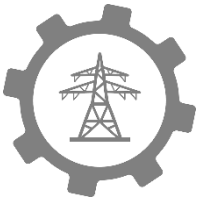
Critical Infrastructure Risk Assessment

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

EXCERPT

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

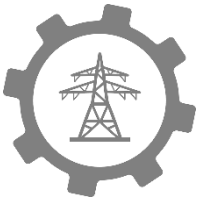
Partner, Fortium Partners

"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!

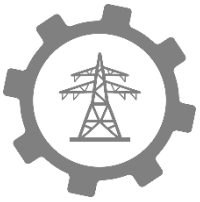
Acknowledgements

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

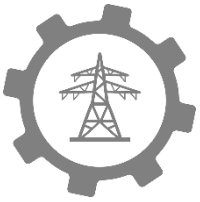
CISO (retired)

University of Washington

Seattle, Washington

x

EXCERPT



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.

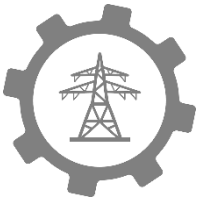
As the need for risk management becomes more apparent in organizations, this book should be in the library of every risk manager as well as every consultant performing risk assessments of critical infrastructure facilities – not on the shelf, but on the desk as a regular desk reference.

Peter Gregory

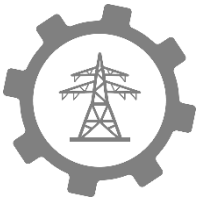
CISM, CISA, CIPM, CRISC, CISSP, CCSK, CCISO, QSA

Seattle, Washington

EXCERPT



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:

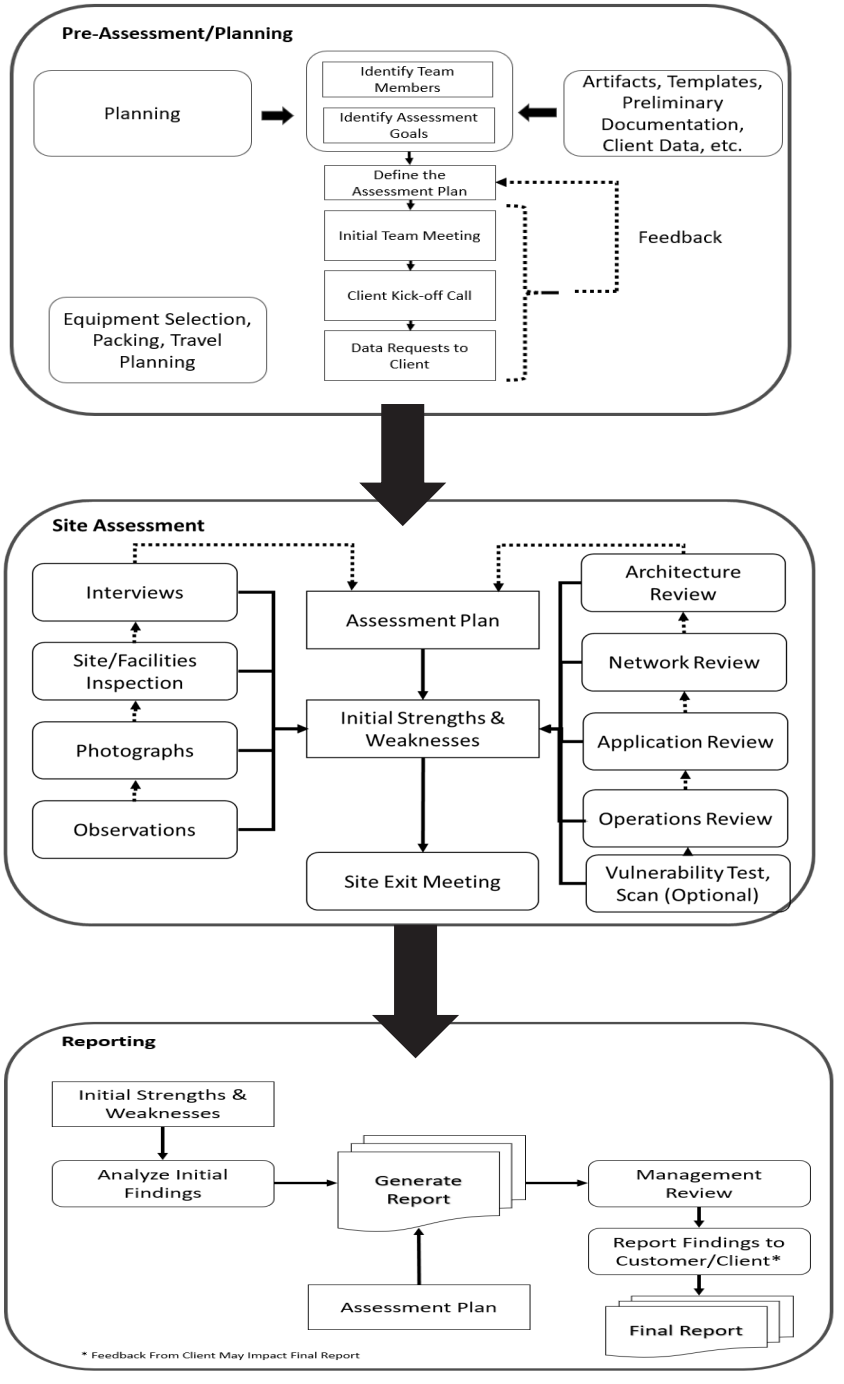


Figure 0-2 Hybrid Facility Risk Analysis Flow Chart

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

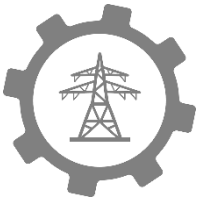
Biss, E. (2020). Eula Biss - Some of the most interesting research that I... Retrieved April 14, 2020, from https://www.brainyquote.com/quotes/eula_biss_724462

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



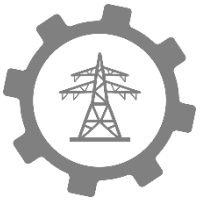
PART I
FOUNDATIONS

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 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.

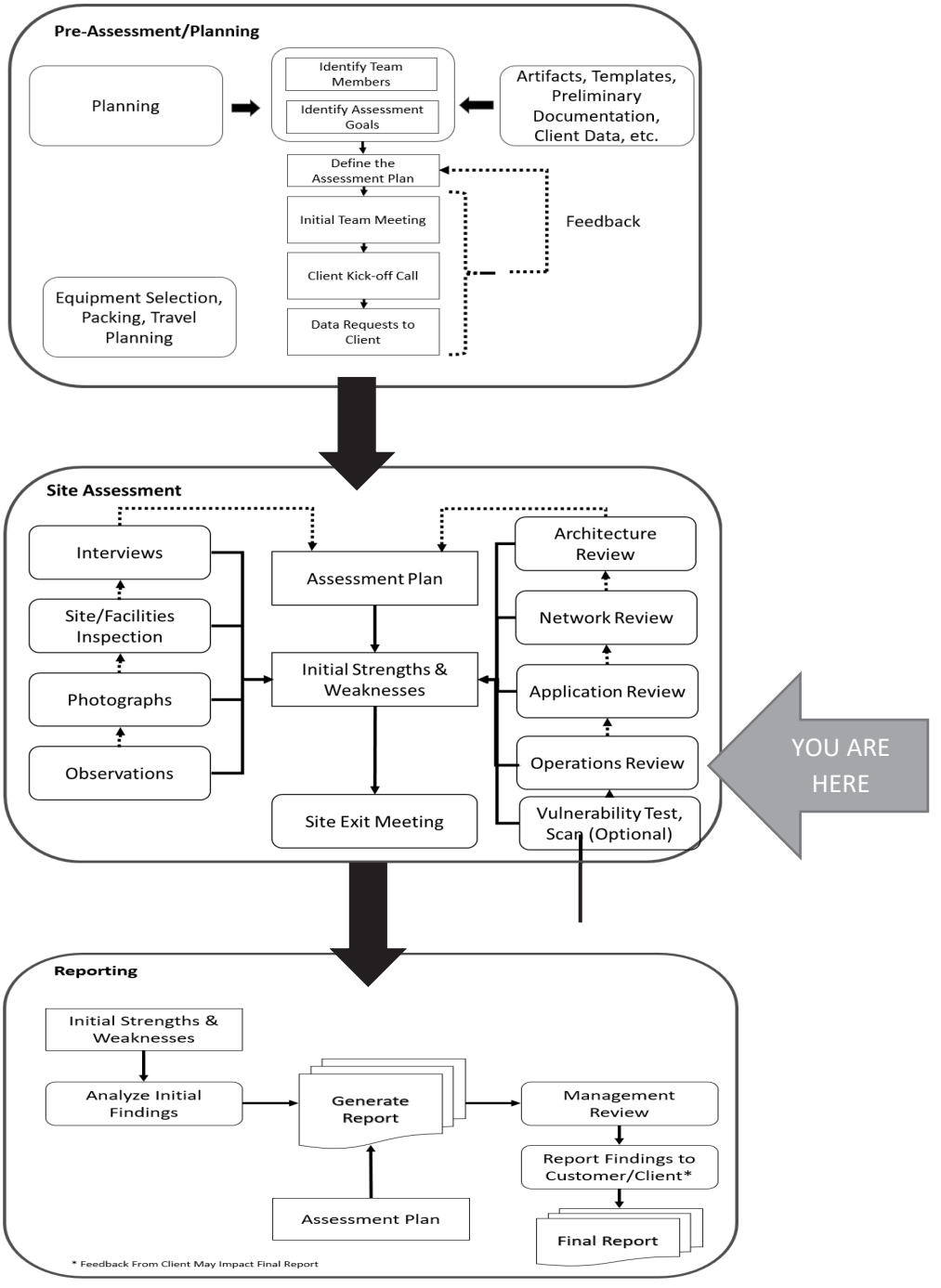


Figure 5-1 Hybrid Facility Risk Analysis Flow Chart

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:

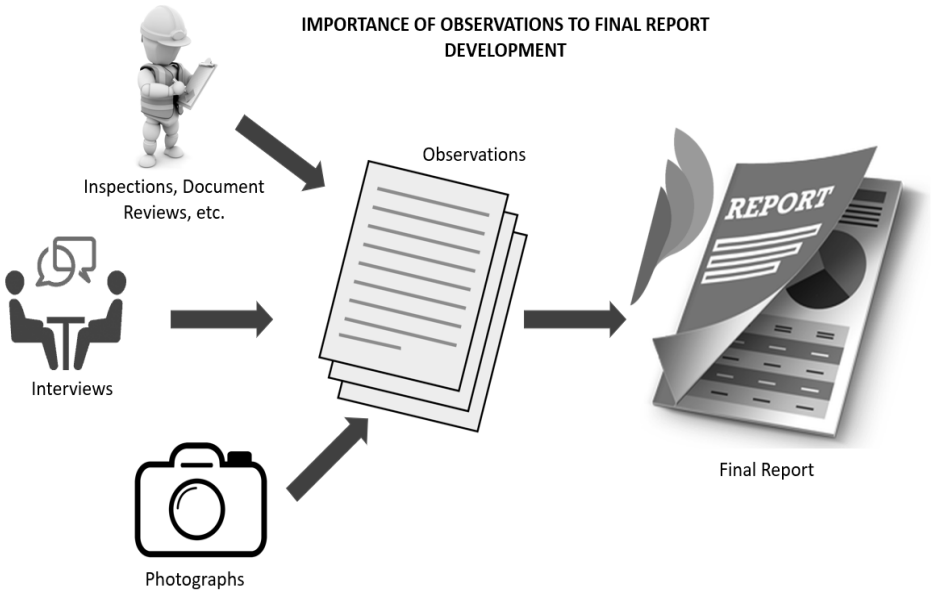


Figure 5-2 Contribution of Observations to the Final Report

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:

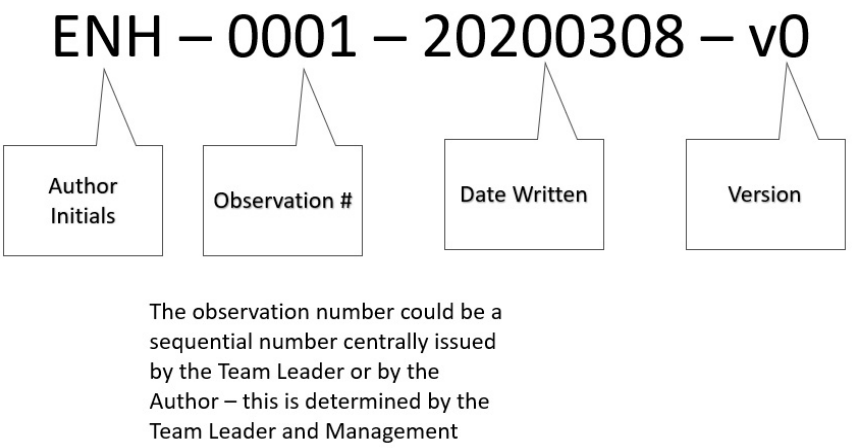


Figure 5-3 Observation Document Labeling/Numbering

- **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.

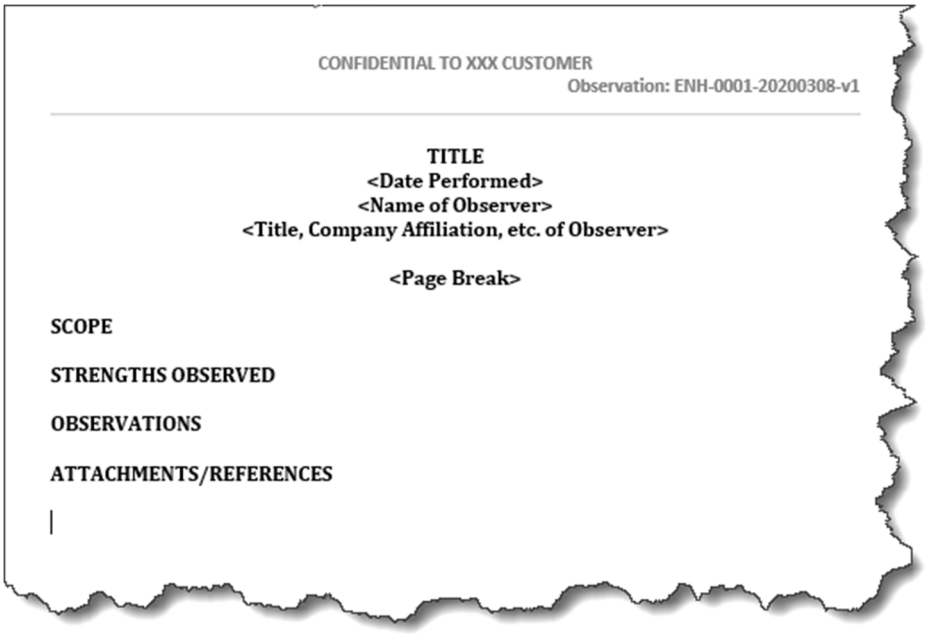


Figure 5-5 Observation Example Format

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/

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).

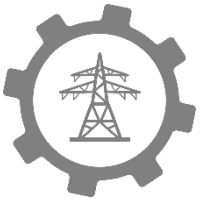
Ernie is an accomplished writer and frequent author of blogs, opinion pieces, and white papers. He is an invited columnist for the "Ask the Experts" discussions on TechTarget-SearchSecurity. Other thought-leadership articles have included authoring a chapter on "Cybercrime's Impact on Information Security," 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.



SPECIAL OFFER!

FOR A LIMITED TIME, SAVE 20%

Purchase Critical Infrastructure Risk Assessment: The Definitive Threat Identification and Threat Reduction Handbook, by Ernie Hayden

https://www.rothstein.com/product/critical-infrastructure/

Enter coupon code FC122020

At Checkout