bureaucracy, ignored red tape, lacerated those he considered stupid, bullied subordinates, and assailed the country's educational system. (Finney, 1986)

days. Similarly, some NRO alumni worked at and/or influenced the risk assessment work of INPO.

The ORSE Boards, the Office of Naval Reactors, and the former Navy Admirals, Captains, and nuclear officers working at INPO, provided some strong influence on the development of nuclear safety risk assessments that I ultimately learned to perform when working at INPO. From my time at INPO, and learning about the power of "the observation," I have used this assessment concept and methodology in many of my professional and personal approaches to complex projects and gathering and organizing data for presentation to a customer or stakeholder.

I have used the observation concept during many of my consulting engagements. For example, at one utility I wrote an observation for every substation, building, and water facility I inspected. Also, I wrote observations for every park and associated facilities for a city parks department requesting a risk and security assessment.

In each case I used the same approach and format when writing my observations. These same observations and associated photos were then used as major contributors to my final reports.

5.2 Just What is an "Observation?"

Think of an observation as a formalized way to collect information and facts as you review documents, watch personnel do work, inspect physical plants and facilities, survey a warehouse of spare parts, and scrutinize the operation of an office or even a company. The observation is a formalized way to bring your facts into one place for later examination and compilation with other observations.

Consider an observation as a formalized "notepad." Use the observation format to collect your facts, figures, notes, acknowledgement of strengths and weaknesses.

To give you a sense of the central importance of observations, above is a simple graphic showing how observations contribute to the risk assessment report development:

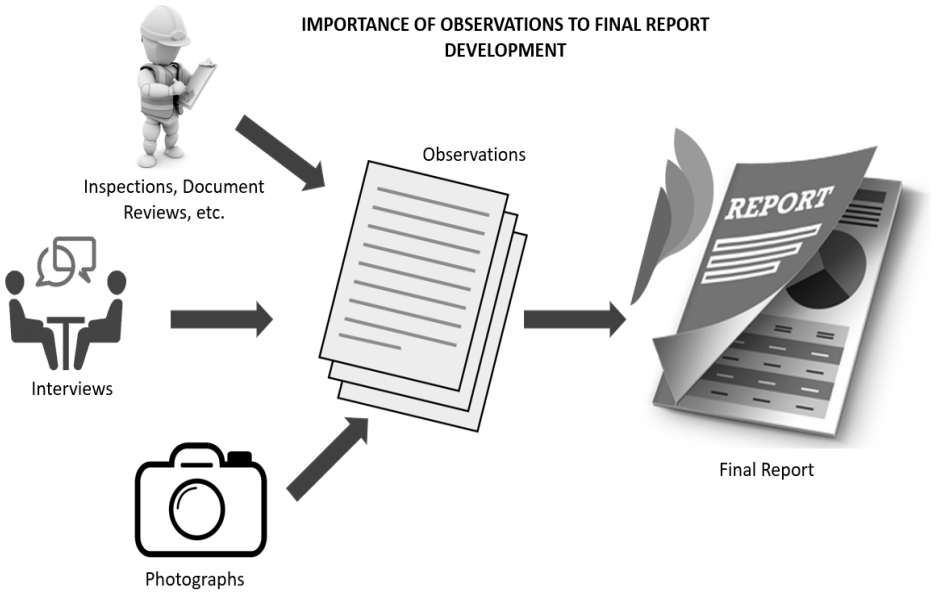


Figure 5-2 Contribution of Observations to the Final Report

Always remember why you are performing the observation: to contribute to the risk assessment.

5.3 Observation Format

Although there are no specific rules per se for documenting an observation, the following key sections are normally included in the writeup:

- **Title of the Observation** – Simple description of the subject of the observation (e.g., Review of Maintenance Procedures, Inspection of XXX Building, Observing Repair of the QRS Pump, etc.)
- **Document Author, Number, Date, and Version** – This format aids in tracking the observation for editing, follow-up questions, etc. One approach to this is a simple format to be included in the observation header or footer and file name:

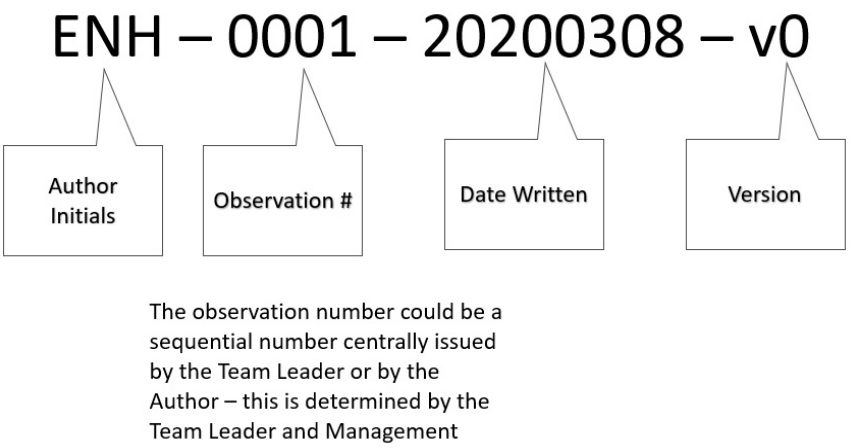


Figure 5-3 Observation Document Labeling/Numbering

- **Scope** – The scope paragraph is intended to give the reader a summary of the "who-what-where-when-how" perspectives of the observation. For instance, the scope for a document review essentially discusses what documents were reviewed and where the review was performed. For observations of field work the scope paragraph will highlight the titles or type of people observed, what work they were performing, when the observation occurred, and how it was performed.

  Consider the Scope paragraph a way to describe the scene of the work observed, documents reviewed, facilities inspected, etc.

Strengths Observed – When you are in the field making observations or reading documents you will inevitably see good practices, good ideas in play, or strengths. Be sure to identify these in the observation notes in order to give the reader a sense that "…not everything is broken…" and to reinforce good practices. I usually include these paragraphs early in the observation before I begin with the negative comments.

A strength could also be an attribute or practice that is beneficial to other organizations doing the same or similar work. You'll hear more about Strengths and Good Practices in the chapter where we talk about the final report development.

- **Observation Notes** – This is the core of the observation document. Guidance for observation notes includes the following:
    - Each paragraph is numbered sequentially. Supporting sub-paragraphs can be numbered (preferred) or use "bullets."
    - Each paragraph details what was observed, viewed, or witnessed by the risk assessor. The paragraph must include a statement of *fact* and a summary clause answering the question *"So What?"* Opinions should be avoided but the reader needs to understand the problem viewed and why it is important to the operation/safety of their plant, personnel, etc.
    - The problem paragraph is followed by a recommended action to correct the observed deficiency or problem. This recommended action can include both a tactical response to fixing the observed problem as well as a more strategic view to solve the problem and its symptoms over the long term. This could include training, updating a policy/procedure, reinforcement by supervisors, etc.
    - The third element of each observation is a reference or citation to a document, website, video, etc. that includes some options to solve the observed problem.
    - Be sure to insert photos into the observation if available to aid the reader's understanding of the problem observed.

  A simple example observation paragraph is included below:

3. Access to the fire sprinkler riser is blocked in one of the storerooms. A photo of this situation is included below:

Figure 21 Sprinkler Riser is Blocked in a Storeroom

a. **Recommendation:** Clear the areas around sprinkler riser of at least 30 inches. Consider marking the floor near the panels to show the "clear zones." **Reference:** State Code XXXYYY, Paragraph ###, requires at least 30-inch clearance.

Figure 5-4 Example Observation Paragraph

- **Observations Can be Chronological or by Category** – When I write my observations, sometimes I include my comments in a chronological order, that is, in the order of when I made the observation. This provides a time sequence for the items or problems raised.

  Alternatively, I may include my observations by category of strength or problem. For instance, when I am doing a facility inspection, I may include my observations under different categories. I will categorize my observations using sub-headers to collect similar problems such as Industrial Safety, Signage Issues, Documentation Problems, etc. This makes it easier for the reader to see the depth and breadth of a particular problem in their plant.

- **Summary Outline of Observation –** Here is a summary outline of what I include in an observation document.

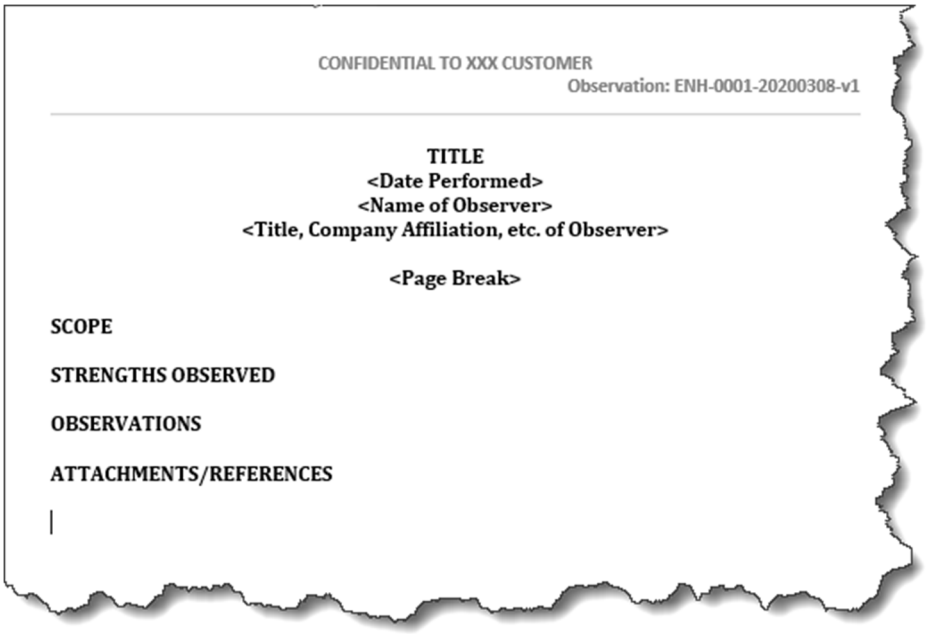


Figure 5-5 Observation Example Format

5.4 Critical Thinking

Some of the best risk assessors I have worked with are also the best observers. They are also the best critical thinkers. According to the Foundation for Critical Thinking, this concept is defined as:

> *Critical thinking is the intellectually disciplined process of actively and skillfully conceptualizing, applying, analyzing, synthesizing, and/or evaluating information gathered from, or generated by, observation, experience, reflection, reasoning, or communication, as a guide to belief and action. In its exemplary form, it is based on universal intellectual values that transcend subject matter divisions: clarity, accuracy, precision, consistency, relevance, sound evidence, good reasons, depth, breadth, and fairness.*

The key critical thinking skills are: analysis, interpretation, inference, explanation, open-mindedness, and problem-solving. (Zety.com) All of these characteristics – albeit not "natural" – are helpful when performing an observation.

As a team leader, you may want to take time to ensure your team members are being groomed and trained as "critical thinkers." Which leads us to asking "Why."

5.4.1 Asking "Why?"

An effective observer is someone who understands what they are watching or reviewing technically but is capable of effectively seeing weaknesses, problems, strengths, and opportunities for improvement. The effective observer can watch an event and look for the subtleties of the activities or documents and ask "Why" frequently.

> *The 5 Whys method is part of the Toyota Production System. Developed by Sakichi Toyoda, a Japanese inventor and industrialist, the technique became an integral part of the Lean philosophy.*
>
> *"The basis of Toyota's scientific approach is to ask why five times whenever we find a problem … By repeating why five times, the nature of the problem as well as its solution becomes clear."*
>
> *- Taiichi Ohno (kanbanize.com)*

Regarding the "Why" question, there are numerous examples in modern industry where asking "Why" multiple times is an imperative to improving organizational performance. For instance, in the LEAN approach to manufacturing quality improvement – also known as the "Toyota Way" – asking "why" at least five times is included in their process.

In my own work, I often found the approach to the "Why" question another tool in my kit to better understand what I am observing. For instance, some

answers to the Why questions are obvious and do not require multiple interrogatories; however, sometimes, if you want to understand the real reason why a worker performs as they do, the multiple "why" questions are very helpful.

This applies to interviews with field workers as well as executive management.

After asking the "Why" questions, be sure to consider the second- and third-order consequences of the problem observed. Consider how the problem may evolve over the longer term across the company. An example would be taking a response from executive management and contemplating what would happen to the company if the answers were not followed through or, even worse, they were dishonest. These answers may result in problems to the company, its reputation, the local community, and its national/international reputation.

5.4.2 Communicating Your Observations

Of course, an effective observer is a solid technical writer and can succinctly communicate what they observe and the problems they identify. This takes practice – it took me a solid year of writing observations before I was considered "competent" by my colleagues at INPO.

Ensure your sentence and paragraph structure are clear and concise. Use proper technical writing techniques and format. Avoid using abbreviations unless you've written them out on first use. Also, as a general rule, numbers are written out for zero to nine and are written as numbers for 10 and above.

5.4.3 Raising Issues

As an observer you must be objective and raise difficult issues with the intention of improving performance of the client and its personnel. It can be difficult to raise bad news or critiques of personnel performance; however, it is important to do this to bring the issues to the attention of the client management.

As a general practice, though, avoid using the names of the individuals being observed. Instead use their titles (e.g., welder, craftsman, technician, manager, etc.). This prevents "targeting" the person being observed and still gives management a sense of the general tone of the problems observed.

5.5 Unintended Influence of the Observation on Performance of Work

When performing an observation of personnel, your actions of watching someone perform work could influence their decisions and quality of their production. That happens all the time. It is simple psychology.

For example, when I am being followed by a police car, my adherence to rules of the road and speed laws is precise and perfect!

The impact on the person being observed is often referred to as the "observer effect." In the social sciences there is the concept of the Hawthorne effect.

A story related to me when I was in the US Navy Nuclear Navy was about Admiral Rickover's "20 Minute Rule." Rickover was smart enough to realize that most people can generally be perfect in their performance for the first 20 minutes of the observation; however, after that time the workers would return to their normal work habits and pay attention to the task at hand rather than that a Naval Reactors inspector was watching their every move. Because of this, it is best to ensure your observation duration is longer than 20 minutes. My experience has usually been to perform the observation for around 45 minutes to an hour in order to gather adequate facts about the work being performed and task at hand.

You are probably asking, how you can minimize your impact as an observer. One technique we used at INPO was to take time at the beginning of a work observation to introduce yourself to the workers, explain the reason for your presence, and allow the workers to ask questions regarding your observation chore. Explain you will be taking notes.

Afterwards, when the observation ends, be sure to thank the workers for their time and the chance to observe their work. Feel free to show your notes to the workers if requested. This adds to the trust level for the risk assessment.

When you complete the observation, take time to move to a quiet place and review your notes. Identify any gaps or follow-up questions you will need to be sure the observation is complete and factual and you answer the "So What" questions.

5.6 Writing the Observation

The best time to write the observation is within 12 hours of the event. I often write my observations later in the day or the evening of the work inspected. This allows me to take my cryptic notes and convert them into coherent sentences effectively. If you wait until the next day you could forget the details of the work being reviewed.

The observation must answer the primary question of "So What?" If your paragraphs cannot satisfy this perspective, either rewrite the statement or eliminate the observation bullet.

On a practical side, I use Microsoft Word for my observation composition. I often use a template and fill in each section as I review my notes. If I am doing a document review, I simply start writing in the observation template as I identify issues with the procedures, etc. I am reading.

As you are writing the observation, and as questions arise on the missing details, be sure to identify these for follow-up the next day.

The observation is a very sensitive document and should not be casually disposed. Instead, shred the document. Newspapers would love to get their hands on this fodder!

5.7 The Power of the Observation

The observation is really a formalize notepad for the risk assessor. It ensures your notes are captured in an organized manner and allows for future editing, update, etc. If you are working as an assessment team, be sure to have a centralized review of all the observations as they are being written to identify repetitive and common issues that would be especially beneficial to the client to aid in their performance improvement program.

So, you are now aware of the observation process and how they are developed and written. The observation process is a key aspect of field risk assessments which we will discuss in the next chapter.

REFERENCES

Cherry, Kendra, (2018). The Hawthorne Effect and Behavioral Studies," VeryWell Mind. Retrieved from https://www.verywellmind.com/what-is-the-hawthorne-effect-2795234#:~:text=The%20Hawthorne%20effect%20is%20a,are%20participants%20in%20an%20experiment.&text=The%20Hawthorne%20effect%20has%20been,to%20industrial%20and%20organizational%20psychology

Finney, J. (1986). Rickover, Father of Nuclear Navy, Dies at 86. *New York Times*. Retrieved from https://www.nytimes.com/1986/07/09/obituaries/rickover-father-of-nuclear-navy-dies-at-86.html

Goodreads. (2020). Observation Quotes (427 quotes). Retrieved February 27, 2020, from https://www.goodreads.com/quotes/tag/observation

Hayden, E., & Alvarado, J. (2017). *Evaluation Methodology*.

Institute of Nuclear Power Operations. (2020). INPO - Institute of Nuclear Power Operations. Retrieved February 27, 2020, from http://www.inpo.info/

Kanbanize. (2020). 5 Whys: The Ultimate Root Cause Analysis Tool. Retrieved March 9, 2020, from https://kanbanize.com/lean-management/improvement/5-whys-analysis-tool/

Mullen, T. (2018). Human performance: Take note of error precursors. Retrieved from https://www.crisis-response.com/comment/blogpost.php?post=401

Nazar, M., Igyarto, D., & Pollock, J. (2017). *Efficiency Bulletin: 17-05 Simplified and Enhanced Management Observation Techniques*. Retrieved from https://www.nei.org/CorporateSite/media/filefolder/resources/delivering-nuclear-promise/2017/eb-17-05-simplified-and-enhanced-management-observation-techniques.pdf

Oakley, G. (2020). *Telephone Interview*.

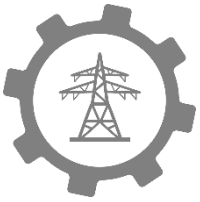
Scriven, M., & Paul, R. (2019). Defining Critical Thinking. Retrieved March 5, 2020, from https://www.criticalthinking.org/pages/defining-critical-thinking/766

Smithers, J. (2020). Effective Safety Inspection Program Based on Training, Observation, Interaction - Workplace Material Handling & Safety. Retrieved February 24, 2020, from http://www.workplacepub.com/material-handling/safety/effective-safety-inspection-program-based-on-training-observation-interaction/

Tomaszewski, M. (2020). Critical Thinking Skills: Definition, Examples & How to Improve. Retrieved March 5, 2020, from https://zety.com/blog/critical-thinking-skills

Willard, R. (2019). *Testimony for the Record An excerpt from the Convention on Nuclear Safety Report: The Role of the Institute of Nuclear Power Operations in Supporting the United States Commercial Nuclear Power Industry' s Focus on Nuclear Safety*.

Zarvana. (2020). Critical Thinking Process: 4 Questions that Improve Any Idea | Zarvana. Retrieved March 9, 2020, from https://www.zarvana.com/critical-thinking-process-4-questions-that-improve-any-idea/



Chapter 6
On Site

There are no secrets to success. It is the result of preparation, hard work, and learning from failure.

- *Colin Powell*

Or

Every time you step out on that field, it's tough. There is no easy way to approach it and no short cuts out there.

- *Sonny Bill Williams*

Now that we've spent time on preparing for the assessment and the importance of the foundational observation concept, we will focus on actual on-site work. The majority of the risk assessment is performed on site.

In this chapter you will discover:

- All the expected activities performed during a site risk assessment.
- An understanding of how the observations developed during these activities are written and developed to aid the team in understanding strengths and weaknesses as well as ultimately write the final report.
- The nuances involved when conducting interviews, performing facility inspections, etc.

Where are we in the overall process? We are focused on ***"Site Assessment"*** as depicted in the graphic below from Chapter 3:

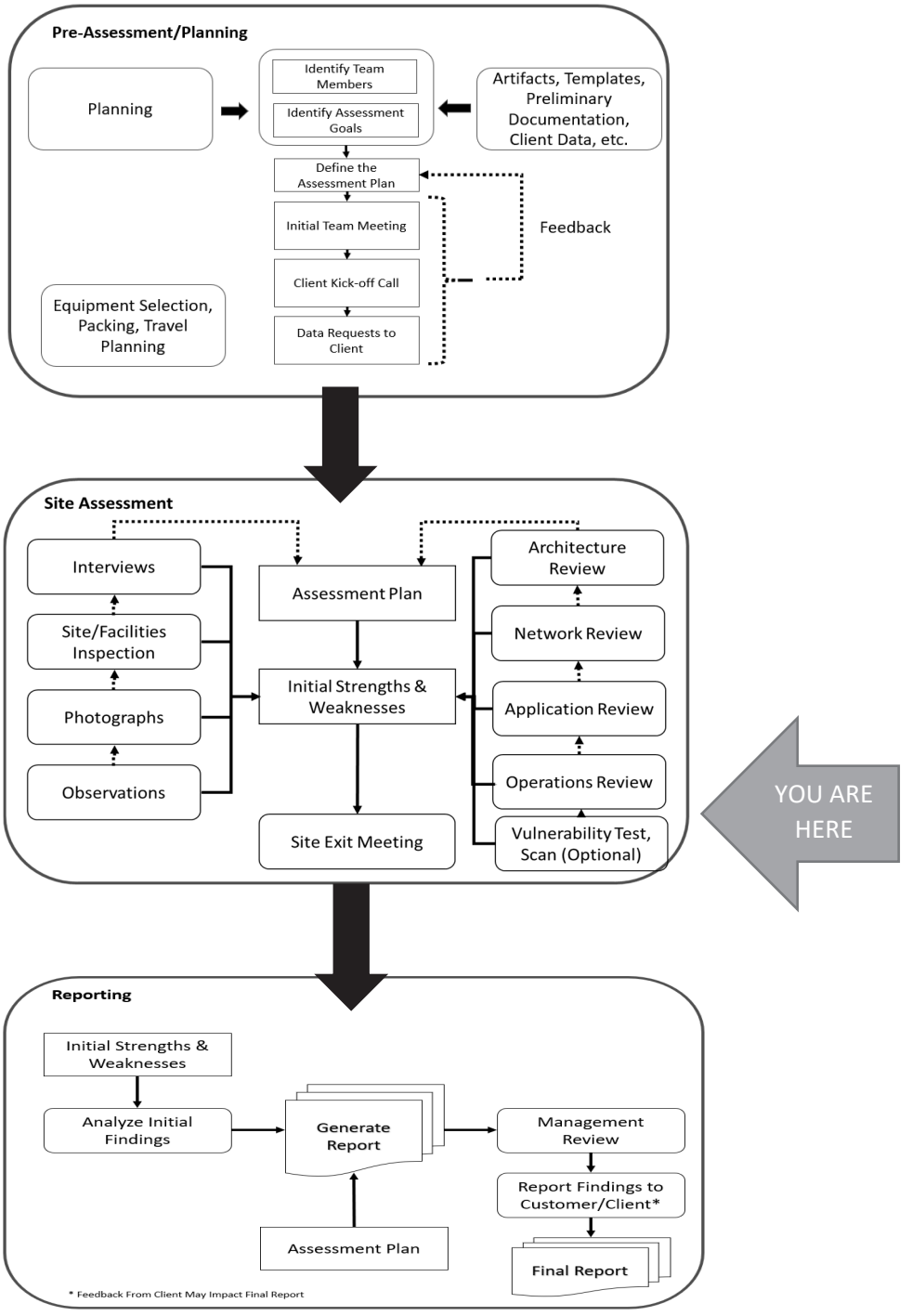


Figure 6-1 Hybrid Facility Risk Analysis Flow Chart

6.1 On Site Arrival – Entrance Meeting

Welcome to the client site! Your first action upon arrival is to conduct the kickoff meeting with the participating site managers. You may need to get your badging and safety testing performed first; however, you want to get the site kickoff meeting done as soon as practical.

By the way, remember you begin the assessment the minute you drive up to the site.

The kickoff meeting is typically an in-person meeting held onsite with the local client project team. Depending upon the customer, sometimes executives from the assessment team's headquarters management may join the meeting by phone or videoconference. However, the onsite assessment team leader will drive the agenda and discussions as well as respond to the customer's questions and concerns.

The entrance meeting should include the following agenda items as a minimum:

- Introduction of the Assessment Team.
    - Name, title, phone number, and email address.
    - Hand out business cards.
- Introduction of the Client Team.
    - Identify the Client Lead Point-of-Contact.
    - Obtain name, title, phone number, and email address.
        - Pass around a sign-in sheet for this information.
    - Collect business cards if possible.
- Provide a brief review of the reason for the risk assessment, goals and objectives, and planned/proposed activities each day while on the client site.
- The Team Leader will review plans for interviews, note-taking, system/network scans (as appropriate), visual examinations, inspections, document reviews, system and facility walkdowns, photographs, etc.
- Review Daily Logistics.
    - Arrival and departure times on site.

    - Site access – escort requirements.
    - Sign-in/Sign-out processes.
    - Lunch arrangements.
    - Resources available for the team (meeting room; access to coffee, copying machine, Internet; etc.)
- Take time to discuss and offer an opinion of the state of documentation and data provided to the team by the client.
- Ensure time is spent discussing and reviewing:
    - Site plan views to orient the team to the plant/facility layout.
    - Information Technology network diagram.
    - Control system network diagram.
    - Any particular assets and systems critical to facility operation.
- Close with an opportunity to answer any client or team questions.

Post-Meeting Documentation

- Meeting minutes.
- Completed sign-in sheet used at the meeting.
- Business cards collected.
- List of any open action items.

6.2 Example Site Schedule and Activities

The onsite schedule for the assessment team is predicated upon the Assessment Plan and Statement of Work (if contractually provided). The duration of time on site and access to key systems and equipment will also affect the site schedule.

Most of my risk assessments tend to run five working days. Below is a chart showing an example five-day evaluation process:

Table 6-1 Example 5-Day Assessment Process

Day 1	• Arrival at Site • Entrance Meeting • Tour of site with emphasis on safety, facilities, workspace, access controls, lunch options, etc. • Commence risk assessment as soon as you arrive on site • Take notes and photographs, write Observations throughout the day
Day 2	• Network architecture reviews • Physical site inspection • Systems/Equipment walkdown and viewing • Establish familiarity with control rooms (if applicable) • End-of-Day Team Meeting o Review Observations, positive impressions, concerns • Take notes/photographs, write Observations throughout the day
Day 3	• Interviews • Inspections • Follow-up on earlier reviews • End-of-Day Team Meeting o Review Observations, positive impressions, concerns

	• Take notes/photographs, write Observations throughout the day

Day 4	• Continue with interviews, inspections, documentation and system reviews, etc.
	• Close out any open issues
	• Team Meeting
	  o Review summary of Observations collected to date
	  o Review positives and concerns to be debriefed with the client management on Day 5
	• Take notes/photographs, write Observations throughout the day.

Day 5	• Open issues close-out • Take notes/photographs, write Observations throughout the day. • Hold Exit meeting with the Client • Departure – Return home

This schedule is very busy and requires a daily plan-of-attack to review all the necessary facilities, assets, systems, etc. and conduct all the required staff/contractor/vendor interviews.

You also need to stay organized and keep your Observations up-to-date and processed through the Team Manager or designee.

6.3 Conducting Interviews

Why do we perform interviews? We have these structured conversations in order to obtain information from client personnel – including customer vendors, contractors, etc. – regarding facility operations, risk management, and security. Becoming an effective interviewer takes practice. Therefore, don't expect to be a premier interviewer immediately.

An excellent website regarding key fundamentals for being an effective interviewer is a ***General Guidelines for Conducting Research Interviews*** (https://managementhelp.org/businessresearch/interviews.htm).This webpage offers guidance on interviewing your subjects.

Some key considerations for interviewing include:

1. Do not use a tape recorder or any other recording device. You will need to take notes instead.
2. Allow the interviewee to view your notes if they ask.
3. Try to ask "open-ended" questions (that is, questions requiring longer, detailed answers rather than "yes," or "no"). Open-ended questions allow for unlimited response from the interviewee in their own words and usually provide a more accurate response.
4. Ensure your questions are not "leading" or could give the interviewee a sense of the answer you are expecting or desire. These may negatively impact the interviewee's memory of the event.
5. Only ask one question at a time.
6. Don't be afraid to ask the "Why" question. We talked about this in the previous chapter. But to reiterate, the Toyota LEAN approach requires multiple (5 to 7) "Why" questions be asked to fully understand the cause of an issue.
7. Be careful about your appearance and body language when note taking. For instance, if you immediately jump at something the interviewee said, this could influence answers to future questions. If possible, calmly write the interview response then raise the follow-up question later on in the interview.
8. Avoid having two or more people conduct the interview. If you do, only allow one assessor to ask questions at a time. I try to orient the interview where I will ask three to five questions first, followed by the second assessor asking queries. Peppering the interviewee with questions can be very intimidating and may not result in satisfactory information.
9. Keep in mind these interviews are not for legal investigations; however, they are to help the risk assessment team and ultimately the client better understand any weaknesses or vulnerabilities that need to be addressed by management.

The opening procedures for the interview should include identifying the interviewer and interviewee. Explain the interview topic and establish rapport.

Don't forget that you want to obtain truthful information. Therefore, the interviewer must recognize the feelings, emotions, and body language of the interviewee. Treat the interviewee with sensitivity.

6.4 Photographs

Like the cliché observes, "A picture is worth a thousand words." Photographs are a very useful tool when performing and documenting your observations. However, there are a few considerations for the risk assessor when taking photos.

The first action by the risk assessment team is to obtain permission from the plant manager or other senior leader to take photos. Some sites will prohibit photography. At one site I was working, the site manager permitted photos but required me to use the site camera which did not have any geographic location tagging capability. It was also known to be intrinsically safe (i.e., it would not be dangerous in an explosive environment).

If you do get site permission to take photographs, you may want to obtain the authorization in writing should you be stopped by a guard or other employee.

When I take photos, I avoid using my cell phone and instead use a compact camera with SD memory card. The camera has no GPS tagging and I can remove the SD card each evening to file the photos by date and by area observed.

These photos may be very sensitive so sending them over insecure email or downloading via public Wifi can be problematic.

Overall, photos can be a substantially positive addition to your observations.

6.5 Site Facility Inspections

Conducting facility and system inspections requires some initial training and subsequent practice. Over the years, it was not uncommon to hear managers order their junior engineers to "…inspect the plant…" or "…walk down the xyz system…" Yet, the junior engineers are not trained on what to precisely look for, why they need to perform such inspections, and how to document their findings.

Material condition inspections are frequently performed at every industrial facility. The inspection can be formal or informal and performed by outside agencies, managers, supervisors, operators, or craftsmen. These inspections and how well they are performed are usually reflected in the overall condition of the plant. Therefore, by walking down the plant, you need to maintain your critical thinking and focus on looking for hazards and problems and maintaining an attitude of attention-to-detail. Otherwise, you will normally not find the threats to plant availability –except for the obvious 5-gallon per minute leak and the 8-foot steam plume. Therefore, one of the first and foremost requirements for a thorough material condition inspection is to ensure that the inspector has a "questioning attitude" and is looking for problems down to the smallest detail.

What is a material condition inspection? Basically, a material condition inspection is a focused, critical, and careful examination of an industrial component, system, or structure. This can include a factory, an aircraft, a multi-story business building, or a refinery. The intent of the inspection is to locate and identify threats to plant availability and problems such as leaks, lubrication problems, missing handwheels, clogged filters, broken gauges, loose fasteners, housekeeping deficiencies, and missing lights. The

In the early 1990s I worked for the Electric Power Research Institute (EPRI) in a variety of roles ranging from nuclear maintenance consultant, to Member Relations Executive, to Executive Director – West Region and Canada. Overall, EPRI was a wonderful organization encouraging new ideas and ways to help our members – US and international electric utilities.

In 1994 I saw an opportunity to write a handbook on performing facility inspections. The document, ***How to Conduct Material Condition Inspections****, is no longer in print. Many of the ideas I included in this guide are captured in this section of the book and updated to reflect new techniques and technologies.*

inspections can be formally scheduled and performed or they can be spontaneously executed.

The key elements or features of a material condition inspection include the following:

- the “right” tools.
- a plan of attack.
- a method to record the deficiencies.
- a systematic technique, and
- the right attitude.

The value of frequent, quality material condition inspections will help ensure that small problems are identified before they expand into larger problems resulting in industrial safety hazards or costly facility shutdowns.

6.5.1 Tools of the Inspection Trade

Thorough performance of the inspection requires that the inspector has the right set of basic tools. These tools include:

- flashlight.
- rag (or similar wiping cloth/paper).
- pen knife.
- inspection mirror(s).
- personal protective clothing and equipment.
- method to record deficiencies, problems, and notes.

Specifics on these tools are detailed in the following sections.

- **Flashlight**

In Chapter 5 I discussed the type of flashlight assessment team members should use. The right flashlight used by the inspector can make a difference when performing the inspection. Basically, the optimal flashlight is one that can be turned on and off with a single hand (some flashlights require two-hand operation by rotating the head of the flashlight – very inconvenient!) and can be carried in a holster, hip or shirt pocket. The flashlight should have an LED bulb for high candle power and fresh batteries installed before beginning the tour.

- **Rag or Similar Wiping Material**

Occasionally during the inspection, it may be necessary to wipe off dirt, grease, oil, or water in order to read a name plate or label, or to generally get a closer view of the component in question. Therefore, a cloth rag or heavy-duty paper wipe is very helpful and can be easily carried in a pocket.

> **Caution**
>
> *Do not use a rag or wipe in a radiologically, chemically, or biologically hazardous environment. In these cases, it is best to not touch the component or puddle to prevent personal injury or spread of contamination.*

- **Pen Knife**

A pen knife or small metal "scratch and poke" tool (e.g., dental tool) is helpful during inspections. This tool should be small enough to carry in a pocket yet sturdy enough to examine scale or rust build up and scratch through caked-up dirt. Again, similar to the caution above for rags, do not use your knife to rub or scratch in a radiologically, chemically, or biologically hazardous environment.

Caution

Do not use a conductive knife or mirror around energized electrical equipment.

- **Inspection Mirrors**

Occasionally, and based on where the inspection will be performed and whether or not ready access to 360° views of the component is available, a small, pocket-sized inspection mirror – similar to those used by dentists – may be handy. This tool may be most appropriate when examining valve stems, valve packing, items immediately against a wall or barrier, etc.

I and some of my colleagues have used their smart phone cameras to perform some of the duties listed for an inspection mirror. The smart phone cameras can zoom in on the area of concern and even record the deficiency with a photo.

As mentioned earlier, be sure use of the smart phone or any camera is permitted by plant management and plant safety officers.

- **Personal Protective Clothing**

When you prepare for your inspection, prepare to get dirty and to be "in the plant." Therefore, equipment such as a hard hat, safety glasses and hearing protection are appropriate. Also, a set of coveralls is very useful because of the cleanliness factor (or lack thereof) as well as the number of available pockets for the inspection tools listed and identified above.

6.5.2 Inspection Data Collection

The purpose of the inspection, of course, is to identify and record the problems in the plant for repair and follow-up investigation. There are five predominant methods used to collect data which include:

- Voice recordings
- 3x5 cards (handwritten)
- Notepads/Steno pads
- Work orders
- Digital notepads.

All of these approaches can be augmented with photography as appropriate and authorized.

- **Hand-Held Voice Recording**

  A smart phone or a small hand-held, battery-operated voice recorder can be used during inspections. The inspector can make verbal notes regarding the deficiencies. Later, the recorded notes can be transcribed to written form via work order/work request forms or inspection reports.

  As a benefit, this technique allows the inspector to work faster and make more detailed observations rather than pausing to write down all details.

  Unfortunately, there are limitations. The recording needs to be transcribed which delays the transfer of deficiencies to the plant's work control system or into follow-up reports. Also, the inspector is not "prompted" to remember all pertinent details such as component identifier, location, etc. Therefore, the narrative may not be complete in order to specifically identify the deficiency location and parameters.

- **3x5 Card Technique (Low Tech!)**

  This technique involves the inspector carrying a collection of blank or preprinted 3x5 inch cards to conduct the inspection. The preprinted cards help prompt the inspector to ensure the appropriate details regarding the deficiency are collected, ensuring the deficiency will be correctly located and corrected when logged into the Work Control System.

  An example pre-printed card is included below:

<NAME OF FACILITY>

INSPECTION CARD

Name of Inspector:_____

Building Name: _____ Floor:_____
Room:_____

Elevation:_____

Location Details:_____

Component ID: _____

Name of Component:_____

Problem Area: Maint ❑ Ops ❑ Eng ❑ IT ❑ Chem ❑ Safety ❑ Security ❑ Other:_____

Description of Deficiency (Quantify!):
_____

_____
_

_____
_

Deficiency Tag/Other Tag #/Date:
_____ Over ❑

Figure 6-3 Pre-Printed Inspection Deficiency Card

General guidelines for using these cards include:

- Quantify the problem (e.g., 15 drops per minute leak, 7 of 10 bolts missing, etc.).
- Fill in the required data to ensure the deficiency can be readily identified.
- Don't skimp on information – more detail is better.

Pre-printed cards assure the inspector is prompted to document complete data on the deficiency observed. Also, the cards are easy to carry and use and can be sorted to categorize common problems. Of course, information can be easily transferred to work orders for later correction.

Unfortunately, the card approach still has some limitations. For instance, it may be difficult to release the cards from a radiologically or biologically hazardous area due to potential contamination. And, as I've frustrated my Team Leaders before, the cards need to be completed by hand and be legible in an environment not conducive to good penmanship.

- **Notepads/Steno pads**

Using simple notepads to collect information about the facility during the inspection is very easy, unstructured, and allows the inspector to write down their observations, include details on what they are seeing and based on what they expect the work orders to be requiring.

This tends to be my preferred approach and what I've used for the past 40 years of inspections. However, if I don't look at my notes soon after I've written them, my handwriting is difficult to read and "self-encrypts."

- **Work Order Technique**

Most facility maintenance programs use some sort of "work order" to capture issues and ultimately log and track the deficiencies in the work management system for the plant or facility. The work order format can range from a single paper form to a paper form with multiple copies using NCR paper. The more modern facilities use digital work orders completed on cell phones or digital pads – to be discussed later.

For this approach, the inspector literally brings a stack of blank work order forms out to the plant and fills out the forms as they identify each deficiency.

This is slow work and can result in more frustration due to dropped forms, dropped pens, etc.

- **Digital Pad/Tablet (iPad, etc.)**

The more high-tech approach is to use a smart phone or digital pad or tablet such as an iPad or Android tablet to collect information on facility deficiencies and issues. The more modern maintenance programs include

the work order forms on the digital pads and allow the inspector to complete the necessary fields, add photographs, and even add voice notes.

This is the most preferred approach since the work order is completed in real time; however, there are always issues with poor cellular/WIFI coverage, dropped devices resulting in breakage, exposure to water, etc.

Also, the digital pads may not be allowed in some facilities because they are not intrinsically safe in explosive atmospheres.

6.5.3 Tour Planning

Have you ever taken time to think about how you approach a very large facility to perform an inspection or assessment? What if it covers multiple acres and tens of buildings? You need to consider a variety of variables before you grab your flashlight and begin looking.

In my years of watching how others perform inspections, I found there are four approaches to consider. They are:

- "Random" inspection.
- Focused area, system, or room/building inspection.
- Material condition feature inspection (i.e., just look at bolting, electrical boxes and their fasteners, signage, etc.).
- Inventory and validation of currently identified deficiencies.

Regardless of the type of inspection you will be performing, consider doing the following planning before you head out:

- Review any drawings or documents appropriate to the areas to be inspected including plant layout drawings, piping and instrument drawings (P&IDs).
- If possible, review any inspection reports prepared by the client.
- Verify you have both security and safety access to the areas and have the appropriate permits, approvals, keys, key-card access, etc.
- Check that all necessary tools, pens, paper, forms, etc. are available and ready.
- As appropriate, inform the site control room or main security office of your inspection and planned route.

- Be sure to provide area inspection assignments to assessment team members as practical.

Now you can begin.

- **Random Approach**

  This inspection approach, also known as inspection by "walking around," is performed in the manner denoted. In other words, the inspector conducts the inspection with minimal pre-planning. The inspection is conducted at the whim of the inspector with no predetermined focus on buildings, components, systems, types of problems, anticipated hazards, etc. The inspector primarily enters the plant with pen in hand and begins to itemize the deficiencies. This approach does result in identified deficiencies; however, the inspector may not be using their time effectively due to the random approach into the plant. Also, this approach would tend to result in inspection to those areas of easy access, hence, the harder-to-view and less-trafficked locations would be missed.

  In general, this approach is not recommended.

- **Focused-Area Inspection**

  The focused area inspection is a commonly used approach in the military. This technique is often referred to as a "zone inspection." At an industrial facility, this approach would include assigning the inspector to a room, area of the plant, or specific building for the inspection. For an office building the inspector may only look at selected floors or non-public areas.

  A prerequisite to performing this inspection technique is to divide the facility into a collection of "inspection zones." These zones could be specific rooms, separate elevations of larger buildings (e.g., basement of the office building), or specific areas of the outside yard between the building and the perimeter fence line.

  The zones should be small enough to accommodate a thorough inspection in about two to four hours; however, they should not be so small such that the facility is segmented into an excessive number of zones. If there are too many zones, then a comprehensive inspection is difficult to complete.

  Once these zones are defined, inspections are then performed in the separate zones on a rotating basis. Therefore, the entire facility is

inspected on a periodic basis assuming the inspections of the zones are performed at a defined interval (e.g., weekly basis).

- **Focused Material Condition Element**

Consider an industry event caused by the failure of a particular component or part. I can remember events in the industry caused by failures of air-operated valves, cameras, or even production line devices such as variable speed motors. If these events have happened at other plants and *could* happen at yours, this type of inspection may be of interest to you and your management.

For this inspection you first study what the other industry events were and understand their pre-failure symptoms, resulting incidents, size and scope of the consequences of the component failure, etc. Then, using this knowledge, develop a checklist for your component inspections in the facility. Using the checklist, review your facility only focused on the possibly failed component/system/device.

This focused-inspection approach is especially useful for safety inspections (e.g., fire extinguishers, lighting, etc.), chemical control,

Nitrogen Line Ruptures at Factory

In 2019 a liquid nitrogen line ruptured at an aircraft manufacturing facility in the US Midwest. The accident resulted in 15 injuries to plant workers and a substantial gas release to the environment. (KSN News 2020)

As a plant manager, this information can be useful to direct a Focused Material Condition Inspection at your plant to inspect and walk down all liquid nitrogen and other liquid gas lines at your plant.

Of course, as more information is released from the event at the aircraft factory, this can be especially useful for more detailed inspections at your own plant.

electrical connections, ground straps, labeling, and housekeeping/fire loading.

Overall, this approach uses industry events and experience to help protect your facility.

- **Inventory and Validation of Currently Identified Deficiencies**

This final inspection approach is useful to validate those deficiencies included in your work control database to actual deficiencies in the field. This inspection relies on digital or paper lists of active deficiencies, their associated deficiency tag numbers, and location coordinates. Using this information, the inspector can check to see if these deficiencies are valid, no longer exist, or are trending worse than originally identified.

6.5.4 "Working a Room"

No, this is not a method to consider at a cocktail party! Instead there are generic techniques to be used when conducting any inspection or assessment. To reiterate, you *always need to have a questioning attitude!* You need to continually look for hazards, deficiencies, problems, etc. and those issues that could be improved upon.

So, how do I approach a room when doing an inspection? Here are some ideas:

- **Surveying the Area**

Whenever you approach an area to be inspected, the natural tendency is to inspect the well-traveled paths and to inspect those areas at eye-level. Unfortunately, the normal pathways tend to remain relatively deficiency-free due to frequent traffic by the workers and other reasons. Therefore, the inspector needs to make it a point to look in areas that are not normally observed, and inspect those areas that are considered limited access, or out-of-the-way.

One approach to working an area or room is to conduct a perimeter tour. Walk around the room or zone by remaining close to the outside wall of the room. This path leads the inspector to viewing areas behind equipment, panels, etc. Also, most pathways through a room are in the center, hence, you can focus your inspection on areas infrequently viewed. That is where I often find problems.

THINK OUTSIDE OF THE BOX

Think in three dimensions when conducting your inspections. Terrorist attacks have occurred where attackers have entered underground facilities of a power station through manholes.

(Tibbs, 2014)

*In my article **Unseen Threat**, I emphasis that the inspector needs to look at all telltale signs and artifacts – many of which are prominently placed – that could tell an attacker where a softer and more vulnerable service feeding the plant is located. For example, site and facility architects use underground vault covers that explicitly label the service. That practice can be helpful for maintenance and emergency response, but it also provides an easy target for criminals.*

Other considerations to include in your inspection are to look up, look down, look behind, and look under. Again, a systematic inspection approach I've used here is to perform a top down "spiral" inspection. In other words, begin at the top of the room and inspect the room in a downward spiral. Hence, you will have inspected almost the entire room. It is a natural tendency to not look up during an inspection, therefore this technique guides the inspector to view the less observed areas.

- **Working a Large Facility**

When I begin a risk assessment of a large facility – such as a refinery, oil sands operation, large factory – my first approach is to walk or drive along the outside perimeter fence. Since this is the first line of defense, I want to look for any weaknesses or vulnerabilities where an attacker can get over, under, or through the fence line.

After examining the perimeter, I then try to begin my review at the starting point of the site processes such as supply input areas and then walk the processes and systems through the production process to the shipping point. As I do these reviews, I am looking for physical and cyber weaknesses in a manner similar to how I work a room.

Additionally, as I look at the processes and systems, I also check for any redundancy in the production lines and evaluate for any single-points-of-failure. Once I find a single-point-of-failure, I spend substantial time reviewing the components and systems for weak links in access control, material condition, etc. to get a sense of how close to failure each single-point-of-failure is.

Take advantage of Google Earth to view a facility, its fence line, and even street level. This will give you a sense during planning of the building security vulnerabilities and strengths but can be used to apply notes and callouts following your inspection.

- **Don't Operate/Don't Touch Rule**

As a general rule for the inspection, it is best if the inspector avoids operating equipment, opening panels, and handling components or equipment. This is especially critical in order to avoid spurious alarms or equipment activation or shutdown caused by cabinet door closures, or other "shocks." If the inspector is interested in looking inside cabinets and enclosures, the inspector should first get permission from facility management.

- **Attention to Detail**

Although this may seem repetitive, the secret to a successful inspection is to maintain a questioning attitude and focus on the details. Photographs are excellent ways to document what you see – especially today's digital files allow for zooming in on a questionable item.

Performing inspections takes practice. Use these tools and ideas to help improve your approach to looking at your plants/facilities.

6.6 Technical Reviews

The performance of technical reviews is predicated on the scope of work and the client expectations. It is also dependent upon the team members and their respective areas of expertise.

For instance, for some risk assessments I've performed with a team, we may have experts in operations, physical security, cyber security, network architecture, industrial controls, work control, etc. However, for some risk assessments I've only had one other team member who tended to be more of a "generalist" when it comes to risk assessments and threat and vulnerability identification.

Regardless of your team makeup, the technical reviews at the facility are dictated by the amount of time available and access to facility systems and critical components.

- **Network and Network Architecture Reviews**

  Network and network architecture reviews require more time evaluating network diagrams and data flows than field work.

  Over the years of focus on industrial control systems, I've developed a checklist to aid in these network and architecture reviews. The checklist is included in the table below:

Table 6-2 Industrial Controls Systems Security Architecture Checklist

	ARCHITECTURE / DESIGN STANDARDS
	1. Design standard for ICS architecture?
	2. Philosophies for identification/authorization, access control mechanisms, network topologies, system configuration and integrity mechanisms.
	3. Evolution of network design? Why? How?
	NETWORK SEGMENTATION AND SEGREGATION
	1. Is the ICS network separated from the corporate network?
	2. VLANs used?
	3. Encrypted VPNs used? Type of encryption (IPsec, SSL, SSH)?

	4. Physical network separation?
	5. Data diodes used?
	6. Network layer filtering that restricts which systems are able to communicate with others in the network based on IP and route info?
	7. State-based filtering that restricts which systems are able to communicate with others on the network based on their intended function or current state of operation?
	8. Port and protocol filtering that restricts the number and type of services that each system can use to communicate with others on the network?
	9. Application filtering that filters the content of communications between systems at the application layer (e.g., application-layer firewalls, proxies, content-based filters)?
	10. Themes: a. Apply technologies at more than just the network layer – each system and network should be segmented and segregated where possible from the DataLink layer up to and including the Application Layer. b. Use the principles of least privilege and need-to-know. c. Separate information and infrastructure based on security requirements. d. Implement whitelisting vs. blacklisting.
	BOUNDARY PROTECTION (Includes: gateways, routers, firewalls, guards, network-based malicious code analysis, encrypted tunnels, managed interfaces, mail gateways, data diodes, etc.)

	1. How do you decide what domains are permitted direct communication?
	2. What are the policies used governing permitted communication?
	3. Criteria used to select devices used to enforce the policies?
	4. What is the Trust Relationship between domains?
	5. Where are your DMZs?
	6. Communications rules: Deny-by-Default? Allow-by-Default? Deny All/Permit by Exception?
	7. Proxy servers/devices used? Where? Why?
	8. How prevent unauthorized exfiltration of data? (e.g., Deep-packet inspection firewalls, XML gateways, DLP devices….)
	9. Concealing network addresses of ICS components from discovery (e.g., network access not published or entered in domain name systems – requiring prior knowledge for access.
	10. How configure boundary devices to fail? Why?
	11. Feedback to senders (disable feedback to senders when there is a failure in protocol validation format… prevents adversaries from obtaining information)
	12. Firewall Rules Used? a. How to block traffic? b. Source/destination filtering? MAC addresses? TCP/UDP port filtering? ICMP type and code filtering? c. Handling:

	i. DNS (Control Network Devices – DNS, DHCP in the IT network and not in the ICS network) ii. HTTP (Port 80) iii. FTP, TFTP iv. Telnet v. SMTP vi. SNMP vii. DCOM viii. MODBUS/TCP ix. EtherNet/IP x. DNP3 xi. … d. How to enforce secure authentication in order to gain access to ICS network? (simple passwords? Complex passwords? Multi-factor? Tokens? Biometrics? Smart cards? etc.) e. How to log traffic? How log access requests/errors/etc.?
	13. Any issues with latency in control system communications?
	PHYSICAL SECURITY OF NETWORK
	1. Physical access controls enforcing limited authorized access to ICS components.
	2. Color coding / labeling schemes for network (aid in physical separation)
	3. Shielded or Unshielded cabling? Fiber-optic?
	4. RJ-45 Connectors – Industrial type?
	5. Access controls to cable runs?
	6. Emergency Power, Emergency Shut Off

	7. Emergency Lighting
	8. Fire Protection
	9. Temperature and Humidity Controls
	10. Water Damage Protection
	OTHER ISSUES
	1. Data Historians
	2. Remote Support Access
	3. Single Point of Failure
	4. Dial-up Modems
	5. Wireless LANs
	6. Anti-virus/Malware
	7. IDS/IPS (Network-based, Host-based)
	8. Patch Management
	9. Configuration Management/Change Management
	10. Backup Control Center
	11. System/Component Procurement
	12. Monitoring & Auditing

There are some excellent resources to help guide these reviews. They include the National Institute of Standards and Technology (NIST) ***Framework for Improving Critical Infrastructure Cybersecurity***, NIST ***Guide to Industrial Control Systems (ICS) Security,*** and the International Society of Automation (ISA)/International Electrotechnical Commission

(IEC) series of standards entitled ***Security for Industrial Automation and Control Systems*** (ISA/IEC-62443).

- **Maintenance and Operations Reviews**

  The maintenance and operation of the facility are very important to the risk profile of the facility. Inadequate maintenance or shoddy operations practices may result in system or equipment failures, injuries, or even death. Therefore, the risk assessment team will need to take time to understand and evaluate the maintenance and operations practices.

  Some categories to consider for these assessments and reviews are shown in the table below:

Table 6-3 Maintenance and Operations Categories for Assessment

Maintenance	Operations
Conduct and Performance of Maintenance	Conduct and Performance of Operations
Contractor Management and Control	Facility Status Controls
Facility Material Condition	Operations Administration
Maintenance Administration	Operations Organization and Staffing
Maintenance Facilities and Equipment	Operations Procedures and Documentation
Maintenance History	Operator Performance and Knowledge
Maintenance Organization and Staffing	Safety and Security Practices
Maintenance Personnel Performance and Knowledge	
Maintenance Procedures and Documentation	
Preventive and Predictive Maintenance	
Procurement and Spare Parts Management	
Safety and Security Practices	

Each topic above can be an opportunity for the assessor to dive in and get a sense of the risk management practices in the facility. But again, this demonstrates the necessity to have experts on your assessment team who understand the area being reviewed.

- **Technical Documentation Reviews**

Of course, effective operation of a complex facility relies on policies, standards, procedures, guidelines, etc. The assessment team will need to review many of these types of documents to better understand management's expectations for employee or contractor performance, and management oversight. The documents should be technically accurate, clear, easily understood, and consistently used so that operations, maintenance, design engineering, etc. is performed safely and consistently.

A checklist of key elements to be included in these documents is listed below:

Table 6-4 Key Aspects of Acceptable Technical Documentation

- Procedures and work guides are readily available and clearly marked as such.
- Procedure preparation, review, approval, and revision is properly controlled.
- Vendor documents used in lieu of procedures receive the same review and approval as procedures.
- Procedures and other work control documents – such as vendor manuals, drawings, reference materials, and posted job-performance aids – are reviewed for technical accuracy and are up-to-date.
- Setpoints, control logic, equipment numbers and identification are correct and consistently referenced in procedures, drawings, system descriptions, etc.
- Strong human-factor elements are incorporated into procedures to promote error-free performance.
- Quality assurance hold points are included in procedures – especially for job actions prone to error.

- Temporary changes to work documents and procedures are used provided they receive appropriate review and approval and the changes are incorporated into the permanent revisions on a timely basis.
- A formal program is established to ensure procedures are periodically reviewed (annually or biannually) for technical accuracy, human factors considerations and inclusion of lessons-learned from facility, corporate and industry operating experience.
- A mechanism is established to allow for ready feedback from the workers using the procedures and work documents. This feedback could include suggested ways to improve the performance of the work, error corrections, and even suggestions to improve document content or format.

- **Cyber Vulnerability Tests & Scans (Optional)**

For some facility risk assessments, the scope of work or client expectation is for a cyber vulnerability scan and test. The details for performing these tests and scans are beyond the scope of this book; however, I offer some high-level points for the risk assessment team manager and facility managers to consider.

Two terms you may often hear regarding these cyber tests are "Vulnerability Scans" and "Penetration Tests." A vulnerability scan is just that: it is a cyber methodology used to identify open ports and services and vulnerable applications requiring patches.

A "Penetration Test" is a vulnerability scan where the tester then tries to gain access into the owner's systems by taking advantage of the vulnerabilities identified. The penetration test attempts to duplicate the actions of an attacker (DHS/CPNI, 2010). Penetration tests are much more aggressive and can cause significant risk to the systems being tested. In most cases a penetration test is unnecessary; however, a cyber vulnerability scan is optimal.

What are the risks associated with a vulnerability scan or penetration test? If done properly and in coordination with the facility owner, the scans generally do not cause problems. Unfortunately, some testing done

on certain systems – especially industrial control systems – can result in system failure, tripping offline, and possibly damage to the facility. As a general rule of thumb, cyber scans of production systems should not be performed unless the production systems are shut down.

In ***Cyber Security Assessments of Industrial Control Systems***, jointly published by the US Department of Homeland Security and the UK Centre for the Protection of National Infrastructure, excellent guidance is provided to managers and practitioners on conducting such cyber assessments. This guide was issued in 2010 but still offers timeless advice on ways to perform cyber security testing – especially on industrial systems.

The overall process consists of three primary steps: Reconnaissance, Exploration, and Exploit Development.

Reconnaissance is the first step in the process. Here the tester actively scans potential targets on the network. The primary off the shelf tools used include port scanners (NMAP), vulnerability scanners (Nessus), and network monitoring software (Wireshark). The output of these scans can include lists of open cyber ports and cyber services and unpatched and vulnerable applications. This information by itself can be very helpful to understand the risk of successful penetration by an attacker. This information can also be used almost immediately by the client to take action to secure their network.

In Exploration, the cyber assessment team can use the data gathered above during the scans to either attack the vulnerable network processes identified, or, inform the client on actions they should take to eliminate or reduce the vulnerability. In a penetration test, the team will continue with both exploration and exploit phases.

Again, it is not recommended that penetration tests be performed to identify vulnerabilities requiring corrective action.

An excellent database of vulnerable components and systems normally used in industrial and commercial facilities is maintained and published by the US Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA). CISA publishes alerts and bulletins associated with current security issues, vulnerabilities, and exploits. Before beginning a risk assessment, it is helpful to understand the types of systems and components used by the client and compare these lists to current CISA alerts and bulletins. This was especially

helpful during one risk assessment where I discovered the client was using a particular brand of building management system. I cross checked the building software with the CISA alerts and bulletins and discovered the client's system was seriously vulnerable due to a missing upgrade. Such a vulnerability would probably not have been discovered by a NMAP or Nessus scan.

6.7 Daily Team Meetings

Open and effective communication between team members is important for the success of this risk assessment process. Daily team meetings are intended to help bring together team member perspectives of what they have seen and not seen. Team members are expected to write their observations every day/evening and begin to develop their views of strengths and weaknesses that may ultimately become good practices and findings.

Optimally the daily team meetings occur at the end of the workday. It is preferred that the team meetings occur at the client site in a conference or meeting room. The team leader facilitates the discussions and asks questions to help the members better understand the team's collective perspective of the threats, vulnerabilities, hazards, and strong areas of performance.

An example team meeting agenda may be structured as follows:

Table 6-5 Example Daily Risk Team Meeting

Agenda Item	Leader/Speaker
Open the Meeting – Announcements and team plans for tomorrow (e.g., lunch, client management meetings, etc.)	Team Leader
"Round the Table" – Each team member offers the following details of their day: o What They Did – Summary of who, what, where, when, how, why, if o Strengths Observed o Concerns Being Developed o Requests for Assistance from Other Team Members o Plans for Tomorrow o Observations Expected to be Submitted Today	All Team Members
Team Leader's Review of Observations and Summary of Trends Under Consideration	Team Leader
Questions/Concerns	All

Each day, the Team Leader should be meeting with the facility leader/manager to provide an overview of activities and thoughts surfacing from the team. These meetings should be very high-level and not provide any details on weaknesses until the final meeting on Friday (or as planned). Why is this the case? You need to be careful about providing details on weaknesses, problems, etc. too early to the management. The facility management could take this preliminary information and negatively affect future observations and risk assessment reviews. The facility management

may tell the staff of problems raised by the assessment team and thus negatively impact the reality of work and operations practices.

6.8 Development of Strengths & Weaknesses

As the risk assessment proceeds it will be obvious to the Team Leader and team members what strengths and weaknesses are evolving. On the day before the site exit meeting, the team should meet and develop a more formalized list of their strengths and weaknesses to be debriefed the next day.

Weaknesses are the beginnings of Findings in the final report. Strengths are the start of Good Practices in the final report. A weakness could be evidence of problems with documentation, work performance, human factors, lack of spare parts, etc. Strengths are those work practices, documentation, training or other performance characteristic helping the organization sustain a competitive edge in their market domain. The risk assessor may simply view a strength as a "good idea" that could be useful in the industry.

In reality most strengths become Good Practices and most weaknesses become Findings in the final report; however, it makes sense to only offer the site management the team's views of strengths and weaknesses since Good Practices and Findings are not "official" until approved by the Assessment Team's formal management and leadership.

Essentially, this provides some flexibility for the team so that as they move to develop the Good Practices and Findings there are opportunities to merge or delete the issues raised onsite.

6.9 Site Exit Meeting

The exit meeting is held on the last day of the onsite risk assessment. The meeting agenda is similar to the entrance meeting with some emphasis on Strengths and Weaknesses. Below is a checklist for the Team Leader to follow:

- Make introductions of the assessment team members.
    - Be sure to pass around an attendance signup sheet
- Thank everyone for their cooperation and participation in the assessment. For any particularly helpful support (e.g., the lunch coordinator, etc.) be sure to offer kudos and thanks by name.

- Perform a summary review of the actions taken onsite during the assessment period in order to "paint a picture" of the assessment and risk assessment activities.
- Remind everyone the Strengths and Weaknesses being discussed during the Wrap Up Meeting are not final because they have not been reviewed or approved by the assessment team management/leadership. As noted above, this is important to allow for some post-site discussions that may change the list of strengths and findings.
- Inform the client of any serious safety or compliance issues uncovered during the assessment.
- Present a summary of the Strengths followed by summaries of the Weaknesses. Ensure the weaknesses are to-the-point and answer the client's questions of "…so what?" Get the client to respond to these issues raised. Of note, the daily management briefings by the Team Leader should prepare the client manager for the lists of strengths and findings delineated.
- Summarize the next steps for report development and ensure the Statement of Work has been fulfilled.
- Offer the client the opportunity to ask questions, offer any perspectives or added information regarding the assessment.

This concludes the onsite risk assessment and the team returns to their offices to prepare the draft report as described in our next chapter.

Questions to Consider

1. As Team Leader, what is your role in ensuring the Statement of Work/Client Expectations are fulfilled? What actions should you take daily?
2. Describe the differences between Strengths and Good Practices and Weaknesses and Findings. Why is there a difference between onsite commentary and the final report?
3. Describe how Observations are used in this onsite risk assessment process.

REFERENCES

Clary, S. (2018). Advice: Stop Relying Solely on Floor Plans and Start Taking Pictures - Security Sales & Integration. Retrieved March 26, 2020, from https://www.securitysales.com/columns/floor-plans-take-pictures/

Hayden, E. (2013). Weighing Active Scanning of Industrial Control Systems. Retrieved March 26, 2020, from https://pentestmag.com/how-to-pentest-mobile-apps-pentest-regular-042013-teaser/

Hayden, E. (1994). *How to Conduct Material Condition Inspections - TR-104514*. Palo Alto: Electric Power Research Institute.

Hayden, E. (2017). The Unseen Threat. Retrieved March 26, 2020, from https://www.asisonline.org/security-management-magazine/articles/2017/11/the-unseen-threat/

Hayden, E., & Alvarado, J. (2017). *Evaluation Methodology*.

INPO Staff. (1990). *Performance Objectives and Criteria for Operating and Near-term Operating License Plants*.

McNamara, C. (n.d.). General Guidelines for Conducting Research Interviews. Retrieved March 14, 2020, from https://managementhelp.org/businessresearch/interviews.htm

News, K. (2020). Update: One remains in the hospital after Beechcraft plant explosion. Retrieved March 23, 2020, from https://www.ksn.com/news/local/update-two-remain-in-the-hospital-after-beechcraft-plant-explosion/

Powell, C. (2020). Hard Work Quote. Retrieved from https://www.brainyquote.com/quotes/colin_powell_121363?src=t_hard_work

Smithers, J. (2020). Effective Safety Inspection Program Based on Training, Observation, Interaction - Workplace Material Handling & Safety. Retrieved March 26, 2020, from http://www.workplacepub.com/material-handling/safety/effective-safety-inspection-program-based-on-training-observation-interaction/

Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security SP 800-82 Rev. 2*.

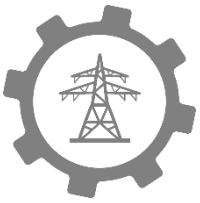
Retrieved from https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

Tibbs, J. (2014). Terrorism underground | Government Security News. Retrieved March 26, 2020, from https://www.gsnmagazine.com/article/40471/terrorism_underground

US Department of Homeland Security, & Infrastructure, U. C. for the P. of N. (2010). *DHS / CPNI - Cyber Security Assessments of Industrial Control Systems Good Practice Guide | WaterISAC*. Retrieved from https://www.waterisac.org/portal/library/2001dhs-cpni-cyber-security-assessments-industrial-control-systems-good-practice

US National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 | CSRC. Retrieved March 26, 2020, from https://csrc.nist.gov/publications/detail/white-paper/2018/04/16/cybersecurity-framework-v11/final

Williams, S. B. (2020). Hard Work Quote. Retrieved from https://www.brainyquote.com/quotes/sonny_bill_williams_772036



Chapter 7
The Final Report

The job isn't finished until the paperwork is done.

- *Anonymous*

Or

Good writing is like a windowpane.

- *George Orwell*

As the first quote above reminds us, the work is not finished until we have completed all the necessary paperwork. Generally, for any risk assessment we need to communicate our findings and key discoveries to our clients and management, or all our hard work is for naught. These findings need to be written and presented in a manner useful for the corporate and facility management. The goal of the report and supporting documents is to provide unbiased and accurate information regarding the risks, vulnerabilities, threats, and good practices. The report should also include necessary recommendations to resolve any findings.

In this chapter you will discover:

- What artifacts to collect and compile in order to develop the good practices and findings.
- How to ascertain the level of risk for each finding and how to prioritize them.
- A recommended format for the written report.
- Suggested ways to incorporate recommended actions to mitigate or correct the identified findings.

Where are we in the overall process? We are focused on ***"Reporting"*** as depicted in the graphic below from Chapter 3.

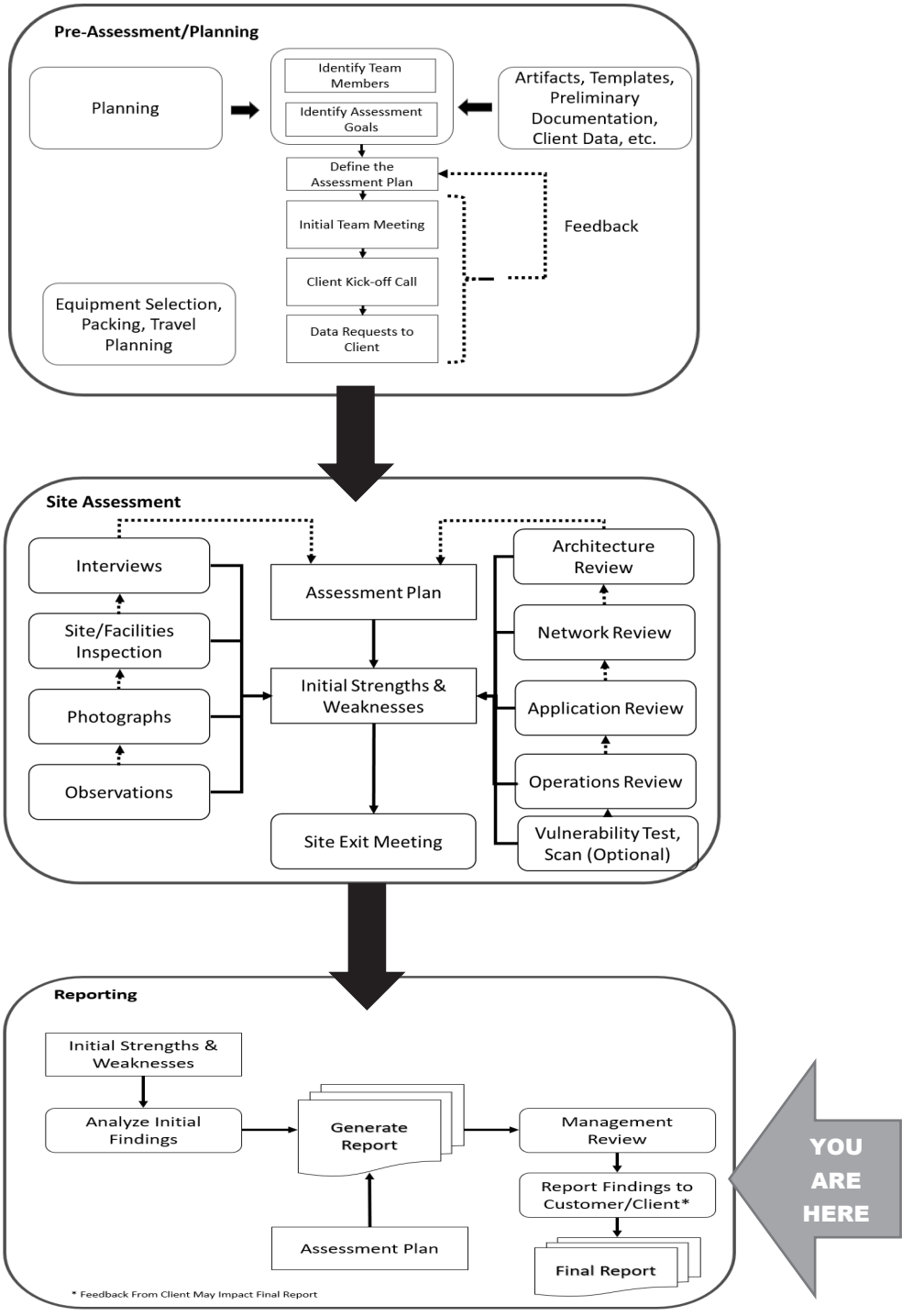


Figure 7-1 Hybrid Facility Risk Analysis Flow Chart

7.1 Back in the Home Office – Compiling the Information

Welcome home! You have returned to the office and you and the risk assessment team members are ready to begin writing the first draft of the risk assessment report. But, before you begin writing, you need to collect and compile the following:

- Meeting notes of all meetings held before arriving on site and while at the facility.
- All written observations which include identified strengths and threats, areas needing improvement and corrective action.
- Any documentation collected and reviewed as part of the risk assessment including preparatory information before departing for the site.
- Photographs.
- Interview notes.
- Any other data that can ultimately be used to write the Good Practices and Findings.

7.2 Important Terms of Art

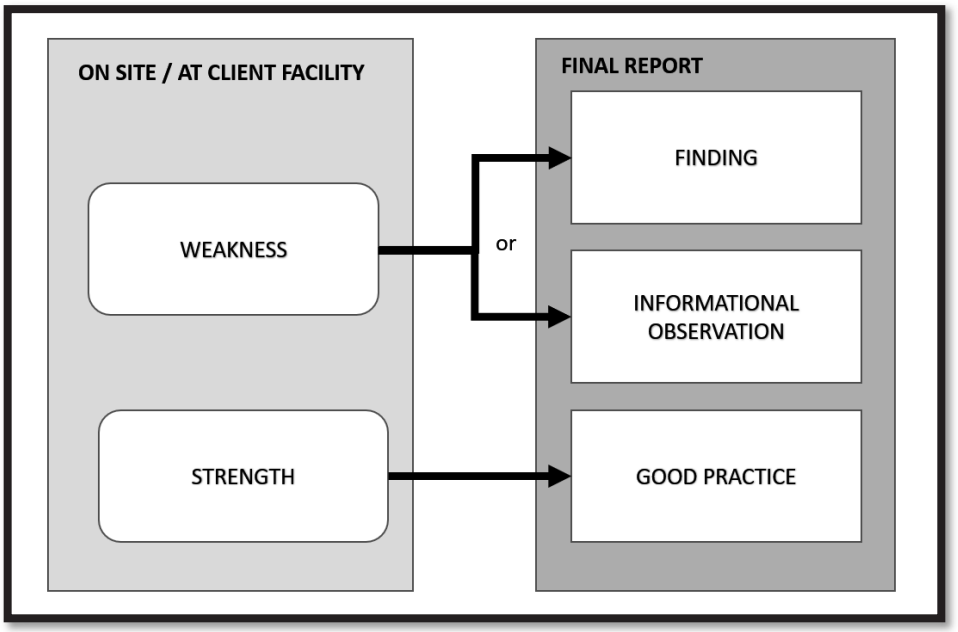


Figure 7-2 Evolution of Field Issues to the Final Report

To help the reader, the graphic above is intended to show how the "field talk" of Strengths and Weaknesses evolves into Findings, Informational Observations, or Good Practices.

When working on site, the risk assessment team should avoid terms such as Findings and Good Practices; however, they should develop their issues around the ideas of a Weaknesses and Strengths. Although we discussed this earlier in Chapter 7, I'd like to reiterate their definition since they will allow for ready development of Findings, Good Practices, and Informational Observations.

7.2.1 Weakness

Weaknesses are the beginnings of Findings in the final report. A weakness could be evidence of problems with documentation, work performance, human factors, lack of spare parts, etc.

Many weaknesses tend to become Findings or Observational Observations in the final report – to be discussed later.

7.2.2 Strengths

Strengths are the start of Good Practices in the final report. Strengths are those work practices, documentation, training, or other performance characteristic helping the organization sustain a competitive edge in their market domain. The risk assessor may simply view a strength as a good idea that could be useful in the industry.

In reality most strengths become Good Practices and most weaknesses become Findings in the final report; however, it makes sense to only offer the site management the team's views of strengths and weaknesses since Good Practices and Findings are not official until approved by the Assessment Team's formal management and leadership.

As you can see, there is a subtle but important change from the field to the home office as the team writes the final report. We've discussed Strengths and Weaknesses but the final report will ultimately delineate the following:

- Findings.
- Informational Observations.
- Good Practices.

Here is more information on these terms.

7.2.3 Findings

A Finding is defined as succinct documentation of a deficiency in security, performance, work practices, or outstanding/uncorrected threat to the operation of the organization. A finding may involve deficiencies in internal controls, fraud, illegal acts, violations of provisions of policies, procedures, standards, or guidelines.

A good definition of a "finding" is offered by the US Government Accountability Office (GAO). According to the US Government Auditing Standards (GAO-07-731G)

> *"...findings may involve deficiencies in internal control, fraud, illegal acts, violations of provisions of contracts or grant agreements, and abuse. The elements needed for a finding depend entirely on the objectives of the audit. Thus, a finding or set of findings is complete to the extent that the audit objectives are satisfied.*

When auditors identify deficiencies, auditors should plan and perform procedures to develop the elements of the findings that are relevant and necessary to achieve the audit objectives."

It is important to recognize that elements needed for a finding depend entirely on the objectives of the risk assessment scope. Thus, a finding or set or findings are complete only to the extent the risk assessment objectives are satisfied. Therefore, when members of the risk assessment team identify deficiencies or weaknesses, they should develop the elements of the findings that are relevant and necessary to achieve the necessary level of performance by the client's employees, contractors, and vendors.

In my experience, Findings normally evolve from Weaknesses; however, there may not necessarily be a one-to-one correspondence. For instance, I've seen times when multiple Weaknesses become one Finding. Alternatively, one Weakness could evolve into more than one Finding as the team and risk assessment management review the information from the site.

7.2.4 Informational Observations

Informational Observations also evolve from the field-defined Weaknesses. However, the subtle difference is that a Weakness identified by the team may be out of scope relative to the risk assessment scope of work or contract. But it is important to raise a concern to the site management to ensure they are aware of the issue and that it is something they should correct.

An example of an Informational Observation would be a serious housekeeping issue. A room may simply be a mess, or a warehouse may be in such disarray that parts cannot be readily located. This could be identified as a Weakness by the risk assessment team on site but, when they are back in the home office, there is recognition the housekeeping or warehouse concerns are not in scope of the risk assessment. Don't throw these concerns away, but instead, identify them as Informational Observations to be included at the end of the report or even in an appendix.

7.2.5 Good Practice

Finally, the concept of the Good Practice has been discussed above. The Good Practice usually evolves from identified Strengths in the field.

7.2.6 More About Findings

Back to the GAO Auditing Standards, findings should include the following key elements:

- **Criteria**: What criteria or industry practice is not being achieved? This could include laws, regulations, standards, facility procedures, expected performance, business and work practices, etc. In essence, you are telling the reader why the finding is being raised. Again, you need to answer the "So What" question.
- **Condition**: The condition is the situation that exists. The condition may have been documented in an observation during the on-site assessment and can support the finding.
- **Cause**: The cause identifies the reason or explanation for the condition or the factor/factors responsible for the difference between the condition (i.e., situation that exists) and the criteria (i.e., desired state). Common factors include lack of management direction, less than adequate monitoring of the work, insufficient management assessment of the employee or contractor performing the work, etc. Lack of training, non-existent or poorly written policies and procedures, or blatant disregard of facility procedures can be discussed here in the finding.
- **Effect or Potential Effect**: Here is where the author can specifically and succinctly identify the "So What" aspects of the criteria not being met, the condition, and the cause. For instance, telling the reader how the finding can result in personnel injury or death, environmental releases, plant shutdown, customer impact, reputational impact, etc. should be included in the finding discussion.

In my past work, when I write a finding, I try to begin the finding with a succinct description of the problem. In my work at INPO this was affectionally referred to as a "FOP" – Fundamental Overall Problem. Writing a FOP is not as easy as it seems and requires practice. Overall, the reader's attention needs to be captured so they realize the gravity of the issue. If you do not draft an effective FOP then the reader's attention may be lost or you may simply be rambling. This requires practice but is worth it in the long run.

7.3 Identifying the Risk Level of Findings

In the different phases of the site risk assessment, the team members will identify and report on vulnerabilities and risky activities observed. In many instances the problems are captured in the Observations prepared and compiled as part of the pre-visit and on-site work. As the risk assessment moves ahead, the problems will be identified as Concerns or Weaknesses on site and will be presented as such to the site/facility manager. Later, back at headquarters, the Concerns will eventually be reviewed and determined to be a Finding or not. Next, however, the team and team manager will need to take each Finding and ascertain two critical elements:

- Potential Impact – that is impact on the facility, corporate reputation, safety, environment, share value, etc., and

The Problem with FOPs!

Writing the "Fundamental Overall Problem" is like writing the lead sentence into a complicated paragraph or report or news article. It is important to succinctly get the point across to the reader an help them begin to understand the FOP.

For instance, one FOP that is usually problematic is "The material condition of the facility needs improvement." Unfortunately that is a bit too vague. Heck, you can say that about my car all the time!

Instead, try something like this: "Numerous issues with the material condition of the facility were observed including several leaking valves, combustible materials stored behind critical equipment, and exposed and uninsulated wires."

This example gives a summary view of the problems observed and causes the reader to want to read more of the details and examples.

- Likelihood of Occurrence/Probability – i.e., is it frequent, occasional, remote, improbable, etc. For instance, an asteroid hitting the earth would be characterized as a remote likelihood. Alternatively, temperatures exceeding 100 degrees is a frequent likelihood for a facility located in a desert.

Using these elements, the team manager can then identify a recommended level of risk which is usually one of the following categories:

- Critical.
- High Risk.
- Medium Risk.
- Low Risk.

However, before we get to labeling the Finding, we need to identify any impact the finding will have on the organization or facility and we need to identify the likelihood the finding will result in damage to the organization's personnel, assets, facilities, finances, reputation, or legal stature.

7.3.1 Impact

When determining impact level for each finding my favorite matrix is from National Institute of Standards and Technology (NIST) Special Publication 800-82, Revision 2, ***Guide to Industrial Control Systems (ICS) Security*** (Page 6-3)**.** The matrix is shown below:

Table 7-1 Possible Finding Impact Parameters

Impact Category	Low-Impact	Moderate-Impact	High-Impact
Injury	Cuts, bruises requiring first aid	Requires hospitalization	Loss of life or limb
Financial Loss	$1,000	$100,000	>>$1,000,000s
Environmental Release	Temporary damage	Lasting damage	Permanent damage, off-site damage
Interruption of Production	Minutes	Days	Weeks
Public Image	Temporary damage	Lasting damage	Permanent damage

This matrix is fairly intuitive and easy to use when evaluating Findings and determining their relative impact category.

In the risk management world, there are a variety of matrices and heat maps used to portray and categorize risk level. One other example below is a hybrid chart I've used for some of my risk assessments.

Table 7-2 Impact Determination Matrix

Impact	Brand, Public Exposure	Business Impact	Environmental Health & Safety	Financial	Legal
Critical	Large-scale (TV or other national or international news media); Incident affecting children	Severe (Facility is closed long-term); Product involved is high-margin and volume	Multiple fatalities; Impact extends beyond corporate property	Impact >$25M	Lawsuit against corporation; Breach of US or International Law
High	Local media interest	High (Facility process shut down for >72 hours)	Fatality; Serious impact to corporate property	Impact $5M - $10M	Lawsuit against regional corporate entity; Breach of US or International Law
Medium	Minor – only members of the public directly affected are aware	Facility shut down up to 48 hours	Serious injury reportable to local entities	Impact $1M - $5M	Threat of legal action; Potential Breach of US Law
Medium-Low	Minimal	Facility or process is interrupted but restored within 24 hours	Minor injury, sprains, strains, small cuts – simple first aid	Impact $500K - $1M	Demand for compensation without involvement of lawyers
Low	None	None	No injury	Impact <$500K	No legal threat or potential breach

7.3.2 Probability or Likelihood

According to British Standards publication ***Risk Management***, there are three general methodologies used to estimate the probability of an event. In summary, these methods are:

- Use of relevant historical data to identify events which have occurred in the past and one can ascertain the probability of these same events occurring in the future.
- Use of fault tree and event tree analysis to develop probability forecasts.
- Use of expert opinion to estimate probability.

Sometimes these approaches can be too cumbersome to determine the estimated probability and its associated categorization. Hence, using the following definitions of event probability can be very helpful.

Table 7-3 Likelihood of Occurrence Parameters

Probability	Nominal Definition
Very Likely/Frequent	Weekly or daily occurrence
Likely/Probable	Monthly occurrence
Possible/Occasional	One occurrence per year
Infrequent/Remote	One occurrence every 25 years – Not likely to occur
Rare/Improbable	Unlikely to occur; Practically impossible

7.3.3 Risk Assessment Matrix Development

Remember back in Chapter 3 where we talked about the Risk Equation? We can now use the information and parameters defined above to identify the level of risk to assign the Finding which will help the facility manager prioritize where to put their resources to solve the most important issues.

The most common approach I've seen and used is the classic Risk Assessment Matrix and Heat Chart. Here is an example I'd recommend – especially now that we have the risk parameters defined above.

Table 7-4 Risk Assessment Matrix

Impact → / Likelihood ↓	Critical	High	Medium	Medium-Low	Low
Very Likely - Frequent	Critical	Critical	High	Medium	Medium
Likely – Probable	Critical	Critical	High	Medium-Low	Medium
Possible – Occasional	Critical	High	Medium	Medium-Low	Low
Infrequent – Remote	High	Medium	Medium	Low	Low
Rare - Improbable	Medium	Medium	Medium	Low	Low

Fundamentally, the assessment team and associated managers should examine the Findings for their Impact and Likelihood. Then, using this matrix, they can ascertain whether a Finding is Critical, High, etc.

This matrix is a guideline and is not necessarily to be used as a final answer. Judgement by the team, team manager, and corporate manager may allow for a Finding to lean to a lower level of risk. For instance, if the likelihood and impact are between a High and Medium, the management may declare a Finding as a Medium due to the facility management's attitude and level of professionalism.

Alternatively, if the likelihood and impact reveal a Finding between a High and Medium, the final decision may be for a High Risk Finding since there are concerns the facility manager may not take the issue seriously enough to take corrective action.

In summary, using the above Risk Assessment Matrix and some professional judgement the Findings can be categorized relative to their criticality and importance. Then, they are included in the Assessment Report in hierarchical order from Critical to Informational Observations.

7.4 Preparing the Draft Report

At this stage in the process the assessment team has identified the Findings, Good Practices, and Informational Observations. Additionally, the Findings have been categorized from Critical to Low. Now, the focus is on writing the draft report for presentation to the client.

Remember, the intention of the report is to inform the facility managers of the positive and negative issues raised by the assessment team. It should be succinct and always answer the “so what” questions.

The nominal table of contents for the draft report is shown below:

Figure 7-3 Example Table of Contents

EXAMPLE TABLE OF CONTENTS

XYZ RISK ASSESSMENT

DATES: ### to ###

1. **EXECUTIVE SUMMARY**
    a. Purpose and Scope of the Risk Assessment
    b. Summary of Team Activities and Methods Used
    c. Summary of Good Practices and Findings
2. **INTRODUCTION & SCOPE**
    a. Purpose of the Report and Risk Assessment
    b. Scope of the Assessment
    c. About the Risk Assessment Team and Members
    d. Assessment Methodologies Used
    e. Explanation of Finding Severity Ratings
3. **GOOD PRACTICES, FINDINGS, INFORMATIONAL OBSERVATIONS**
    a. Good Practices
    b. Findings
        i. Critical Findings
        ii. High Risk Findings
        iii. Medium Risk Findings
        iv. Low Risk Findings
        v. Informational Observations
    c. Miscellaneous Supporting Information
        i. Potential Vulnerabilities
4. **SUPPORTING TABLES & FIGURES**
5. **DOCUMENT CHANGE CONTROL**
6. **ATTACHMENTS (AS REQUIRED)**

Of course, this format can be modified as necessary to satisfy the statement-of-work, the assessment plan, the client's requirements, etc., including a review of the background stimulating the risk assessment, etc.

There is a topical section in 3.c.i, Potential Vulnerabilities. I've used this section for some risk assessments to discuss items where there is a suspicion of a problem; however, there is not adequate data or information to support declaring a Finding. Hence, the team can declare any potential vulnerabilities for the client's awareness without making a hard and fast Finding that may not be fully supported.

One other consideration for the report development is possibly clustering all Good Practices and Findings according to a topical area. This approach is useful when the corrective actions will be assigned to the client manager owning the problems. For instance, the Operations Manager may find it useful to read a report where all operations-related findings are clustered together, and the Procurement Manager would find the same benefit for his findings. Overall, this approach can work, but a general hierarchy of Findings from Critical to Low will give the client general management a better sense of the problems identified by the risk assessment team.

It is best to take time before the risk assessment begins to understand the Final Report expectations from the client rather than wait until the drafting phase where a myriad of questions on format and style may arise.

7.5 Report Review Process

The report review and approval process should also be reviewed with the client long before the report needs to be finalized. Consider determining these steps in the pre-assessment phase of the schedule.

Nominally, once the first draft is written, it is forwarded to the appropriate risk assessment team administrative support to check for format, font, style, grammar, and so forth. Corrections should be made as necessary and the Team Manager approves the first draft.

At this point corporate reviews are performed as required by the assessment team management such as legal. Concerns and issues are identified to the Assessment Team Manager who resolves the problems and updates the report.

At this time the DRAFT report is forwarded to the client manager or representative for review, markup, comment, etc. It is appropriate for the client to have the right and responsibility to review the DRAFT report and identify issues, concerns, areas needing additional information, etc.

The customer's comments and red-lines of the DRAFT report are returned to the Team Manager for resolution.

Finally, the resolved comments are incorporated into the FINAL report and submitted to the client.

An elementary flow chart of this process to finalize the risk assessment report is shown below:

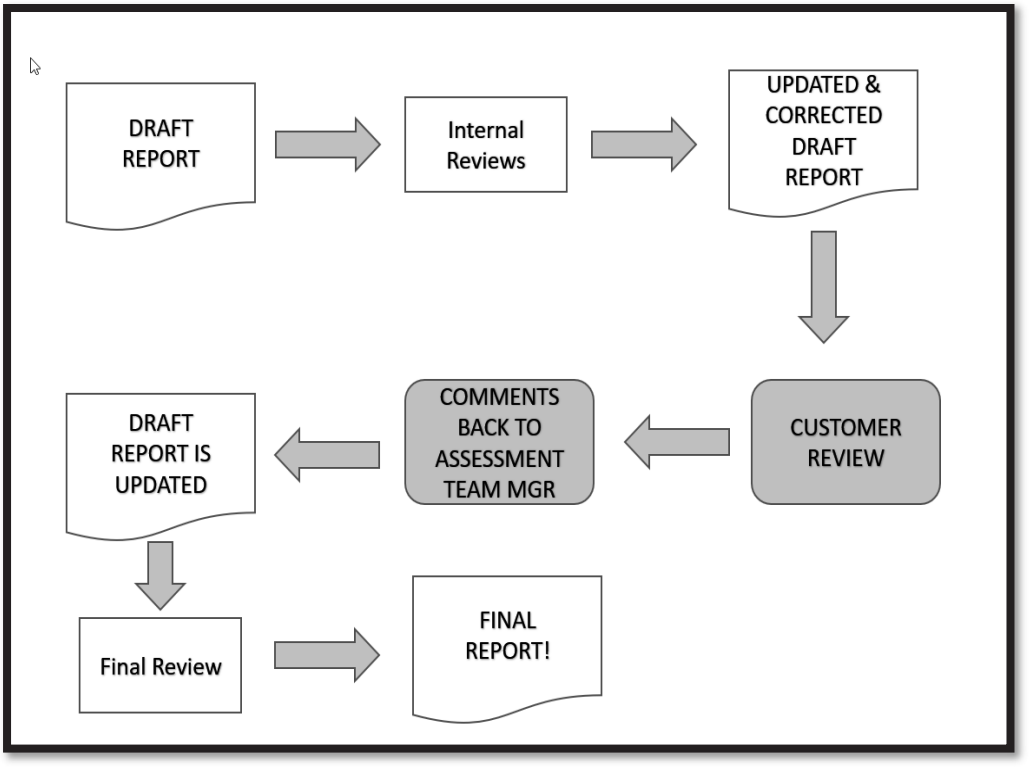


Figure 7-4 Risk Assessment Report Review Process

7.6 The Future of the Report

The intention of the report is to communicate the areas needing attention and resources by the facility management. The report is written in a fashion that the higher risk Findings are listed first in the report giving the facility manager a sense of what needs to be attended to first and foremost.

Nominally, the facility manager should at least focus on the Critical and High-Risk Findings and develop an action plan to resolve these issues. Secondly, the facility manager should look at the remaining Findings and take corrective action on the "low hanging fruit" and less expensive issues. It is doubtful that every finding will be corrected immediately; however, it is in the facility manager's best interest to assign a project manager to monitor the corrective actions and close out the Findings a quickly as possible.

Another future for the Report is associated with the next risk assessment. As a risk assessment Team Manager, I try to review any previous risk assessments performed for the facility/corporation and get a sense of past Findings, Good Practices, etc. Of course, if the next risk assessment is a review of past Findings, then the report will provide the foundation for the next facility risk review.

Overall, writing the report is important to give the client a succinct sense of the key issues needing corrective action and the report itself can be used as a reference for future risk reviews.

REFERENCES

British Standards Institute. (2010). BS EN 31010:2010 Risk management. Risk assessment techniques. Retrieved April 13, 2020, from https://shop.bsigroup.com/ProductDetail/?pid=000000000030183975

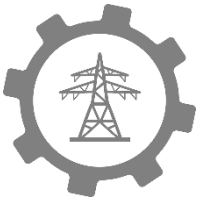
Garcia, M. L. (2006). *Vulnerability Assessment of Physical Protection Systems*. New York: Butterworth-Heinemann/Elsevier.

Hayden, E., & Alvarado, J. (2017). *Evaluation Methodology*.

Orwell, G. (2020). Good writing is like a windowpane. Retrieved April 7, 2020, from https://www.brainyquote.com/quotes/george_orwell_189107

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security*. Gaithersburg, MD USA. Retrieved from nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

US Government Accountability Office (GAO). (2007). *Government Auditing Standards*. Retrieved from https://www.gao.gov/new.items/d07731g.pdf



Chapter 8
Remediation

Don't find fault, find a remedy; anybody can complain.

- *Henry Ford*

Or

The point is to solve problems, not point fingers.

- *Jane Harman*

Setting the stage: You are the facility manager and you've just undergone a multi-week risk assessment. The final report is on your desk. It is three volumes constituting:

- Volume 1 –management findings,
- Volume 2 – physical security findings, and
- Volume 3 – cyber security findings.

Roughly 150 findings in all ranging from Critical to Informational findings. What should you do? How do you attack this beast?

This chapter is intended to give you some ideas and thoughts on how to proceed with the risk assessment remediation process.

In this chapter you will discover:

- How to put your arms around what to do next.
- Some techniques for tracking and correcting the issues.
- How to take advantage of the lessons learned for future operations.

8.1 Rule #1 – Don't Shelve the Report and Findings!

As a consultant I can't tell you how many times I've watched companies spend a lot of money and time to have a risk assessment or audit performed at their facility, and then put the report on a shelf (or hard drive) to collect dust and digital mites. This is simply irresponsible and does not fulfill the executive's fiduciary responsibilities.

Besides, the contents of the report may contain a simple issue that if addressed will save the company thousands of dollars and/or prevent an accident, injury, or death. Wouldn't it be terrible if an accident at the site is audited and it is realized that a finding in a dusty old report – if remediated – could have prevented the event?

If you recall, early in the assessment process, it is a good practice for the risk assessor to collect any previous risk assessments and audits and review the findings for any repetitive issues – before heading to the site. If you are expecting an audit or review, be sure to take time and read your previous reports to ensure past issues are not still prevailing – otherwise you can expect another finding.

8.2 Remember Your Objective

In spite of having multiple findings, remember that your objective is to reduce your facility's vulnerabilities and mitigate threats. Simply focusing on the quantity of findings and how many you can ignore or discard is not appropriate and will not fulfill the reasons you originally conducted the risk assessment.

8.3 Assign a Professional Project Manager

Regardless of the number of findings and issues, the first task for executive management is to assign the remediation process to a professional project manager. It is key the executive management provide *obvious* support to the project manager to ensure the organization takes this assignment seriously and spends the time to resolve the issues in a quality manner – to reduce the risks faced by the enterprise.

It is best the chief executive direct a broadcast message to the organization to a) announce the assignment of the project manager to the remediation project, b) direct the staff to support and aid the project manager in the process, and c) understand that the project manager is a direct representative of the chief executive.

The project manager's role should normally include engaging the fundamentals of the PMBOK – the Project Management Body of Knowledge – and immediately initiate the following sequence of steps:

- **Review the entire risk assessment report**. Gain a big picture of the identified risk issues and look for overlapping and similar issues.

The PM…What?

The Project Management Body of Knowledge (PMBOK) is a set of standard terminology and guidelines for project management. The PMBOK has evolved over time and is presented in **A Guide to the Project Management Body of Knowledge**, a document resulting from work overseen by the Project Management Institute (PMI) (www.pmi.org). The sixth edition was released in 2017.

According to some sources, much of the PMBOK Guide is unique to project management and includes such concepts as critical path method and work breakdown structure (WBS). The PMBOK also overlaps with general management regarding planning, organizing, staffing, executing, and controlling the operations of an organization. Other management disciplines which overlap with the PMBOK include financial forecasting and budgeting, organizational behavior, management science, as well as other planning methods.

- **Identify and categorize the findings**. Even consider ways to bundle responses to some of the findings.
- **Build the response team**. Ascertain who are the best players (and their direct supervisors) to respond to the findings.
- **Build a team matrix.** Identify these players by name, title, email, and phone number.
- **Hold a kick-off meeting.**

We'll go into more detail on each of these activities below.

8.4 Review the Entire Risk Assessment Report

Normally the risk assessment reports are treated as business confidential and contain very sensitive information. It could be a serious issue if the report were ever released to the press or to a competitor. Therefore, it should be held close to the corporate vest; however, the responding players and management need to understand the findings as well as the context of the issues identified. Consider handing out controlled and numbered copies of the report to those with a "need to know."

The project manager should review the report and ascertain the following elements, perhaps building a simple matrix and chart. Some examples are shown below:

Table 8-1 Risk Assessment Finding Breakdown: Table and Graphs

Domain	Strengths	Critical Risk	High Risk	Medium Risk	Low Risk	Informational Findings
Management	0	0	2	0	0	4
Physical Security	20	0	3	7	3	2
Cyber Security	7	9	17	38	41	1
Industrial Safety	3	1	4	4	1	2
Total	**30**	**10**	**26**	**49**	**45**	**9**

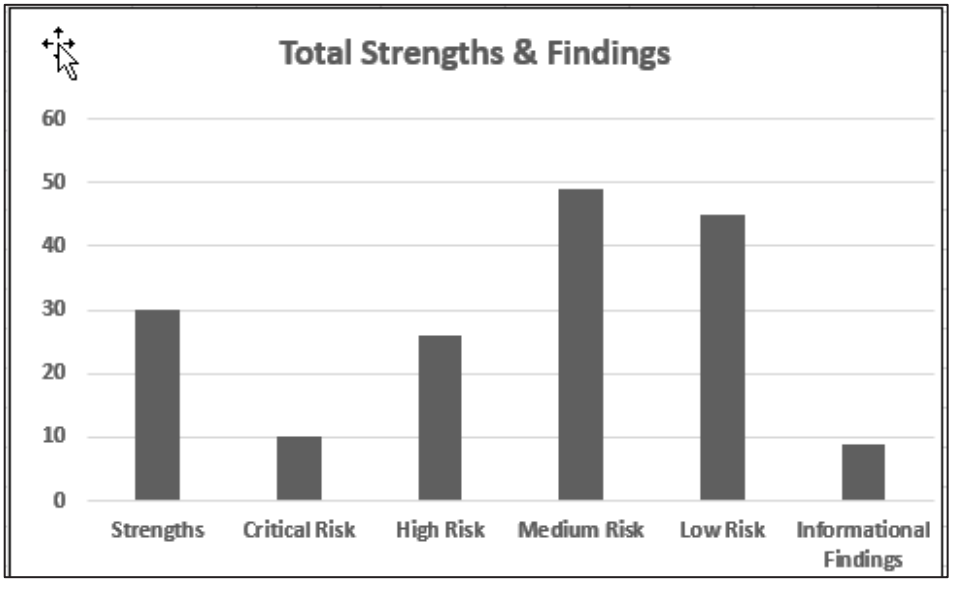


Figure 8-1 Total Strengths & Findings

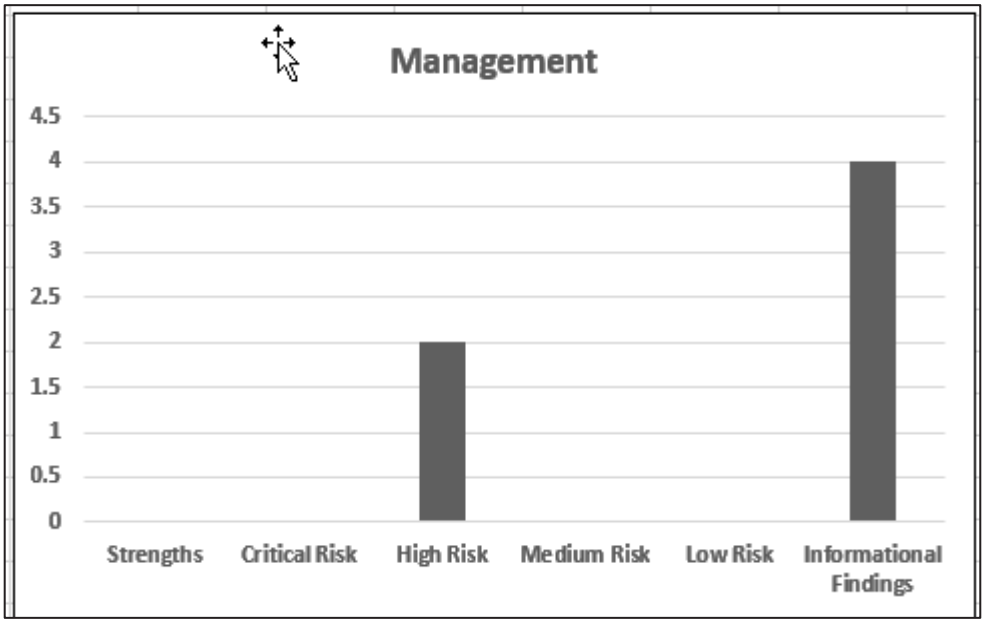


Figure 8-2 Management

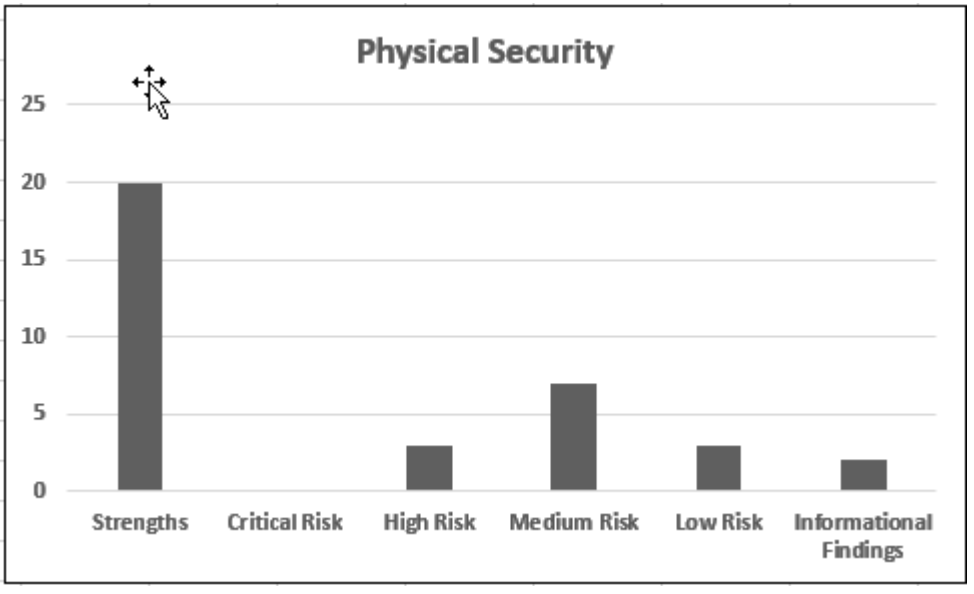


Figure 8-3 Physical Security

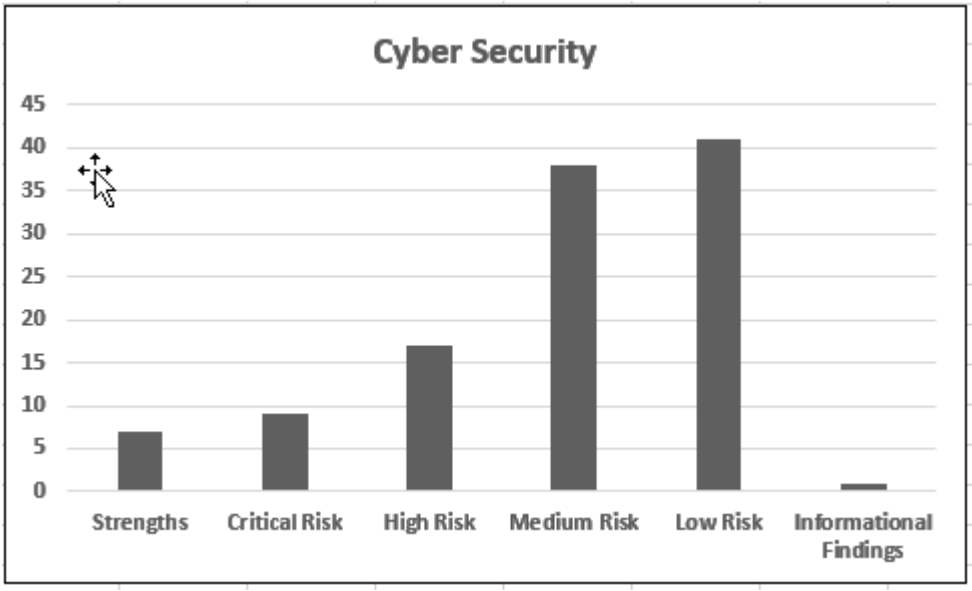


Figure 8-4 Cyber Security

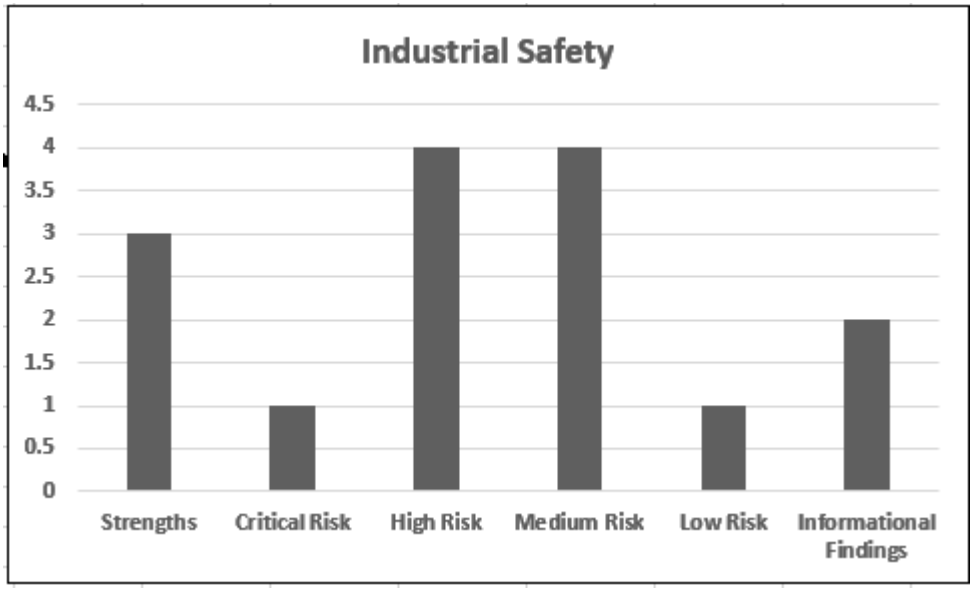


Figure 8-5 Industrial Safety

8.4.1 Recognize the Strengths!

Don't forget to consider the identified Good Practices/Strengths! Since these were identified by the risk assessment team, the facility executive should acknowledge and reward those responsible for the strengths with letters of acknowledgement, simple rewards such as gift cards, etc. You want to encourage everyone to be smart and creative – perhaps taking advantage of the identified strengths can be one avenue.

8.4.2 Assign Unique Numbers to Each Finding

Once you've read the report, ensure each finding has a uniquely assigned number. A technique I've seen – if not already included in the report – is to sequentially assign a letter and number. For instance, a Critical finding would be "C-#" and a High finding would be "H-#", etc. Alternatively, all the findings can be numbered sequentially from the first Critical finding to the last Informational Finding.

You will find this numbering scheme very beneficial later on when you are attempting to track and trend the finding remediations.

8.5 Build the Remediation Team

Using the information gleaned from the thorough review of the report, build a team matrix identifying those – by name – who should be assigned to address the corrective actions. This assignment would be based on their technical and cultural knowledge of the finding and why it occurred or was discovered. The individual may even be the cause of the finding; however, it is imperative they be part of the solution.

One utility I worked with called this group the Governance Committee.

The assignment matrix should also include the direct supervisor for these key remediation players to ensure they are given adequate support and resources to resolve the identified issues.

One such approach I've seen is a matrix like the following:

Table 8-2 Remediation Team Assignments

Department	Supervisor	Assigned Remediation Staff/Individual	Responsible Findings
Industrial Safety	John Smith	Alice Jones	• C-1 • H-2, 5 • L-17 • IO – 1, 4, 7
Information Technology	Aux Kahn	Robert Cole	• C-3 • H-1, 8 • M-1, 2, 3, 4, 5 • L – 8
Etc.			•

8.6 Kick Off Meeting

With the assignments made and listed in the matrix, hold a kick-off meeting. This meeting should include the following parties at a minimum:

- Chief Executive/Facility Executive – In order to show executive support for the team's efforts and set the "…tone at the top…" This is an operational imperative.

Auditor vs. Assessor

Earlier in the book we discussed the difference between an Audit and Assessment. It is also worthwhile to understand the difference between an Auditor and an Assessor.

According to the ISACA Code of Ethics (isaca.org), an Auditor must maintain their independence from the client organization in both "…fact and appearance." (Gregory 2010). However, an Assessor may not be bound by such requirements. This is difficult to pristinely address, but an Assessor may have more flexibility in helping the client with their findings and finding remediation. Such a decision should be well thought out before the Assessors are used to help resolve the risk assessment findings.

- Project Manager (Meeting Facilitator/Leader).
- Appropriate Supervisors.
- Primary Corrective Action Players.
- Subject Matter Experts.
- Assessors themselves who identified the issues and findings.

Alternative attendees could include members of the Board, subsidiary executives, etc.

The kick-off meeting is intended to do the following. First, have the chief executive provide the overall message to the players that the findings need to be addressed quickly, thoroughly, and in a timely manner. Second, have the chief executive emphasize that the Project Manager is their representative and should be respected and obeyed due to their position of

project leadership. Third, the team needs to review all the findings as well and look at ways the findings can be "bucketized" or "chunked" in order to effectively and efficiently address the issues.

For instance, there may be many findings that are easily addressed – regardless of their criticality or risk. Similarly, there may be a collection of findings that can be simultaneously addressed with the corrective actions. Thus, corrective actions can be performed in parallel rather than in series.

Root Cause

Root Cause is the fundamental cause(s) and associated corrective action that, if corrected, will prevent recurrence of an event or adverse condition.

• Root Causes are underlying, reasonably identifiable.

• Root Causes can be controlled by management.

• Root Causes allow for generation of recommendations.

Source: Introduction to Root Cause Course, Ernie Hayden (2009)

Use the kick-off and subsequent meetings to educate the executives and team on ways to look at the findings and identify the ***root cause*** rather than just fixing the symptom.

One subject for team education is the impact one system may have on other systems at the facility. For instance, a cyber finding could have an impact on cyber systems as well as physical security because the physical security systems rely on computer networks and protocols.

Another subject for the training is to include presentations from the risk assessors or other qualified risk assessment experts to discuss how they assess systems and components and perform risk analyses. This will help the team better understand the techniques to use when looking for vulnerabilities (similar to the contents of this book!).

Before I forget, ensure you remind the team members that there will be a post-mortem at the end of the remediation project and everyone should keep notes on what went right, what went wrong, and what they found most effective to closing the findings.

8.7 Monthly Meetings (or More Frequent)

The remediation team should meet as a group at least monthly. The facility/corporate executive (or representative) should also be in attendance to support the effort and Project Manager and to "show the flag."

These meetings are intended to do the following:

- Demonstrate progress in addressing the risks and findings.
- Identify areas where individuals and teams require assistance and resources in order to close the finding. This could include such things as new equipment, budget, training, etc.
- Consider including presentations from some of the team members on how they closed a finding in order to help the team absorb lessons learned they can apply to closing their own assigned findings.

8.8 Addressing the Findings

As the findings are addressed by the team members there are some key considerations I've alluded to above but want to reiterate.

First, the Executive Management needs to drive this remediation process through the Project Manager. Expecting everyone to simply run out and correct the issues is a bit of a misunderstanding. People will be distracted from the remediation tasks due to their current workload.

It is also recognized that the corporation does not have infinite funds and resources and not all findings will be addressed. This again requires the

Executive to address budget constraints so priorities on remediation can be determined. I'll talk about a method used to help identify the budgetary

Incidents During Remediation

During the course of the remediation project actual events and emergencies may occur. If this is the case, be sure to take advantage of the run-ins that occur during remediation and reflect on the current remediation findings. As my good friend Jennifer Tavaglione says, "Don't let any good emergency go to waste!"

issues when addressing many findings.

As observed above, use project management techniques and methodologies to manage the remediation mission. These methods should help with establishing accountability for each team member and provide visibility into the remediation process including progress and risks to completion. The project management process will help with scheduling and timelines.

Sometimes the team members will get bogged down addressing a finding. They simply don't understand why the finding exists or how to resolve it. This may be a time to use process mapping techniques when you can compare current state and future state and identify what is required to be done to close the finding. Include vendors in these discussions since they may have been the cause of the finding.

Include change management when performing the remediation. Just making a fix to a cyber system could violate change management policies and procedures. Be sure the change management procedures are followed. The responsible staff member should bring this up to the Project Manager if there are complications or barriers in the way.

A key point is to not blame anyone for the finding – even if blame could be imposed. It defeats the objective of remediating the issue. Instead, if it is obvious one or more individuals are the cause consider the root cause could

be a lack of adequate training, poor documentation (procedures, manuals), or inadequate management direction and oversight. If any of these are the case, work on these issues and don't point fingers, which causes challenges and team turmoil.

As the findings are considered closed, it is best to enact an independent verification and validation to ensure the remediation was a success. At one utility I assessed, the utility brought the assessment team back onsite to validate the findings were closed. This worked well since the assessors were steeped in knowledge about the findings, the utility, and the utility culture. Then, if the findings were not adequately addressed or closed, the assessors could help the Project Manager and affected team members better identify ways to completely fix the problem.

8.9 Costs and Budgeting

Remember, you've been assigned dozens and dozens of findings to address and remediate; however, your budget may not endure all the expenses to correct these issues. How can you proceed?

One technique used at one company I assessed is shown in the cost breakdown table below. We populated this table to the best of our knowledge and used cost ranges to categorize the anticipated finding remediation costs. Admittedly, this is not perfect; however, the information gathered helps the company executive approach the finance team and even the Board of Directors when requesting additional funds to correct the findings.

Table 8-3 Remediation Cost Estimation Spreadsheet (Example)

Finding Number	Risk Severity	Finding Title	Recommendations	Implementation Cost Category $ < $10K $$ $10K - $50K $$$ >$50K
2.2.1	**HIGH**	**Physical and IT Security Leadership, Management, and Oversight**	R1: Establish a single point of accountability and leadership for cyber and physical security for the company.	**$$**
			R2: Establish frequent OT/IT Governance Board Meetings (weekly) to continue the formation of the governance and oversight processes and begin to establish a methodology for intake, review, and decision-making for requests for new technology and security changes.	**$**
			R3: Develop a Governance Board Charter.	**$**
			R4: Develop cyber and physical security policies and procedures.	**$$**
			R5: Implement an Office of the Chief Security Officer and Security Organization.	**$$$**

You can also use the risk severity (Critical, High, etc.) as a multiplier on the fund estimate. For instance, the Critical finding multiplier could be 5 and Low could be 1. At least this gives the finance team a sense of which expenses are first and foremost when making financial arrangement.

8.10 Postmortem/After-Action Review

When the project is done – or at least close to completion – perform a post-mortem or after-action review of the project. This is a process used by professional project managers and career emergency management staff. The idea is to review the activities performed to start, monitor, steer, etc. the project and gain lessons-learned for the next remediation project.

A project post-mortem is a process, usually performed at the conclusion of a project, to determine and analyze elements of the project that were successful or unsuccessful. The Department of Homeland Security Homeland Security Exercise and Evaluation Program (HSEEP) refers to this review process as capturing "lessons-learned." Project post-mortems are intended to identify process improvements and to promote best practices.

One technique is to bring the risk remediation team together for a full-day workshop. The workshop would do a few things. First, it is a way to celebrate the hard work performed and to offer some recognition to the key players who did the heavy lifting. Secondly, the post-mortem would give everyone an opportunity to identify a) what went right and was done effectively, b) what was problematic and needs more attention, and c) the key lessons learned to implement for the next risk assessment findings remediation effort.

In this process consider making checklists to be used for the next remediation project.

An excellent resource and tickler for topics to ask and address during the post-mortem is in the US Department of Homeland Security Exercise and Evaluation Program (HSEEP) After Action Report/Improvement Plan Template. This can be located at: https://www.fema.gov/hseep

The post-mortem and the other documents generated for this project are business documents containing sensitive information and need to be protected and available should there be any legal action.

8.11 Questions for Consideration

1. Why do you think risk assessment reports are ignored and shelved?
2. What is the most important aspect of the remediation process? Why?
3. Why do you think people are blamed for findings rather than credited for solving the problem?
4. What would you do if you were given 150 findings to resolve? What would you do different than the processes described above and why?

REFERENCES

Eby, K. (2018). 5 Phases of Project Management. Retrieved from https://www.smartsheet.com/blog/demystifying-5-phases-project-management

Ford, H. (2020). Remediation Quote. Retrieved November 5, 2020, from https://www.goodreads.com/quotes/search?utf8=✓&q=REMEDIATING+FINDINGS&commit=Search

Fullin, R. (2016). How to Create a Great Compliance Remediation Plan (While Controlling Costs). Retrieved November 5, 2020, from https://www.complianceteaminc.com/how-to-create-a-great-compliance-remediation-plan/

Gaudin, S., & Lewis, D. (2006). UBS Trial Aftermath: 10 Tips for a Successful Postmortem. Retrieved from https://www.liquidmatrix.org/blog/ubs-trial-aftermath-10-tips-for-a-successful-postmortem/

Gentile, M. (2016). Information Security Remediation Plan. Retrieved November 5, 2020, from https://cisohandbook.com/articles/information-security-remediation-plan/

Gregory, P. (2010). Ethics and Independence. In T. Green (Ed.), *All in One CISA Certified Information Systems Auditor Exam Guide* (pp. 497–498). New York: McGraw Hill.

Harman, J. (2020). Solve Problems Quote. Retrieved November 5, 2020, from https://www.brainyquote.com/quotes/jane_harman_206369

Hayden, E. (2009). *Root Cause Analysis Course*.

ISACA. (2020). Code of Professional Ethics. Retrieved May 15, 2020, from https://www.isaca.org/credentialing/code-of-professional-ethics

Kroll, K. (2020). When Audit Findings Go Ignored. Retrieved November 5, 2020, from https://internalaudit360.com/when-audit-findings-go-ignored/

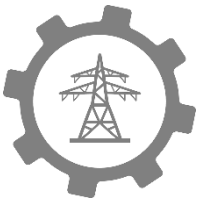
Morgan Franklin Consulting. (2020). The MorganFranklin Way. Retrieved November 5, 2020, from https://www.morganfranklin.com/services/government/audit-remediation/

Muldoon, J. (2014). *PMBOK Summarized*. Retrieved from http://johnmuldoon.ie/wp-content/uploads/2014/08/PMBOK-Summarized.pdf

SC&H Group. (2019). Audit Remediation Monitoring: Fostering Accountability and Effective Risk Mitigation. Retrieved November 5, 2020, from https://www.schgroup.com/resource/blog-post/audit-remediation-monitoring-fostering-accountability-and-effective-risk-mitigation/

Tavaglione, J. (2020). Telephone Interview.

US Department of Homeland Security. (n.d.). Homeland Security Exercise and Evaluation Program (HSEEP) - After Action Report/Improvement Plan (Template). Retrieved from https://www.fema.gov/hseep



Chapter 9
Continuing the Journey

Just do it!

- Nike

"Hey Boss, I know how to do a Risk Assessment!"

Remember the opening story in Chapter 1? How a boss called and expected a site manager to do a risk assessment… and they didn't have a clue? Well, this book is your handbook to jump in and perform the assessment and record your results and recommendations.

In reading this book, you now have the tools and understanding to address the following key topics:

- What constitutes Critical Infrastructure?
- The fundamentals of risk and the risk equation.
- Overall risk assessment process and methodology.

- Ideas on how to prepare for the assessment.
- Guidance on performing the onsite assessment.
- Entry and exit Meetings.
- Interviewing site personnel.
- Reviewing client documentation.
- Conducting physical plant inspections.
- Performing and documenting observations.
- Developing the final report and findings.
- Details on identifying risk and risk severity ratings.
- Preparation of the initial draft.
- Issuing the report and follow-up.

Remember, as you move ahead with your risk assessments, feel free to use the map below to guide you with ideas and concepts as you proceed.

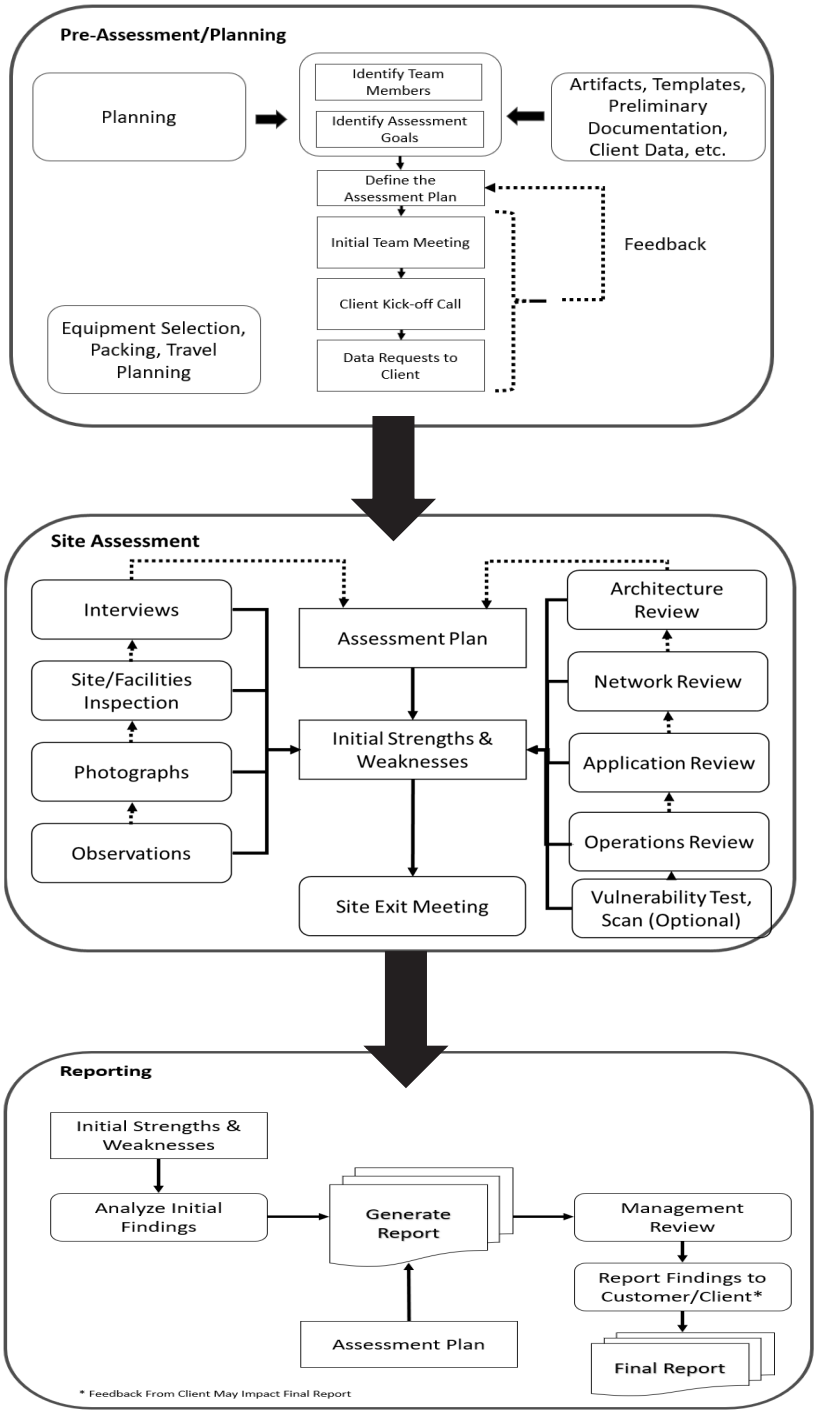


Figure 9-1 Hybrid Facility Risk Analysis Flow Chart

Your Job

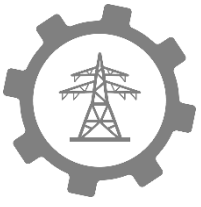
Your job is to jump in and use this handbook to guide you and your teams when they perform risk assessments and other facility vulnerability analyses. There's a lot going on and I think you'll find this a worthwhile manual. You'll also find this information in your personal and professional development as you learn how to look at things and circumstances with the mind of a critical thinker. You'll even begin to develop your own techniques and methodologies that compliment this process. Maybe the future will include more photo documentation using 3-D images! Even discoveries of vulnerabilities in a complicated facility may be directly loaded into the work control system for repair!

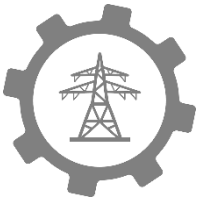
It is an exciting time and this is just the beginning!

Good Luck! Enjoy your journey as you try to eat the elephant!

Thank You!

I trust you will find this book beneficial and will offer you many ideas to apply to your current and future jobs. I look forward to your feedback and comments on the book and encourage you to pass along your ideas, suggested changes, etc. to me at enhayden1321@gmail.com.





APPENDIX A
EXAMPLE RISK ASSESSMENT REPORT

The following is an example risk assessment report representative of reports I have written or been a contributor over the years. The intention of this example report is to demonstrate the flow of a report with example – but fictional – contents. It is not intended to reveal any client secrets or confidential material; however, I have included some text – with modifications – from previous reports I have prepared. This is a representative report for an industrial facility risk assessment.

Vendor names are changed as appropriate and there is no intentional or accidental attribution to any clients.

RISK ASSESSMENT

BOONDOCKS FABRICATION PLANT

12345 Boondocks Road
Nowhere, KS 66767 USA

Phone: XXX-XXX-XXXX

Photo by Ernie Hayden

Conducted on 24 - 28 February 2020

Performed by: (Project Lead Name)

projectleademail@gmail.com

Cell: ###-###-####

EXECUTIVE SUMMARY

In early Fall 2019 Mr. Ernie Hayden (Consultant and Project Lead) was approached by Boondocks Fabrication Plant (Factory) to perform a risk assessment of their Kansas production factory with focus on physical and cyber security, industrial safety and controls, and operations and maintenance personnel performance. A Statement of Work (SOW) was developed in and used to guide the performance of this assessment.

The actual assessment was performed on site on 24 to 28 February 2020 by the Project Lead and a team of two additional qualified consultants and analysts.

The assessment activities were primarily performed onsite at the factory and coordinated with the Customer at their direction. The activities generally started with an overall review of the physical plant, the cyber systems, and the industrial control security program. Once this walkdown was completed a variety of reviews and inspections were conducted usually starting at the Program level and then with deeper reviews on individual systems and components as necessary. Focus of this effort included:

- Physical security and physical access controls.
- Cyber security and information protection.
- Cyber security of industrial control systems.
- Industrial safety practices, procedures, and signage.
- Etc.

As these assessments are performed, information is collected and usually documented in a Confidential Observation that attempts to capture the scope of the review and specific strengths and weaknesses identified. The Observations are then used to generate this report to be provided to the Customer via Counsel.

The inspection and review of the factory grounds and facilities, appropriate policies/procedures, and onsite activities revealed the following:

- 6 Strengths were identified.
- 15 Findings were identified with the following assigned risks:

Critical Risk	1
High Risk	3
Medium Risk	7
Low Risk	4

- 2 Informational Observations.

The details from the assessment and the associated strengths, findings and informational observations are contained herein. Overall, impressive actions were observed and in place to protect the employees at the factory; however, there are many opportunities for improvement that may not require extensive expense or capital costs.

Should you have any questions regarding the contents of this report, please direct your queries to Mr. Ernie Hayden, the Project Lead.

TABLE OF CONTENTS

INTRODUCTION & SCOPE

Acme Corporation owns and operates the Boondocks Fabrication Factory located at 12345 Boondocks Road, Nowhere, KS 66767 USA. The factory primarily manufactures widgets and derivative framitzes (pronounced “fram-it-ziz”) used in the farming and mining sector. The factory employs 290 personnel and is supported by multiple contractors and vendors as dictated by market requirements and associated production schedules.

After negotiating a Statement of Work for this effort with Boondocks management, it was agreed that the Consultant Team would inspect the factory and associated grounds and systems to identify risks/vulnerabilities requiring attention.

The inspection and assessment were performed the week of 24 to 28 February 2020.

SCOPE AND TYPE OF ASSESSMENT AND INSPECTIONS

The scope of the assessment included the following:

- Preparatory review of documentation, web sites, Google maps, etc. to better understand the factory and its physical presence in the State of Kansas and surrounding county.
- Physical inspection and walkdown of the factory building and grounds.
- Observation of activities in and around the factory including the following:
    - Receipt of Raw Materials.
    - Inspection and Processing of Raw Materials.
    - Production of multiple types of widgets and one line devoted to exclusive manufacturing of framitzes.
    - Observations of factory personnel performing crane operations, forklift operation, and high-elevation work (etc.).
    - Interviews with Factory staff.

    - Photographing key examples of strengths or evidence supporting findings and recommended areas for improvement.
- Some of the cyber effort included:
    - Password Management of Industrial Control System (ICS) Systems.
    - ICS Network Management.
    - ICS User Management.
    - ICS Software Management.
    - Network Patching and Vulnerability Management.
    - Remote Access to ICS Systems and Components.
- The general areas included in this review were as follows:
    - Physical and Cyber Access Control.
    - Building Exteriors.
    - Building Interiors.
    - Physical Plant Security and Access Control.
    - Communication Systems.
    - Emergency Operations Planning.
    - Fencing and Gates.
    - Procedures and Documentation.
    - Reporting Procedures.
    - Fire Safety.
    - Factory Security and Safety Culture.
    - Security Equipment.
    - Security Personnel.
    - Video Surveillance.
    - Employee, Contractor, and Visitor Registration and Management.
    - Etc.

- The Cyber assessment tools included use of the following:
    - Burp Suite Web Application Security Platform – Burp Suite is a package of tools for assessing modern web applications. Burp provides functionality for web spidering, scanning, and custom manipulation of web application inputs.
    - The Metasploit Framework – The Metasploit Framework is a platform for the development and execution of vulnerability assessments and exploit code. Metasploit contains exploit code for a variety of known vulnerabilities and is readily available as a free, open-source package.
    - Nessus Vulnerability Scanner – Tenable's Nessus Vulnerability Scanner is a tool used to automate vulnerability scanning against network assets. Nessus catalogs and tests targeted systems for known vulnerabilities.
    - Nmap – Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.
    - SSLScan – SSLScan queries SSL services, such as HTTPS, in order to determine the ciphers that are supported. SSLScan is designed to be easy, lean, and fast. The output includes preferred ciphers of the SSL service, the certificate and is in Text and XML formats.
    - Wireshark – Wireshark is a common packet analyzer that is used for network troubleshooting, analysis, software and communications protocol development, and education.
    - Snmpwalk – Snmpwalk is an Simple Network Management Protocol (SNMP) application that uses SNMP GETNEXT requests to query a network entity for a tree of information

- Enum4Linux – Enum4Linux is a tool for enumerating information from Windows and Samba systems using similar functionality to enum.exe. Written in Perl, Enum4Linux automates tasks using the Samba tools smbclient, rpclient, net and smblookup.

EXPLANATION OF RISK SEVERITY RATINGS

Each vulnerability identified in the assessment is accompanied by a discussion of its potential impact and recommendations for corrective action. Each vulnerability is assigned a ***qualitative*** estimate of the risk it represents to the factory's assets delineated as: critical, high, medium or low. These ratings are general estimates based on the Consulting Team's extensive experience in conducting risk assessments and vulnerability analyses. The level of risk for each vulnerability was determined through an assessment of the information obtained via the various phases of the assessment – especially from the Observations performed and documented. Both the likelihood of the threat occurring and the potential impact to the factory (should the threat occur) were considered in the risk analysis process.

Below is the classic risk equation this report relies upon:

RISK = THREAT X VULNERABILITY X CONSEQUENCE or IMPACT

Risk is a measure of the vulnerability's impact should it be exploited by a potential threat. For risk to exist there must be some likelihood that a threat exists, some potential impact if it should materialize, and a weakness in controls (i.e., vulnerability) that permits the threat to adversely impact the assets.

The equation above is the "classic" way to represent risk. As the reader can observe, risk is a consequence of the threat posed, the vulnerabilities that exist, and the associated consequences. During the course of this assessment the following Threats generally considered for this review of the factory included:

- Cyber Attacks – Especially on Industrial Control Systems and non-Information Technology (IT) Systems such as:
    - Building Systems Management (e.g., Heating, Ventilation and Air Conditioning)
    - Chilled Water Controls
    - Communications Systems
    - Elevator, Conveyor Belt, and Escalator Controls
    - Lighting

    - Warning and Alert Systems
    - Closed Circuit Television
    - Etc.
- Natural Hazards
    - Earthquakes (Natural or Due to Fracking)
    - Tornados
    - Major Flooding Events
    - Major Snow and Freezing Events
    - Range Fires
    - Lightning
    - Etc.
- Man-Made Threats
    - Individual
        - Outsider
        - Insider
        - Trusted Insider
        - Privileged Insider
    - Group
        - Ad hoc
        - Established
    - Organization
        - Competitor
        - Supplier
        - Partner
        - Vendor
        - Customer
    - Nation State

Examples of vulnerabilities that are an element of the Risk equation include such things as open and unlocked doors, unbadged/unaccounted for visitors, deteriorating fences, etc.

The table below – entitled Risk Matrix – depicts the logic of risk determination through a combination of the likelihood of occurrence of a particular threat and the potential impact if it were to occur. Though these separate factors are not listed individually for the risk ratings, it is important to understand that they form a basis for risk determination.

Impact → ---------- Likelihood ↓	Critical	High	Medium	Medium-Low	Low
Very Likely - Frequent	Critical	Critical	High	Medium	Medium
Likely - Probable	Critical	Critical	High	Medium - Low	Medium
Possible- Occasional	Critical	High	Medium	Medium – Low	Low
Infrequent - Remote	High	Medium	Medium	Low	Low
Rare - Improbable	Medium	Medium	Medium	Low	Low

Table 17 Risk Matrix

LIKELIHOOD OF OCCURRENCE

The likelihood that a threat will occur is shown on the left side of the table. The likelihood of occurrence is largely based on a combination of the natural and manmade threats and the architecture of the facilities/system, as modified by any existing protective measures.

For instance, an earthquake has a low likelihood of occurrence but could have a high impact.

CONSEQUENCE OR IMPACT

The other factor in determining risk is the potential impact that exploitation of the vulnerability would have to the factory. Here, potential impact ratings of critical, high, moderate, and low are used. Explanations of these impact conditions are described below:

- **Critical Potential Impact** – These are vulnerabilities that, if exploited, could severely and negatively impact business, operations, information, and reputation in a manner from which it would be difficult and potentially expensive to recover. Such impact would be catastrophic to the continued operation of the business.
- **High Potential Impact** – These vulnerabilities, if exploited, would seriously and negatively impact business and operations and would require significant effort and expense to repair or recover. Multiple instances of High Impact vulnerabilities could be catastrophic to the continued operation of the business.
- **Medium Potential Impact** – These are vulnerabilities that, if exploited, could moderately impact business and operations and may require some expense from which to recover.
- **Low Potential Impact** – These are vulnerabilities that, if exploited, could represent a minimal impact to business and operations and may not require any significant investment from which to recover.

The table below from the National Institute of Standards and Technology (NIST) ***Guidelines to Industrial Controls Security,*** (SP800-82 R2)***,*** **(**https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final), page 6-3, will give a reader a sense of what different levels of impact constitute.

Table 6-1. Possible Definitions for ICS Impact Levels Based on ISA99

Impact Category	Low-Impact	Moderate-Impact	High-Impact
Injury	Cuts, bruises requiring first aid	Requires hospitalization	Loss of life or limb
Financial Loss	$1,000	$100,000	Millions
Environmental Release	Temporary damage	Lasting damage	Permanent damage, off-site damage
Interruption of Production	Minutes	Days	Weeks
Public Image	Temporary damage	Lasting damage	Permanent damage

Table 18 From NIST SP800-82 R2

Overall, the reader is encouraged to view this matrix as a guide used by the Consultants when assigning the level of risk to a particular finding/observation. Also, the factory management team should use the resulting risk scores as a means of prioritizing level of effort to address each risk/finding. For instance, primary efforts and budgets should be focused on mitigating and correcting the Critical and High Impact vulnerabilities first.

STRENGTHS, FINDINGS AND RECOMMENDATIONS

Please be advised that some recommendations may refer to vendors and products. There is no intent to endorse any particular vendor or device. This is informational in nature.

STRENGTHS

Strengths identified during an assessment are those work practices, documentation, training or other business operations or performance characteristics that help the organization sustain a competitive edge in their market space. A Strength is also an attribute that would be beneficial to other organizations doing the same or similar work. Fundamentally, the Strength is viewed as a “good idea” or “good practice.”

Six strengths were identified by the Consulting Team during the assessment. These include the following:

###

S-1: Utilizing Attorney-Client Process for Security Vulnerability Identification and Communication

By using the Attorney-Client protection protocol, sensitive information regarding critical security issues affecting the factory are readily protected from casual or inadvertent disclosure. This is a unique approach to protecting such information and is rarely used in the security or critical infrastructure industry.

###

S-2: Extensive Management and Use of VLANs for Network Segmentation and Security

Although not all industrial control systems at the Factory are attached to the Enterprise Network, those systems using the Enterprise Network are segmented using an extensive array of Virtual Local Area Networks (VLANs). This is an excellent practice to segment traffic and separate data flows and control signals thus assuring improved system security.

###

S-3: Effective Use of System or Equipment "Decommissioned" Tags as Part of the Plant Industrial Safety Program

The factory operations and maintenance teams are often decommissioning old systems due to plant modifications and improvements. Rather than leave the decommissioned systems in a dangerous and unlabeled state, the Boondoggle team has developed a "Decommissioned Equipment" tagging process to ensure the systems remain de-energized and depressurized and are not inadvertently operated which could result in injuries and possibly death. An example of the tag is shown below:

To learn more about the decommissioned equipment tag process, please see the author's blog at:

http://infrastructuresecuritytoday.blogspot.com/2014/11/hazards-of-decommissioned-equipment.html

Figure 4 Decommissioned Equipment Tag

###

S-4: Seismic Pipe Hangers are Effectively Labeled Throughout the Factory

Seismic pipe hangers are effectively labeled and used throughout the factory proper.

Figure 5 Example of Seismic Pipe Hangers (Photo by Ernie Hayden))

###

S-5: Open Attitude Towards Improvement of the Factory's Security Posture

Interviews by the Consulting team with the factory control engineers, the maintenance manager, and the factory information technology security team showed a very positive attitude towards addressing and correcting major as well as minor ICS security issues identified during the course of the assessment.

###

S-6 Move Towards a Strategic Plan for Future ICS Network and Component Upgrades and Enhancements

Under the leadership of the factory maintenance manager the network control engineers are developing a strategic plan for the next 10+ years focused on factory production network and components upgrades. This effort is just starting but appears to be a useful foundation for planning and coordinating future factory upgrades and security vulnerability corrections and improvements. Additionally, by relying primarily on a single controls vendor –

Anderson Controls – this may be to the long-term benefit of Boondocks. It will assist the factory in avoiding increased network and component configuration issues when using a myriad of vendors' products and the associated device protocols.

FINDINGS

The following section contains descriptions of all findings related to the Factory security posture identified during the assessment as well as recommendations for mitigating any vulnerabilities where appropriate.

Critical Findings

Critical vulnerabilities create direct and immediate risk to the staff and students and can be exploited with readily available and public tools or with very little expertise. Issues that have been identified in this category should be given the highest level of remediation priority, as there may be an imminent risk to factory operations, safety and/or security.

One Critical Finding was identified during the assessment.

###

FINDING C-1: Overly Permissive Firewall Rule

The Risk Assessment Team discovered a firewall rule in the primary production network that allows packets from any source to any destination on any port. This rule is shown below in the figure below.

Rule	Active	Action	Protocol	Source	Src Port	Destination	Dst Port	Log
2	Yes		Any	Any	Any	Any	Any	N/A

Figure 6 Overly Permissive Firewall Rule

This rule could allow an attacker or malicious software to move easily through the network. The primary cyber consultant reviewed this rule with the firewall system administrator who deemed the access unnecessary and removed it from the ruleset.

RECOMMENDATIONS

1. We recommend a comprehensive review and analysis of all production and enterprise firewall rules be conducted to determine the appropriate level of access needed for each device and network and to identify rules that no longer have a business justification.

2. Once the appropriate level of access is defined, rule updates should be implemented in a phased and controlled manner to reduce the likelihood of unplanned loss of communication between devices or networks.
3. Annual firewall rule reviews should also be conducted to identify potential excessive access in the future.

ADDITIONAL INFORMATION

- "Best Practices for Firewall Rules," ***Liquid Web Website***, by Jennifer Walsh, April 24, 2020 https://www.liquidweb.com/kb/best-practices-for-firewall-rules/
- ***Guidelines on Firewalls and Firewall Policy*****,** US National Institute of Standards and Technology (NIST) Special Publication 800-41 Rev. 1, by Karen Scarfone, et al, September 2009 https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final

High Risk Findings

High-risk vulnerabilities create direct and immediate risk to the staff. Issues identified in this category should be given a high level of remediation priority, as there may be an imminent risk to factory operations.

Three High Risk findings were identified during the assessment.

###

FINDING H-1: Anderson Controls SysMet Building Controls System Requires Security Improvements

The Anderson Controls SysMet Building Controls System (SysMet) is a critical system used to manage the building heating/ventilation controls and many other key factory systems. SysMet is controlled from an engineering workstation located in the Control Room behind a locked door. Inspection of the cyber and physical deployment of the system revealed the following weaknesses that require attention:

- Investigation of the DHS Cybersecurity & Infrastructure Security Agency (CISA) Industrial Control Systems website (https://www.us-cert.gov/ics) revealed Advisory ICSA-XXX-YY-ZZZZ was issued on July 31, 2018. The Advisory noted that

SysMet version 8.0 and earlier had a cyber vulnerability where successful exploitation of this vulnerability could allow an attacker to obtain technical information about the SysMet server, thus allowing an attacker to target a system for attack.

- The SysMet engineering workstation is also connected to the Internet without separation by a Demilitarized Zone/Firewall. Ensuring that ICS controls are separated from the Internet is strongly advised to avoid the opportunity for direct connection from the Internet into a control system by an attacker.
- The SysMet configuration does not appear to be backed up. Anderson Controls may have a copy of the current configuration but that was not ascertained by the Consultant. This could be problematic if the system needed to be rebuilt following failure of the workstation hard drive and the backup configuration files are not available.

RECOMMENDATIONS

1. Immediately upgrade the current SysMet version to Version 9.0 or higher.
2. Remove any direct Internet connectivity from the SysMet Workstation.
3. Verify the current SysMet configuration is backed up, a copy of the current configuration is on file and securely stored – preferably off site in a secure storage facility. Ensure the SysMet configuration is backed up every time the system is modified and the backup files are maintained on site and with the Anderson Controls vendor offsite. Consider storing the backup files offsite in a secure facility (e.g., digital tape storage, documentation storage, etc.) for security and easy retrieval in an emergency.

ADDITIONAL INFORMATION

- DHS CSIA, Advisory ICSA- XXX-YY-ZZZZ, Anderson Controls SysMet, issued July 31, 2018
- NIST 800-82 R2, *Guide to Industrial Control Systems (ICS) Security*, May 2015

###

FINDING H-2: Physical Key Management Requires Immediate Attention

A brief review of the physical key management process was performed by the Consultant team. Several concerns were raised during this inspection and included:

- The last key audit was performed in 2015. Thus, there is lack of current awareness of missing keys and which doors/locks are highly insecure due to the number of uncontrolled keys.
- A master file of the keys and locks is maintained in the Director of Operations and Security office. There is only one copy of this document which also includes hand-written notes and updates. The assigned contract locksmith does not have a copy of this file. This document is extremely important to the current security of the Factory.
- A key management and assignment system has been partially implemented in Excel; however, it is not up to date and there are many former employees/contractors identified who have not turned in their keys upon departure.
- The Command Center does not possess any “master” keys for lockable control boxes such as Fire Control, Access Control, etc.

RECOMMENDATIONS

1. Immediately make a paper and digital copy of the Master key/lock file. Securely store the paper copy and digital copy off site in order to have an up-to-date duplicate should the Master key/lock document be damaged, lost or stolen.
2. Perform a key audit. Identify those doors and locks that are most susceptible to being opened by an “uncontrolled key.” Change the locks for the most vulnerable doors and locks.
3. Implement a digital system to manage lock/key assignment, distribution, return, disposal, damage, etc. Consider implementing as part of the factory maintenance management software system being rolled out.
4. Ensure the Control Room has access to the important and critical keys necessary for emergency response in the factory.

5. Ensure that keys are recovered under the following circumstances:
    - Employee quits or is terminated and fails to return keys at the time of their departure.
    - Employee fails to return to work and is terminated but keys are never retrieved.
    - Employee leaves company and turns keys in to departmental supervisor or manager. Keys are kept in department and never returned to person responsible for managing the key system.
    - Employee is promoted or transferred to another department or site and is issued keys for new job but fails to return keys from previous job.

ADDITIONAL INFORMATION

- "Key Control and Lock Security Checklist," by John E. Hunter from ***Effective Physical Security,*** page 154, by Lawrence J. Fennelly.

###

FINDING H-3: Bridge Between Production and Enterprise Networks

A computer in the Framitz Packaging Office was identified as being "dual-homed." In this case the computer is connected to both the factory production network and the Boondocks enterprise IT network. And, with some added testing by the Consultants it was ascertained that the computer could readily access the Internet without being protected by a firewall or demilitarized zone (DMZ). Therefore, this configuration could not only pass network traffic from one network to another but the components and systems on the production network were subject to scanning and attacks directly from the Internet.

This computer was apparently configured to allow SAP traffic to traverse to and from the production network; however, there did not appear to be any port or protocol filters in place or any firewalls to better secure this traffic. Also, this configuration was not apparently approved by Security or Engineering.

During interviews it was revealed that there are no written or specified prohibitions against direct connections between the production and

enterprise networks or any uncontrolled/unauthorized connections to the production network.

Figure 7 Dual-Homed PC Configuration

RECOMMENDATIONS

1. Due to the high-risk nature of this configuration immediate actions are recommended to break this direct connection between the Production and Internet as well as any Enterprise Networks. No systems other than firewalls should be configured as dual-homed to span both the production and enterprise networks. All

connections between the production network and enterprise network should be through a firewall. Production control systems and computers should never have direct connection to the Internet.

ADDITIONAL INFORMATION

- ***Guide to Industrial Control Systems (ICS) Security***, National Institute of Standards and Technology (NIST) Special Publication 800-82, Revision2 (http://dx.doi.org/10.6028/NIST.SP.800-82r2)

Medium Risk Findings

Medium severity vulnerabilities create an immediate risk to the onsite staff, which may or may not be direct in nature. An elevated level of factory access may be required to leverage such vulnerabilities. Issues that have been identified in this category should be given a high level of remediation priority, based upon the specific determined exposure.

Seven Medium Risk findings were identified during the assessment.

###

FINDING M-1: Access Control to Some Critical Spaces Needs Improved Security

Tours of the factory generally revealed most critical spaces were locked; however, there were a few instances where unauthorized access to critical areas could occur. One example includes the following:

- When examining the architecture of the factory office building there are many spaces such as telecom and electric distribution rooms that are only key-locked and are not controlled by an access control key card. With Finding H-3, Physical Key Management, there is concern that these rooms are not highly protected with their key control alone. By having each door with a key card control, access to the room can be more disciplined and more readily turned off for terminated employees/contractors/vendors.

RECOMMENDATION

1. Review the current list of “critical rooms” and install key card access control for the telecom and electrical distribution rooms. Consider installing key card access control on most doors in the factory.

ADDITIONAL INFORMATION

- None

###

FINDING M-2: Multiple Open and Unsecure Critical System Control and Power Boxes Exist in the Factory and Require Improved Security

Throughout the Factory there are many open and unsecure critical system control boxes. Some of these boxes have a key lock installed but they are not being used to secure the door closed. One substantial concern is many Access Alarm and Control boxes were found open, unlocked and/or the locks were missing.

A photographic example of these important and open cabinets is shown below:

Figure 8 Open/Unlocked Control Cabinets

RECOMMENDATIONS

1. Improve the conduct of maintenance to ensure that all control boxes are closed and locked/secured when work is not in progress.
2. Ensure that keys are available in the Control Room for the various lockable control cabinets/boxes.

ADDITIONAL INFORMATION

- None

###

FINDING M-3: Potential Unauthorized Wireless Access Points

The Consultants conducted an internal and external wireless (802.11x) survey of the Boondocks factory campus and determined that the company does not have a robust capability to detect rogue wireless access points connected to the Production Network.

The assessment consisted of automated scanning and analysis in order to identify existing wireless networks and any weaknesses associated with them that may create risk for client assets, and Boondocks as an organization. The Consultants used a variety of software at each location to identify and locate wireless networks. In addition to software monitoring, the Consulting team employed the use of a Global Positioning System (GPS) antenna in order to map the estimated location of each WiFi network when possible.

During the course of the assessment, the Consultants discovered 14 unique wireless network SSIDs, eight of which are confirmed to belong to Boondocks. While some of the other networks likely belong to on-site printers and projectors installed at the factory, there are a few SSIDs that clearly belong to individual mobile hotspots, likely brought on-site by contractors or employees.

Of the 14 unique SSIDs, six were not protected by any authentication or encryption. This does not include the BoondocksGuest network, which is open by design

While Boondocks cannot easily control the existence of wireless networks nearby and outside the fence line of the factory, these networks can present a threat in that they can potentially allow internal users to circumvent network controls while accessing the Internet. Users wishing to stand up their own networks to simply get to the Internet may be unknowingly providing an uncontrolled and unmonitored “backdoor” into sensitive networks.

RECOMMENDATIONS

1. Boondocks is encouraged to implement network security policies that clearly forbid users from accessing the Internet through networks and media that are not controlled or authorized by the company while they are utilizing Boondocks information assets.
2. Once these policies are in place, it is also recommended that Boondocks personnel conduct periodic wireless surveys similar to

the one described above in order monitor adherence to those policies.

ADDITIONAL INFORMATION

- ***Guidelines for Securing Wireless Local Area Networks***, National Institute of Standards and Technology (NIST) Special Publication 800-153 (http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf)
- ***Guide to Securing Legacy IEEE 802.11 Wireless Networks***, National Institute of Standards and Technology (NIST) Special Publication 800-48, Rev 1 (http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf)

###

FINDING M-4: Vendor Cybersecurity Management

Interviews with factory control engineers and other security staff revealed that controls over the cyber activities for onsite vendors and contractors are insignificant. Examples noted include the following:

- Prior to attaching to the factory networks, vendor computers, USB drives, and test equipment are not tested for malware or are not verified to be malware-free and the anti-malware software is up to date. This practice could lead to a factory vendor accidentally or maliciously contaminating the production or enterprise networks due to the vendor's equipment containing malware.
- Vendors often send system patches and updates to the factory control engineers via mail in USB drives. The drives are not checked for malware before they are attached to the production network.
- The XYZ controls network is currently under construction at the factory. An interview with factory construction management revealed there is no formal turnover of the XYZ controls network configuration and associated details to the factory control engineers. Hence, any future controls troubleshooting efforts would be hampered by the factory control engineers not being

aware of the details of the newly installed controls or even their system set points, idiosyncrasies, etc.

RECOMMENDATIONS

1. Develop, implement, and enforce a policy and supporting procedures that vendors shall not connect to the factory production or enterprise network without first verifying that there is no malware present on the connecting devices and that the devices are patched and up to date thus minimizing Boondocks network contamination.
2. Develop, implement, and enforce a policy and supporting procedures that all portable media must be checked for malware prior to connecting to the production network. This includes vendor-provided USBs as well as contractor-owned devices and employee-owned devices.
3. On a periodic basis (suggest monthly) verify that portable media and laptops used to troubleshoot factory-installed production controllers and supporting devices are checked for malware and anti-virus/patching updates as appropriate and before use.
4. Establish and implement a formal method of production system turnover from the vendor/contractors to the plant network controls engineers to ensure the factory personnel are aware of set points, configurations, vendor contacts, vendor manual availability, etc.

ADDITIONAL INFORMATION

- ***Guide to Industrial Control Systems (ICS) Security***, National Institute of Standards and Technology (NIST) Special Publication 800-82, Revision2 (http://dx.doi.org/10.6028/NIST.SP.800-82r2)

Department of Homeland Security: Cyber Security Procurement Language for Control Systems, US Department of Homeland Security, September 2009 (https://www.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf)

###

FINDING M-5: Staff and Contractor Termination Process Is Incomplete and Requires More Follow-Through

Interviews with security management and the Human Resources Director revealed that the staff and contractor termination process needs improvement. In particular there was evidence that critical materials were not returned to the factory by the terminated staff. These items included in some cases keys, key cards, and laptop computers. Additionally, computer access was not turned off for the departing individuals until several days after the event due to lack of notification of Security/Information Technology by Human Resources.

RECOMMENDATIONS

1. Work closely with Human Resources to ensure that personnel terminations, retirements, resignations, etc. are closely handled to ensure that materials such as keys, key cards, laptop computers, etc. are returned and that computer access is turned off within hours of the individual's departure.

ADDITIONAL INFORMATION

- ***Effective Key Management Procedures****,* Silva Consultants http://www.silvaconsultants.com/effective-key-management-procedures.html
- ***Termination Checklist*****,** Society for Human Resource Management (SHRM) https://www.shrm.org/resourcesandtools/tools-and-samples/hr-forms/pages/termination_exitinterviewchecklist.aspx

###

FINDING M-6: PASSWORD MANAGEMENT

Password management for the production network needs added discipline and improvement. Handwritten user names and passwords were observed written inside control system cabinets at the factory (please see photo below). The master password list maintained by the senior controls engineer is in an Excel spreadsheet that may be accessible to other unauthorized personnel due to its unprotected placement on the enterprise network. Also, the only password complexity and rotation rules are applied to the production network Active Directory instance; however, other device component passwords are not complex and not periodically changed. Lastly it appeared that some device

passwords were not changed from the factory default or were simple “admin-admin” user name/password pairs.

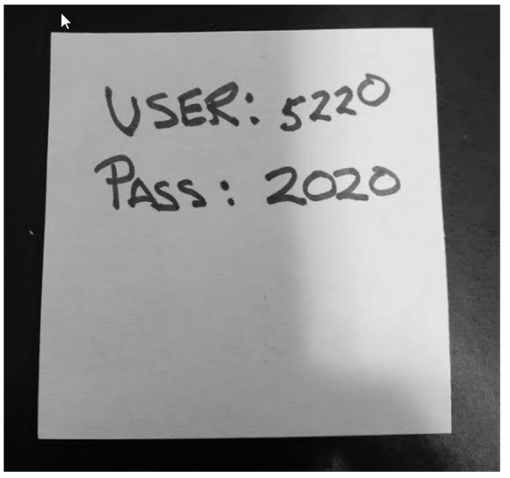


Figure 9 "Yellow Sticky" On Factory Control Cabinet

RECOMMENDATIONS

Computer systems in ICS environments typically rely on traditional passwords for authentication. Control system suppliers often supply systems with default passwords. These passwords are factory set and are often easy to guess or are changed infrequently, which creates additional security risks. Also, protocols currently used in ICS environments generally have inadequate or no network service authentication.

Key recommendations for Boondoggle are:

1. Remove posted passwords on system equipment/components and stop this practice,
2. Ensure default passwords are changed now and for future new equipment installations, and
3. Store any copies of the master passwords in a very secure location with limited access.

ADDITIONAL INFORMATION

The following are general recommendations and considerations with regards to the use of passwords from NIST 800-82, ***Guide to Industrial Control Systems (ICS) Security***:

1. Ensure default passwords have been changed.
2. The length, strength, and complexity of passwords should balance security and operational ease of access within the capabilities of the software and underlying operating system.
3. Passwords should have appropriate length and complexity for the required security. In particular, they should not be able to be found in a dictionary or contain predictable sequences of numbers or letters.

###

FINDING M-7: Lack of Formalized Documentation

The consultants discovered many of the policies, processes and procedures proscribed by industry best practices are functionally in place but are not formally documented or implemented evenly across the Boondocks environment. The following are policies, processes or procedures not formally documented or consistently implemented:

- Account provisioning/de-provisioning processes.
- Change management processes for significant system changes.
- Cyber security incident response procedures.
- Cyber equipment disposal procedures.
- Log review and rotation procedures.
- Lost or stolen removable media reporting processes.
- Patching processes.
- Removable media use policy.

Comprehensive operational, system, and organization documentation demonstrates the commitment of the organization to consistently review, measure, and ultimately ensure progress towards a stated goal. In terms of security controls comprehensive documentation ensures a stable, safe, and secure environment where all responsibilities, requirements and needs are clearly defined and regularly reviewed for effectiveness.

RECOMMENDATIONS

1. Perform a comprehensive review of all existing Boondocks security-related system documentation to identify where documentation gaps exist in addition to those listed above.
2. Identify areas where security-related documentation is lacking and correct deficiencies through the development and socialization of policies, processes, procedures, or other system documentation artifacts.
3. Maintain all security-related documents in a secure manner befitting the information they contain. Only the appropriate users should have access to the documents.
4. Maintain the security-related documents in a centralized repository that is regularly backed up according to Boondocks' standards and policies.

ADDITIONAL INFORMATION

- "Guidelines for Security Documentation," ***Australian Government Security Information Manual***, May 2020 (https://www.cyber.gov.au/sites/default/files/2020-05/06.%20ISM%20-%20Guidelines%20for%20Security%20Documentation%20%28May%202020%29.pdf)

Low Risk Findings

Low severity may or may not be direct in nature, as an elevated level of initial access is often required to leverage such vulnerabilities. While findings classified as low severity do not present an imminent threat to the factory, customers, contractors, staff, or visitors, they should not be ignored.

Four Low Risk Findings were identified.

###

FINDING L-1: Lighting

Generally, Boondocks facility lighting appeared to be satisfactory with the following notable exceptions:

- Two light stanchions at the incoming 230 kV Center Substation from Kansas Power & Light were not completely restored following apparent maintenance. The wires for the lighting were exposed to the elements and may prematurely fail due to environmental exposure. Photos of the two stanchions are shown below:

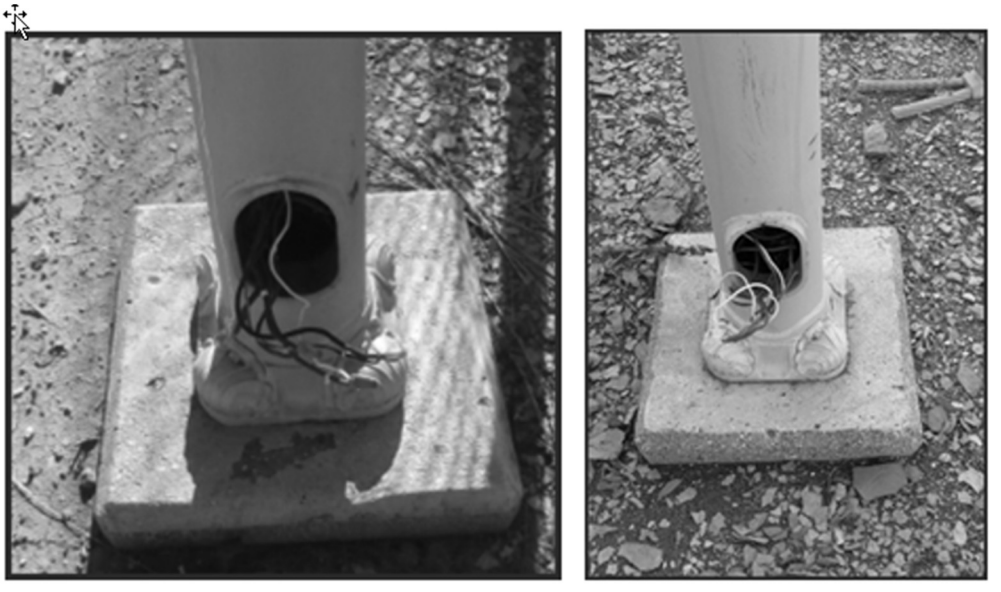


Figure 10 Light Stations Inside 230kV Substation (Photo by Ernie Hayden)

- During a nighttime survey of the Boondocks facilities, two lights in the main parking lot and one light at the east end of the main warehouse were not lit. It appeared the timer for the lights was not correctly set because the parking lot lights were on the following morning when arriving back at the factory site.
- Some of the emergency light boxes tested in the hallways of the Boondocks factory offices did not light when the test button was depressed.
- Three lights on an eastward stanchion for the railway spur/yard were not connected to the power supply and did not light up when all site lights were powered.

RECOMMENDATION

1. Correct the identified issues noted above and consider establishing a preventive maintenance program to check for plant and facility lighting at least annually.

ADDITIONAL INFORMATION

For future lighting surveys and assessments, consider the following checklist:

- ☐ Is the perimeter of the installation protected by lighting?
- ☐ Does protective lighting provide a means of continuing during the hours of darkness the same degree of protection available during the daylight hours?
- ☐ Are the cones of illumination from lamps directed downward and away from the facility proper and away from guard personnel?
- ☐ Are lights mounted to provide a strip of light both inside and outside the fence?
- ☐ Is perimeter lighting used so that guards remain in comparative darkness?
- ☐ Are lights checked for proper operation prior to darkness?
- ☐ Are repairs to lights and replacement of inoperative lamps performed immediately?
- ☐ Do light beams overlap to provide coverage in case a bulb burns out?

- ☐ Is additional lighting provided at active gates and points of possible intrusion?
- ☐ Are gate guard shacks provided with proper illumination?
- ☐ Are light-colored finishes (e.g., white) or stripes used on lower parts of buildings and structures to aid guard observation and quickly identify silhouettes?
- ☐ Does the facility have a dependable source of power for its lighting system?
- ☐ Does the facility have a dependable auxiliary source of power?
- ☐ Is the protective lighting system independent of the general transit facility lighting or power system?
- ☐ Is the power supply for lights adequately protected?
- ☐ Is there provision for standby or emergency lighting?
- ☐ Is the standby or emergency equipment tested frequently?
- ☐ Is emergency equipment designed to go into operation automatically when needed?
- ☐ Is wiring for protective lighting properly mounted?
- ☐ Is it in tamper-resistant conduits?
- ☐ Is it mounted underground?
- ☐ If above ground, it is high enough to reduce possibility of tampering?
- ☐ Are switches and controls properly located, controlled, and protected?
- ☐ Are they weatherproof and tamper resistant?
- ☐ Are they readily accessible to security personnel?
- ☐ Are they located so that they are inaccessible from outside the perimeter barrier?
- ☐ Is there a centrally located switch to control protective lighting?
- ☐ Is adequate lighting for guard use provided on indoor routes?
- ☐ Are materials and equipment in shipping and storage areas properly arranged so as not to mask security lighting?

The following references may also be useful for this effort:

- ***Guideline for Security Lighting for People, Property, and Public Spaces***, IESNA G-1-03, by the Illuminating Engineering Society https://www.ies.org/product/security-lighting-for-people-property-and-critical-infrastructure/
- ***Physical Security Field Manual No. 3-19.30***, US Army, January 2001 https://www.wbdg.orghttps://www.wbdg.org/FFC/ARMYCOE/FIELDMAN/fm31930.pdf/FFC/ARMYCOE/FIELDMAN/fm31930.pdf
- ***Site and Urban Design for Security FEMA 430***, Arnold, Christopher and Lasch,Mary Ann, December 2007 http://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf

###

FINDING L-2: Inadequately Secured Door Locks

Multiple doors on the outside of the Boondocks office building can be easily “picked” to open if locked. All perimeter doors do not have any anti-pick protection.

RECOMMENDATION

For all doors, consider inclusion of a lock guard (see photo below) for consistent and hardened protection of door latches to prevent picking the latch for unauthorized entry.

Figure 11 Latch Guard Installation (Photo by Ernie Hayden)

ADDITIONAL INFORMATION

None

###

FINDING L-3: A Process to Identify and Monitor Temporary Modifications is Needed

In at least two instances, a temporary cable was installed and ran across a door frame or across a control cabinet seal. These cables were not marked or identified to demonstrate they were authorized and their purpose. Also, these cables are positioned where they could be cut and lead to an electric shock to an individual during door opening and closing.

Figure 12 Cable Running Across Door Threshold (Photo by Ernie Hayden)

RECOMMENDATIONS

1. Avoid running wires across door thresholds to minimize shock hazards.
2. If these are intended to be temporary modifications, consider tagging the wires/cables to show the modification is authorized by operations and the control room and the name of the “owner” is by name and phone number. Also consider including an “expiration date” to avoid allowing the “temporary modifications” to become permanent.

ADDITIONAL INFORMATION

None

###

FINDING L-4: Incorrectly Directed Barbed Wire

During a tour of the Boondoggle Factory perimeter fence it was observed that the top barbed wire assembly was facing towards the plant and not towards the threat as recommended by industrial security practices.

Figure 13 Perimeter Fence Barbed Wire Top Cap Facing the Wrong Direction – Facing Away from the Threat (Photo by Ernie Hayden)

RECOMMENDATION

1. During upcoming fence repairs, redirect the top barbed wire towards the threat (i.e., facing away from the plant).

ADDITIONAL INFORMATION

- ***Physical Security Field Manual No. 3-19.30***, US Army, January 2001
  https://www.wbdg.org/FFC/ARMYCOE/FIELDMAN/fm31930.pdf
- ***Security Fences and Gates***, United Facilities Criteria (UFC), US Department of Defense, October 1, 2013
  https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-022-03

INFORMATIONAL OBSERVATIONS

Informational observations are simply included in order to convey more information that may be useful from a security perspective. They do not necessarily present any threat nor will they warrant a remediation or recommendation. They are included for completeness.

Four Informational Observations were identified.

###

INFO-1: Blocked Access to Some Fire Extinguishers and Some Components

During the observations of the factory activities and rooms the Consultants observed many instances of blocked fire extinguishers and components. Blocking these items can lead to delayed emergency response at a minimum.

Photographic examples of some blocked fire extinguishers and a key circuit breaker panel are shown below:

Figure 14 Blocked Fire Extinguisher (Photo by Ernie Hayden)

Figure 15 Blocked Circuit Breaker Panel (Photo by Ernie Hayden)

RECOMMENDATIONS

1. Ensure all fire protection equipment on the Boondocks campus is not blocked at any time. Consider painting a yellow “keep clear” box on the floor adjacent to the hanging fire extinguisher, hose reel, etc.
2. Ensure access to electrical circuit breakers and panels is kept clear for a minimum of 30 inches.

ADDITIONAL INFORMATION

- “Fire Extinguisher Keep Clear Stencil” https://www.accuform.com/Plant-Facility/floor-marking-stencils---fire-extinguisher-keep-area-clear-PMS325
- 30 Inch Minimum Clearance from Circuit Breakers https://www.ecmag.com/section/codes-standards/working-space#:~:text=To%20be%20on%20the%20safe,6%C2%BD%20feet%20of%20headroom%20space

###

INFO-2 — No Hearing Protection Required Signs in Diesel Generator Room

There are no “Hearing Protection Required” signs or warnings in the diesel generator room. This is required by the Occupational Safety and Health Administration (OSHA) when the diesel is running.

RECOMMENDATION

1. Install signs requiring hearing protection when the diesel is running.
2. Enforce wearing hearing protection during diesel operations.

ADDITIONAL INFORMATION

- US Occupational Safety and Health Administration (OSHA) Noise Exposure Guidelines https://www.osha.gov/SLTC/noisehearingconservation/

INDEX OF TABLES

TABLE OF FIGURES

DOCUMENT CHANGE CONTROL

Version	Date	Author	Notes/Explanation
V0	5/24/20	Ernie Hayden	Initial Draft
V0.1	5/25/20	Adam Smith	Initial Review
V0.2			QC/QA Review
V1			Customer Initial Review
Final			Final Issue

ATTACHMENTS

ATTACHMENT A – KEY DOCUMENTS REVIEWED, REFERENCED

"Best Practices for Firewall Rules," ***Liquid Web Website***, by Jennifer Walsh, April 24, 2020 https://www.liquidweb.com/kb/best-practices-for-firewall-rules/

"Guidelines for Security Documentation," ***Australian Government Security Information Manual***, May 2020 (https://www.cyber.gov.au/sites/default/files/2020-05/06.%20ISM%20-%20Guidelines%20for%20Security%20Documentation%20%28May%202020%29.pdf)

Department of Homeland Security: Cyber Security Procurement Language for Control Systems, US Department of Homeland Security, September 2009 (https://www.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf)

Effective Key Management Procedures*,* Silva Consultants http://www.silvaconsultants.com/effective-key-management-procedures.html

Five Best Practices to Improve Building Management Systems (BMS) Cybersecurity, by Gregory Strass and Jon Williamson, Schneider Electric (Link http://acscompanies.com/download/attachment/11350)

Guide to Industrial Control Systems (ICS) Security, May 2015, US National Institute of Standards and Technology (NIST) Special Publication SP800-82 R2

Guide to Securing Legacy IEEE 802.11 Wireless Networks, National Institute of Standards and Technology (NIST) Special Publication 800-48, Rev 1 (http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf)

Guideline for Security Lighting for People, Property, and Public Spaces, IESNA G-1-03, by the Illuminating Engineering Society

https://www.ies.org/product/security-lighting-for-people-property-and-critical-infrastructure/

Guidelines for Securing Wireless Local Area Networks, National Institute of Standards and Technology (NIST) Special Publication 800-153 (http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf)

Guidelines on Firewalls and Firewall Policy**,** US National Institute of Standards and Technology (NIST) Special Publication 800-41 Rev. 1, by Karen Scarfone, et al, September 2009 https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final

Noise Exposure Guidelines, US Occupational Safety and Health Administration (OSHA) https://www.osha.gov/SLTC/noisehearingconservation/

Physical Security Field Manual No. 3-19.30, US Army, January 2001 https://www.wbdg.org/ccb/ARMYCOE/FIELDMAN/fm31930.pdf

Security Fences and Gates, United Facilities Criteria (UFC), US Department of Defense, October 1, 2013 https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-022-03

Site and Urban Design for Security FEMA 430, Arnold, Christopher and Lasch,Mary Ann, December 2007 http://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf

Termination Checklist**,** Society for Human Resource Management (SHRM) https://www.shrm.org/resourcesandtools/tools-and-samples/hr-forms/pages/termination_exitinterviewchecklist.aspx

ATTACHMENT B – LIST OF KEY PERSONNEL INTERVIEWED

- Adam Smith, Chief Technology Officer
- Frank Smith, Production Engineer
- Graham Smith, Security Manager
- Howard Smith, Executive Vice President & General Counsel
- Hugo Smith, Director of Risk Management
- Jackie Smith, Director, Sustainability & Operations
- John Smith, Director, Operations & Facility Services
- Kenny Smith, Director, Security
- Mark Smith, Maintenance Manager
- Oscar Smith, Field Electrician

INDEX

Boxes, figures, and tables are indicated by b, f, and t following the page numbers.

Q

R

S

T

Z

ABOUT THE AUTHOR

Ernie Hayden, **MIPM, CISSP, CEH, GICSP(Gold), PSP** is a highly experienced and seasoned technical consultant, author, speaker, strategist, and thought-leader with extensive experience in the critical infrastructure protection/security domain, industrial controls security, cybercrime, cyberwarfare, and physical security areas. His primary emphasis is on offering expert advice and commentary on performing risk assessments of industrial controls, energy supply, and chemical/oil/gas/electric grid security, with special expertise on CIP-014-2 – Physical Security of Substations, and risks of commercial drones to critical infrastructure.

Hayden is currently the founder and principal of 443 Consulting, LLC. He has held roles as the Chairman, President, and CEO of MCM Enterprise – an advanced sensor company; industrial control security lead at Jacobs Engineering & Technology and BBA Engineering; executive consultant at

Securicon LLC; and information security officer/manager at the Port of Seattle, Group Health Cooperative (Seattle), ALSTOM ESCA, and Seattle City Light.

Ernie was a commissioned officer in the US Navy nuclear program and was on the commissioning crew of the USS Texas (CGN-39). For the first 25 years of his civilian life Ernie worked in the commercial nuclear arena as a technical manager at Westinghouse Electric, the Institute of Nuclear Power Operations (INPO), the Trojan Nuclear Plant, and the Electric Power Research Institute (EPRI).

Ernie is an accomplished writer and frequent author of blogs, opinion pieces, and white papers. He is an invited columnist for the "Ask the Experts" discussions on TechTarget-SearchSecurity. Other thought-leadership articles have included authoring a chapter on "Cybercrime's Impact on Information Security," in the Oxford University Press Cybercrime and Security Legal Series and several articles in Information Security Magazine including his original research on data lifecycle security and an article on data breaches in the same publication. Hayden has been quoted in DarkReading.com, the Boston Globe, Symantec Blog, and other major media outlets.

Ernie is a very active contributor in global security forums. He is currently a member of the European Union Network and Information Security Agency (ENISA) Stakeholder Board on Industrial Controls Security and was an invited contributor to the Caspian Strategy Institute (Hazar) (Turkey). He has been an instructor, curriculum developer, and advisor for the University of Washington Information System Security Certificate program in Seattle. Additionally, Ernie has been a contract instructor for the Cyberterrorism Defense and Analysis Center, sponsored by the U.S. Department of Homeland Security.

Ernie holds several cyber and physical security certifications including a CISSP - Certified Information Systems Security Professional, Certified Ethical Hacker (CEH), GICSP – SANS Global Industrial Cyber Security Professional (GICSP) with "Gold" designation and holds the ASIS Physical Security Professional (PSP) certification. He received a Master's Degree in Infrastructure Planning & Management (MIPM) in 2015 and a Bachelor's

Degree in Business Administration (with International Business emphasis) in 1974, both from the University of Washington in Seattle. He is a graduate of the FBI Citizens Academy, Seattle Police Department Citizens Academy, US National SCADA Test Bed (NSTB) SCADA Security Course, and Center for Creative Leadership – Leadership Development Program. He is also a member of the Western Washington Chapter of Infragard. In early 2018, Ernie was recognized by Indegy Consulting in its article "10 Industrial Cyber Security Influencers Offer Expert Insights for 2018."

Ernie is married to Ginny Pausch Hayden and they have a daughter Karina. Ernie and Ginny and their Corgi Meghan live in Anacortes, Washington in the San Juan Archipelago in northern Puget Sound. In his spare time Ernie is also an accomplished photographer taking photographs of landscapes and wildlife.