
# ASIS School of ESRM
# November 16 and 18, 2021

# ASIS International (www.asisonline.org)

## WE ARE A GLOBAL AND DIVERSE COMMUNITY

### Who We Are

Founded in 1955, ASIS International is a global community of security practitioners, each of whom has a role in the protection of assets - people, property, and/or information.

Our members represent virtually every industry in the public and private sectors, and organizations of all sizes. From entry-level managers to CSOs to CEOs, from security veterans to consultants and those transitioning from law enforcement or the military, the ASIS community is global and diverse.

### What We Do

No other organization possesses the vast array of knowledge, expertise, and experience.

We offer a range of education programs, publications and events to help you thrive professionally, whether you're a young professional or an industry veteran. Developed in consultation with leading industry experts, our resources are designed to support you at every stage in your career.

# ASIS School of ESRM Faculty

## Tim Kelly

National Account Manager, ADT

ASIS Global ESRM Steering Committee

## Rachelle Loyear

VP, Integrated Security and Innovation, AUS

ASIS Global ESRM Steering Committee

## Paul Mercer

Managing Director, HawkSight SRM

ASIS Global ESRM Steering Committee

## Amy Poole

Global Project Manager, RightCrowd

ASIS Global ESRM Community Vice Chair

## Bill Phillips

CEO,  Managing Consultant, New Source Security

ASIS Global ESRM Community Chair

# ASIS School of ESRM Two-Day Agenda

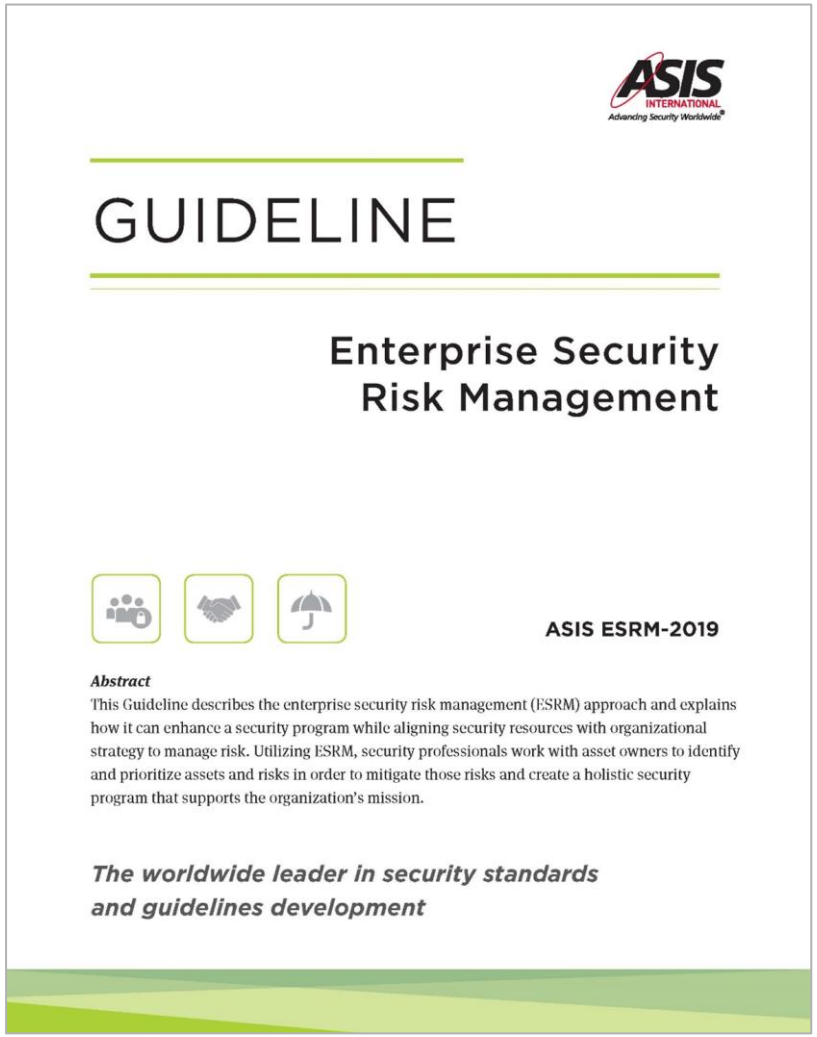
## Tuesday, November 16

| | | |
|---|---|---|
| **Session 1 – Introduction to ESRM and Transitioning to an ESRM Model** | 9:00am – 9:55am | All |
| ***Break*** | 9:55am – 10:00am | |
| **Session 2 – Understanding Assets and Risks** | 10:00am – 11:15am | Rachelle Loyear, Paul Mercer |
| ***Break*** | 11:15am – 11:20am | |
| **Session 3 – Continuous Monitoring and Improvement** | 11:20am – 11:50am | Rachelle Loyear, Paul Mercer |
| **Exercise Discussion** | 11:50am – 12:00pm | Amy Poole |

## Thursday, November 18

| | | |
|---|---|---|
| **Exercise Discussion** | 9:00am – 9:20am | Rachelle Loyear |
| **Session 4 – Building Foundational Relationships** | 9:20am – 10:25am | Tim Kelly, Bill Phillips |
| ***Break*** | 10:25am – 10:30am | |
| **Session 5 – How to Discuss (sell) ESRM with (to) your Leaders and Team** | 10:30am – 11:30am | Bill Phillips, Amy Poole |
| **Questions & Discussion** | 11:30am – 12:00pm | All |

# Official ASIS ESRM Guideline



GUIDELINE

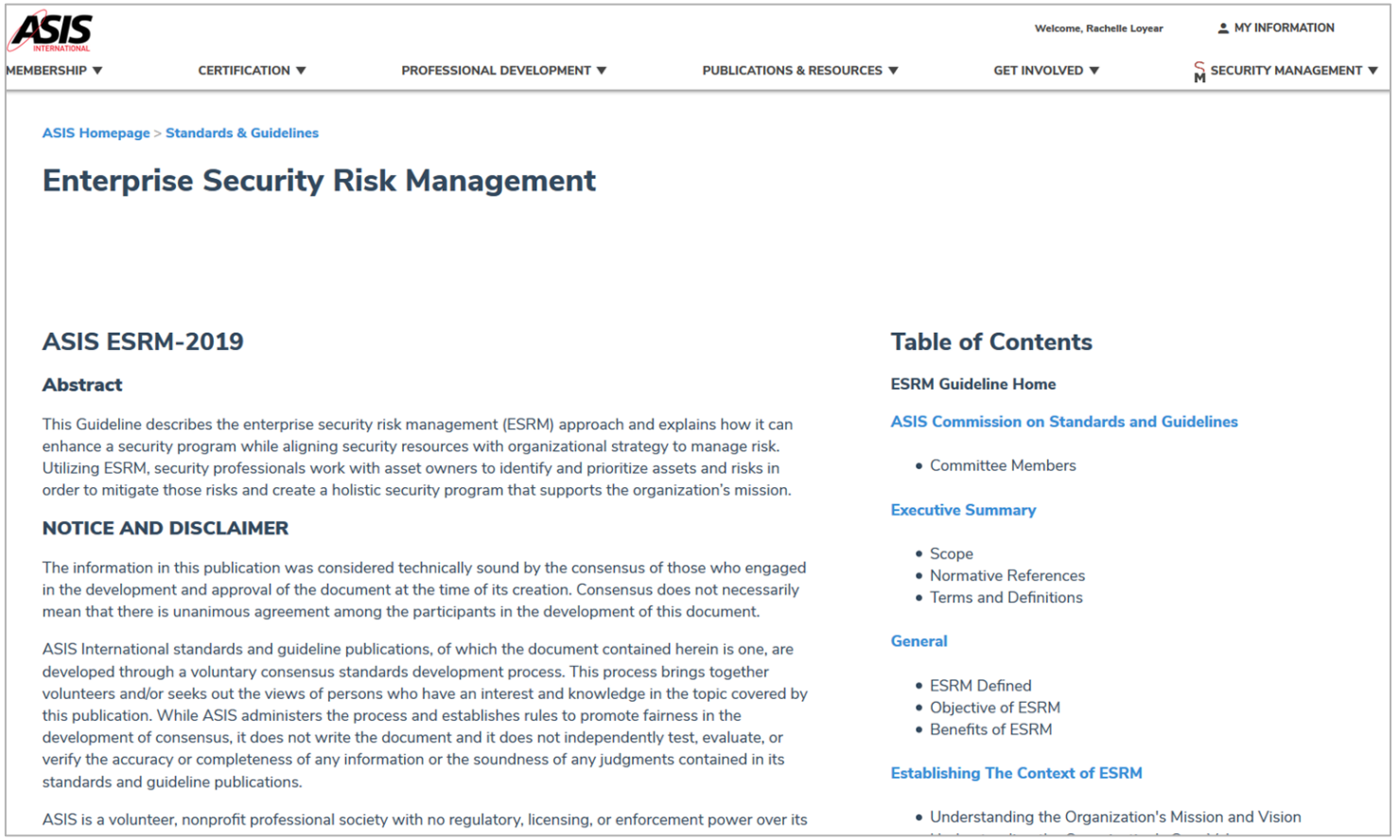
Enterprise Security Risk Management

ASIS ESRM-2019

*Abstract*

This Guideline describes the enterprise security risk management (ESRM) approach and explains how it can enhance a security program while aligning security resources with organizational strategy to manage risk. Utilizing ESRM, security professionals work with asset owners to identify and prioritize assets and risks in order to mitigate those risks and create a holistic security program that supports the organization's mission.

*The worldwide leader in security standards and guidelines development*



MEMBERSHIP ▼ CERTIFICATION ▼ PROFESSIONAL DEVELOPMENT ▼ PUBLICATIONS & RESOURCES ▼ GET INVOLVED ▼ SECURITY MANAGEMENT ▼

Welcome, Rachelle Loyear MY INFORMATION

ASIS Homepage > Standards & Guidelines

## Enterprise Security Risk Management

### ASIS ESRM-2019

**Abstract**

This Guideline describes the enterprise security risk management (ESRM) approach and explains how it can enhance a security program while aligning security resources with organizational strategy to manage risk. Utilizing ESRM, security professionals work with asset owners to identify and prioritize assets and risks in order to mitigate those risks and create a holistic security program that supports the organization's mission.

**NOTICE AND DISCLAIMER**

The information in this publication was considered technically sound by the consensus of those who engaged in the development and approval of the document at the time of its creation. Consensus does not necessarily mean that there is unanimous agreement among the participants in the development of this document.

ASIS International standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest and knowledge in the topic covered by this publication. While ASIS administers the process and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

ASIS is a volunteer, nonprofit professional society with no regulatory, licensing, or enforcement power over its

**Table of Contents**



https://www.asisonline.org/publications--resources/standards--guidelines/esrm-guideline/

# Essentials of Enterprise Security Risk Management (ESRM) Certificate

**Description**

The practice of Enterprise Security Risk Management (ESRM), a risk focused process for managing security, has grown as its benefits have been more fully understood and communicated. This certificate course gives you the essential knowledge and skills to advance ESRM at your organization.

This self-paced, online course explains the components of ESRM- Context, Foundation, and Cycle- and explores how they work together to create a holistic approach to risk management. This course features exercises that demonstrate the ESRM approach, so you become familiar and comfortable with the process.

This online certificate course includes 6-month access to the course material and a certificate exam. Successful completion of the course and passing the exam awards a certificate of competency. This certificate demonstrates you have gained the knowledge and skills essential to ESRM.


**https://store.asisonline.org/essentials-of-enterprise-security-risk-management-esrm-certificate.html**

# ESRM Maturity Model

At GSX, the ESRM Community Steering Committee unveiled the new ESRM Maturity Modeling Tool **Proof of Concept**


This tool is designed to:

- Help you understand where you are on the ESRM path.
- Support your organization in taking the next steps in ESRM, no matter what the program maturity level is.
- Bring the theoretical knowledge gained through ESRM training into the "real world"

The ESRM Maturity Model Tool helps you:

**Review Your Security Program**

- Review each element of ESRM maturity
- Align each element to a definition that most closely matches the current state of your organization, then...

**Chart Your Level**

- By answering a set of easy to understand questions.
- If you can answer Yes to all those questions, you are compliant at that level of maturity for that element of ESRM maturity.  You can then go to the next level of maturity to answer more questions and find out your level of ESRM maturity.

*If you would like to try out the new ESRM Maturity Model Proof of Concept tool and provide your feedback to the ESRM steering committee, please let us know and we'll provide you the appropriate information.

# ASIS ESRM Community


This is an open community for all members. The Enterprise Security Risk Management (ESRM) Community supports and promotes the practice of ESRM in the security profession. This community aims to create, support and leverage ESRM models, tools, publications, standards, guidelines and education to foster the ongoing evolution of security professionals to be an integral part of enterprise business leadership and to transition security practices from programs to risk management.

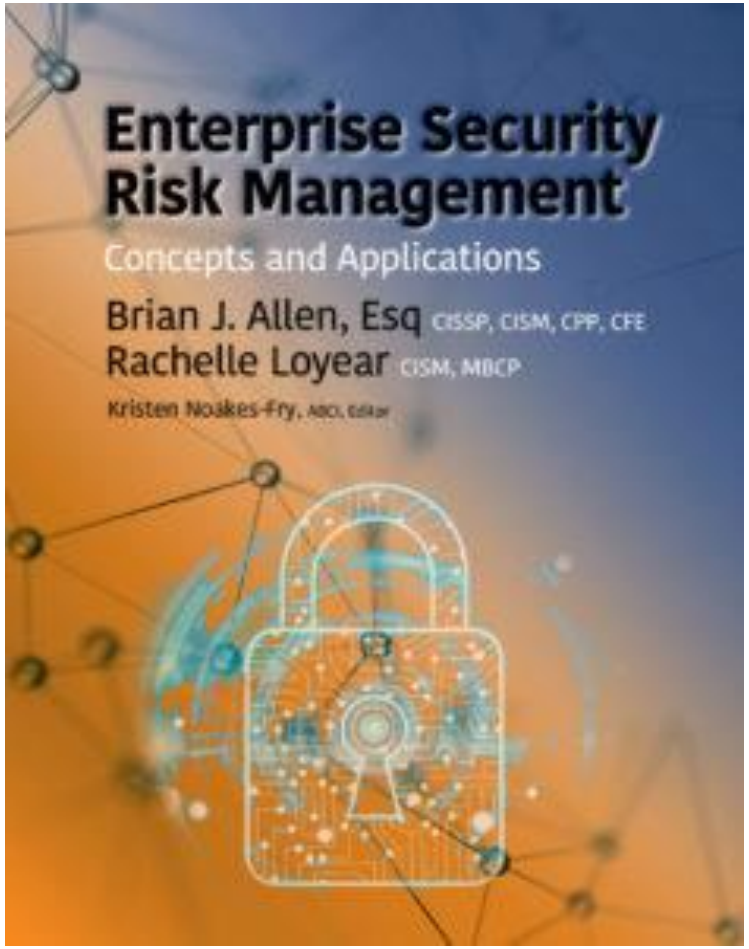
https://community.asisonline.org/communities/ESRM

# Enterprise Security Risk Management: Concepts and Applications

## By Brian Allen and Rachelle Loyear

By redefining how everyone thinks about the role of security in your enterprise, your security organization can focus on working in partnership with business leaders and other key stakeholders to identify and mitigate your security risks.

As you begin to use ESRM, guided by this book, you'll become a recognized and trusted partner in the business-critical effort of protecting your enterprise and all its assets.



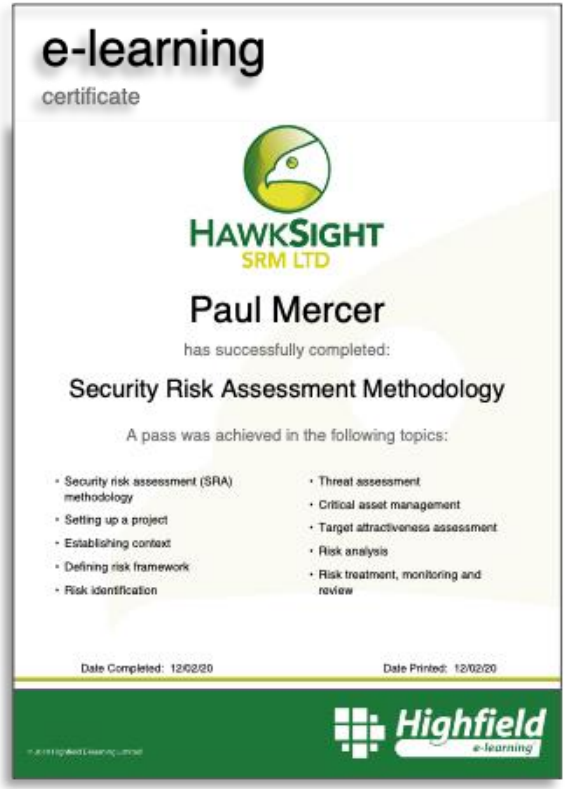

https://www.rothstein.com/enterprise-security-risk-management-2/

# Training in Digital Security Risk Management

**Description**

This e-learning Certificate in SRA methodology offers users training in ISO standardised security risk assessment methodology as an essential foundation to digital security risk management onboarding.

The digital SRM course builds on the certificate in SRA methodology  and  is designed for those who wish to be trained in the operation of the award-winning HawkSight SRM software platform.

ASIS INTERNATIONAL®
JAMAICA CHAPTER

# ASIS School of ESRM

## Session 1 - Introduction to ESRM and Transitioning to an ESRM Model

# Enterprise Security Risk Management

## 4. GENERAL

### 4.1 ESRM Defined

Enterprise security risk management (ESRM) is a strategic approach to security management that ties an organization's security practice to its overall strategy using globally established and accepted risk management principles. In ESRM, the security professionals and the asset owners share security responsibilities, but all final security decisions are the responsibility of the asset owner.

# ESRM IS... PARTNERSHIP

ESRM recognizes that security responsibilities are shared by both security and business leadership, but that all final security decision making is the responsibility of the business leaders.

The role of the security leader in ESRM is to manage security vulnerabilities to enterprise assets in a risk decision making partnership with the organization leaders in charge of those assets.

# ESRM IS…
# INCLUSIVENESS

**A mature ESRM program** encompasses all aspects of security risk mitigation practices to prevent security risk impacts to the enterprise.

Value exists because ***the business owns the security*** *risk.* Therefore, we now provide business deliverables.

# Why Does ESRM Include ALL Security Disciplines?
## **Because RISK IS RISK**

| Physical Security Risk | Cyber Security Risk |
|---|---|
| **Intrusion Risk in a Warehouse** | **Intrusion Risk on a Network** |
| What asset is inside the warehouse? | What data is on the server? |
| Whose asset is it that is being protected? | Who uses that data? |
| How important is that asset to the mission of the business? | How important is the information asset to the mission of the business? |
| What are the security risks to the warehouse? | What are the security risks to that information? |
| Who are the stakeholders? | Who are the stakeholders? |
| What would be the impact to the business if the assets in the warehouse were intruded upon, and potentially stolen or vandalized? | What would be the impact to the business if the information assets in the network were intruded upon and potentially stolen or manipulated? |
| How would you recover? | How would you recover? |

# ESRM IS... PARTICIPATION

Managing the security decision making process requires:

- Educating business partners.
- Presenting potential security strategies.
- Implementing the business leader's decision.
- Documenting the residual risk and continuing to educate your business partners.

# Session 4 Topics!

## COMMON QUESTIONS WE GET…

How do you go about building these partner relationships in your organization?

Have you seen benefits from being more inclusive in your security program?

# HOW IS ESRM DIFFERENT?

Security Risk **Management** Is Strategic

Security Risk **Mitigation** is Tactical

## A Difference in Focus

- Go further than “who” to “how” and find the underlying gap or risk.

**Gap Finding vs. Guilt Finding**

## A Difference in Goals

- Go further than individual correction to fill the gap and avoid additional future impact from the same risk.

**Risk Mitigation vs. Punishment**

## A Difference in Perception

- Every task is carried out for a reason.

**Security is more than a task**

## A Difference in Approach

- Security risk mitigation activities can provide protection … plus added benefits

**Risk Management as a Business Benefit**

# Session 5 Topics!

## COMMON QUESTIONS WE GET

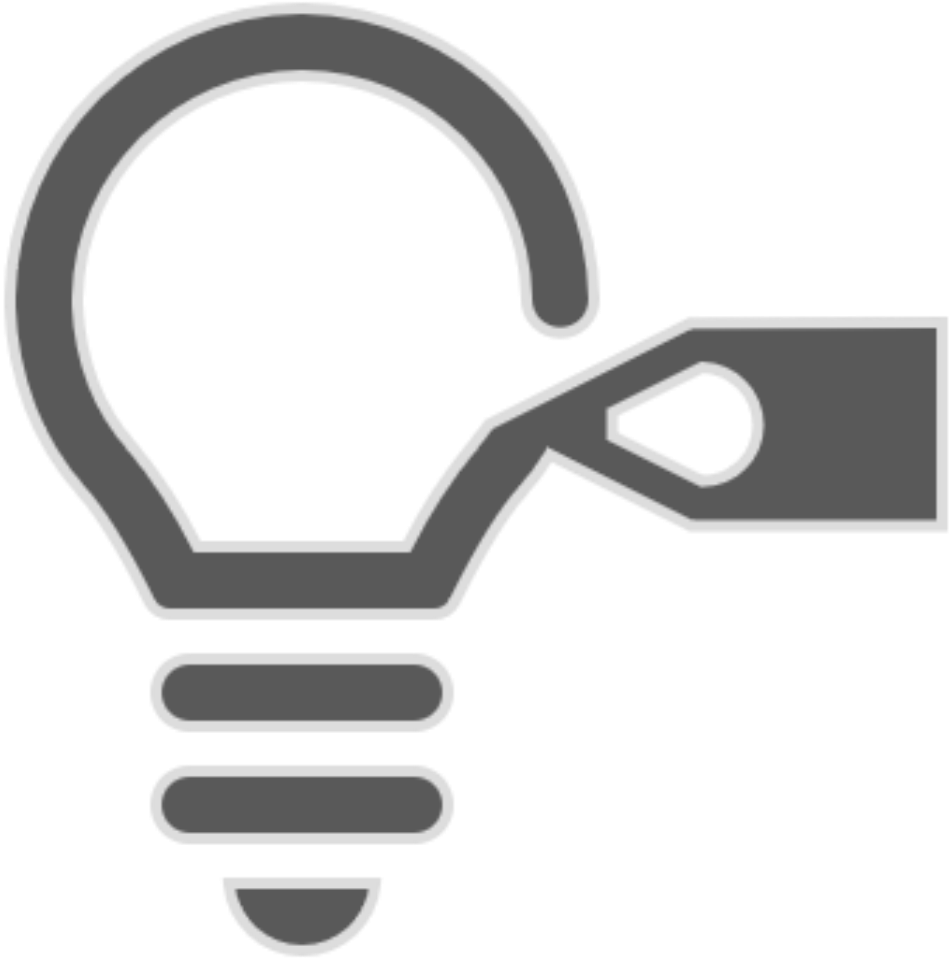
How do you help your teams to embrace the different focus and goals of an ESRM program?

How do you explain this change and the benefits of ESRM to your leaders?

# Adopting an ESRM Model

# Where Do I Start?

You Cannot Protect What You Do Not Understand…

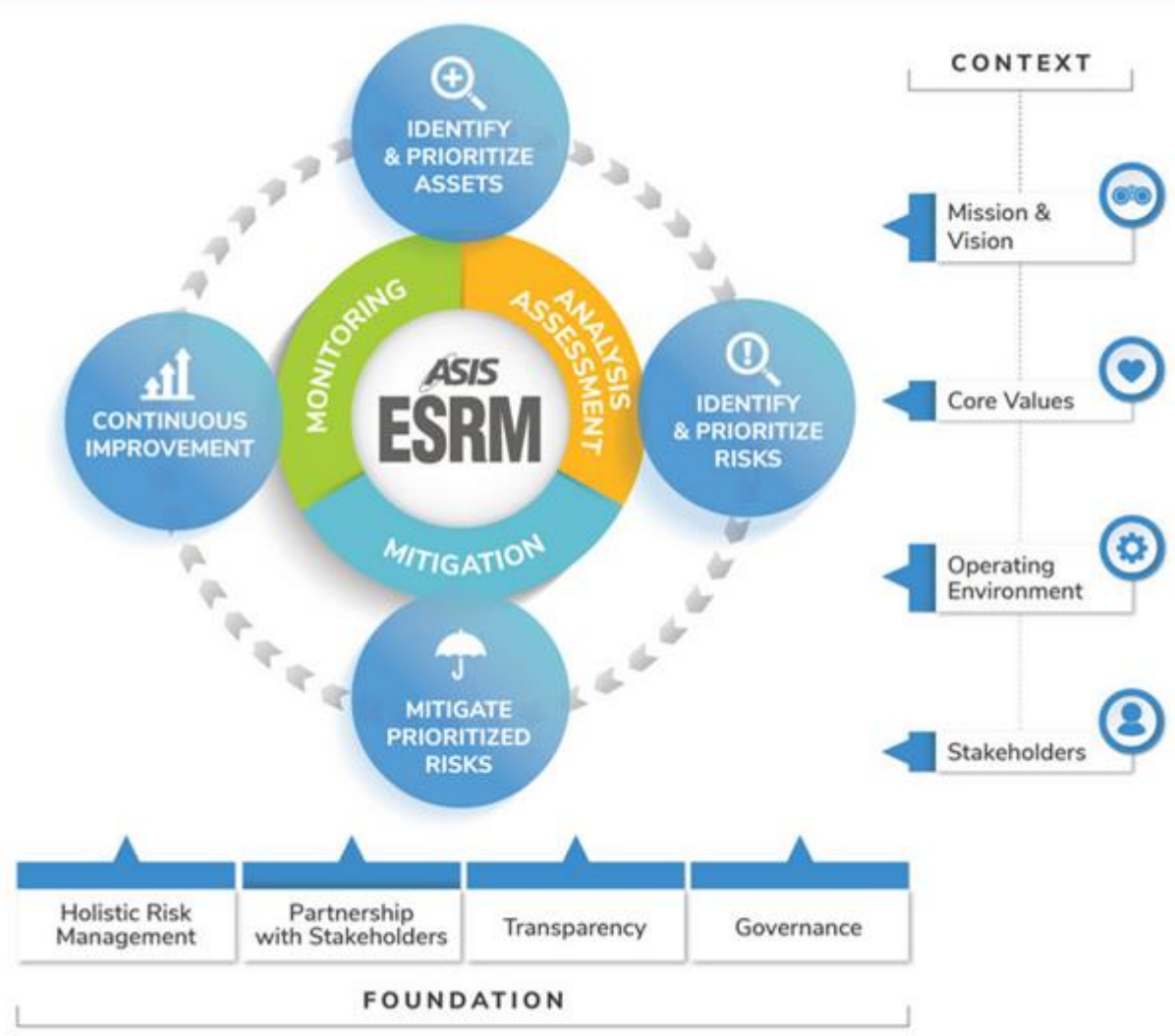


# FIRST UNDERSTAND YOUR ORGANIZATION

- What does the business do? Why? How?
- What are the enterprise objectives and priorities?
- What is the mission?
- What are the products and services?
- What environment does the enterprise operate in?
- Who are the stakeholders?
- Who controls the assets that need to be protected?
- Who makes the final decisions about those assets?

# THE ESRM LIFE CYCLE

- **Identify and Prioritize Assets:** The process of identifying, understanding, and prioritizing the enterprise's assets.
- **Identify and Prioritize Risks:** Identifying, understanding, and prioritizing the security risks to the enterprise and their relationship to the assets value.
- **Mitigate Prioritized Risks:** Taking the necessary, appropriate, and realistic steps to protect against the most serious security threats and risks.
- **Continuous Improvement:** The risk paradigm of managing security risks is a cyclical approach to continuously improve and advance the security posture of the enterprise.

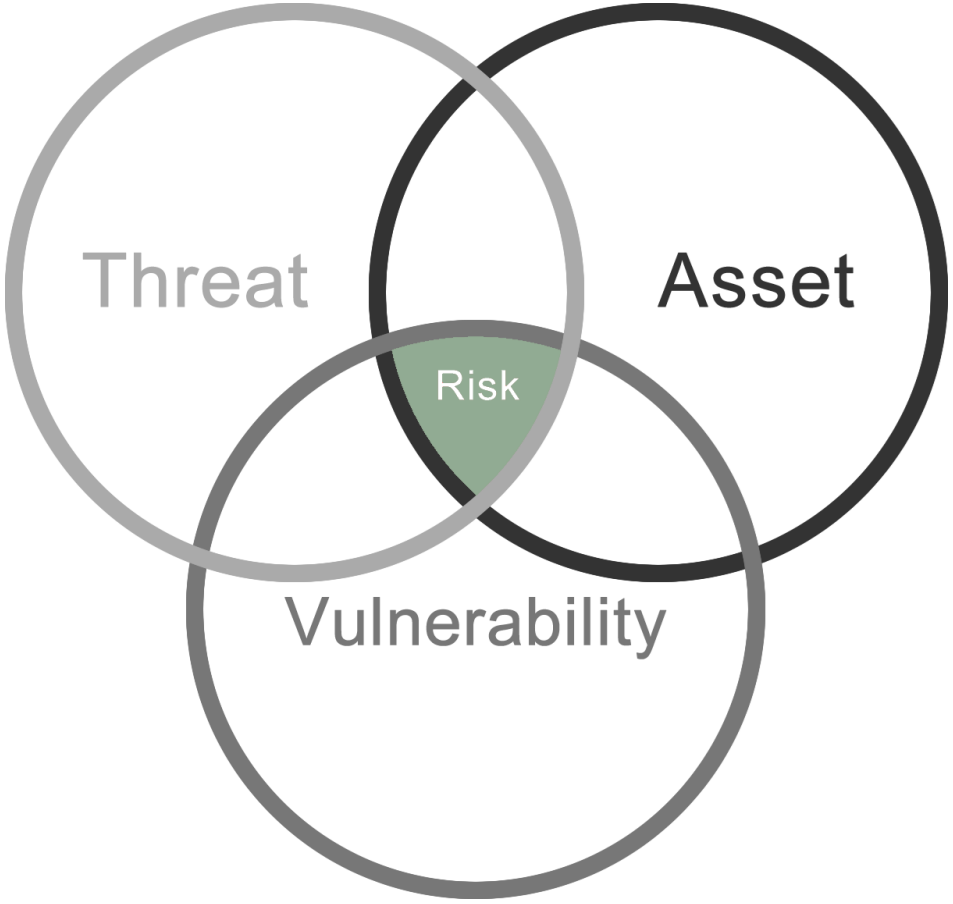



Reference: *Enterprise Security Risk Management: Concepts and Applications*

# ESRM STEP 1:
# IDENTIFY AND PRIORITIZE ALL ASSETS

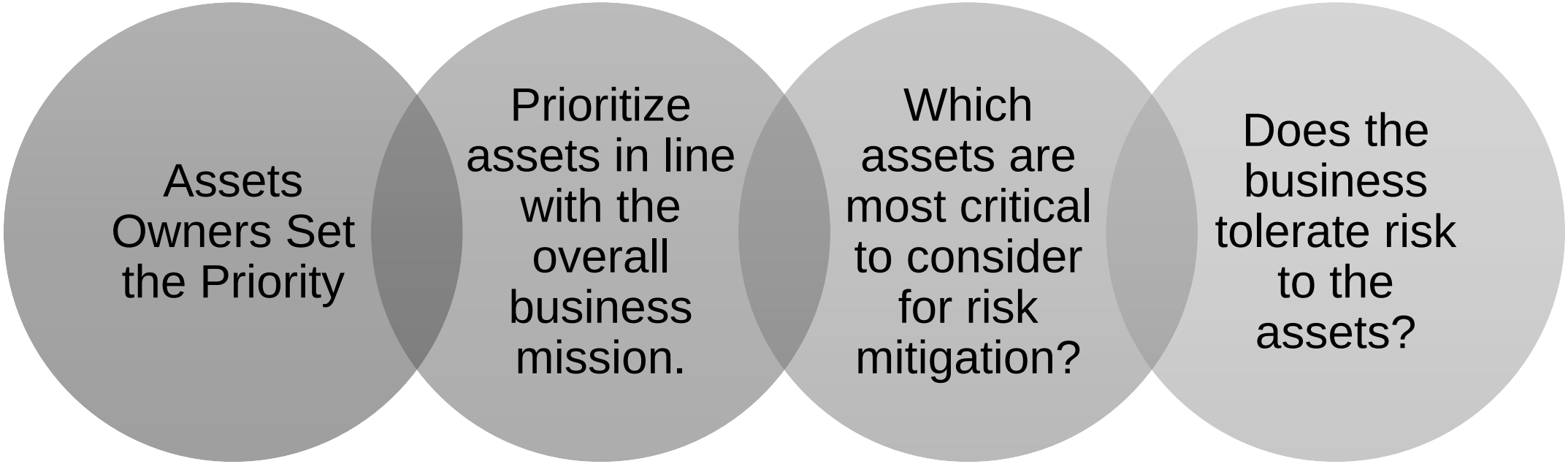

“What does the organization need and want to protect?”

# STEP 2:
# IDENTIFY AND PRIORITIZE RISKS




“What do our assets need to be protected from?”

# PRIORITIZING ASSETS AND RISKS




“What assets are critical?” “What risks are tolerable?”

# STEP 3:
# MITIGATE PRIORITIZED RISKS

Managing the security decision making process requires:

- Educating internal business partners on the realistic impacts of security risks to assets under their control.
- Presenting potential security strategies to decision-making business leaders to mitigate those impacts.
- Enacting the business leader’s security risk mitigation choice, driven by business risk tolerance.

# STEP 4:
# IMPROVE AND ADVANCE YOUR SECURITY PROGRAM

The cycle as a management tool enables you to partner with the clients in a comprehensive security risk decision-making process.

Security risks change constantly… all aspects of the program should be revisited on an ongoing basis.

# What ***Else*** Does Security Need to Be Successful?

Security needs a commitment to *holistic risk management* to properly identify risks across the enterprise that are within the defined scope of the security role, and the authority of a *governance body* to make those risks *transparent* and respond to the risks in *partnership* with the business leaders.


# Holistic Risk Management

- Remove Silos
- Capture “true” security risk
- Consider all security risks
  - Physical
  - Virtual

# Partnership With Stakeholders

- Gain immediate benefits
  - Higher levels of engagement
  - Comprehensive understanding of security risk
  - Greater organizational support

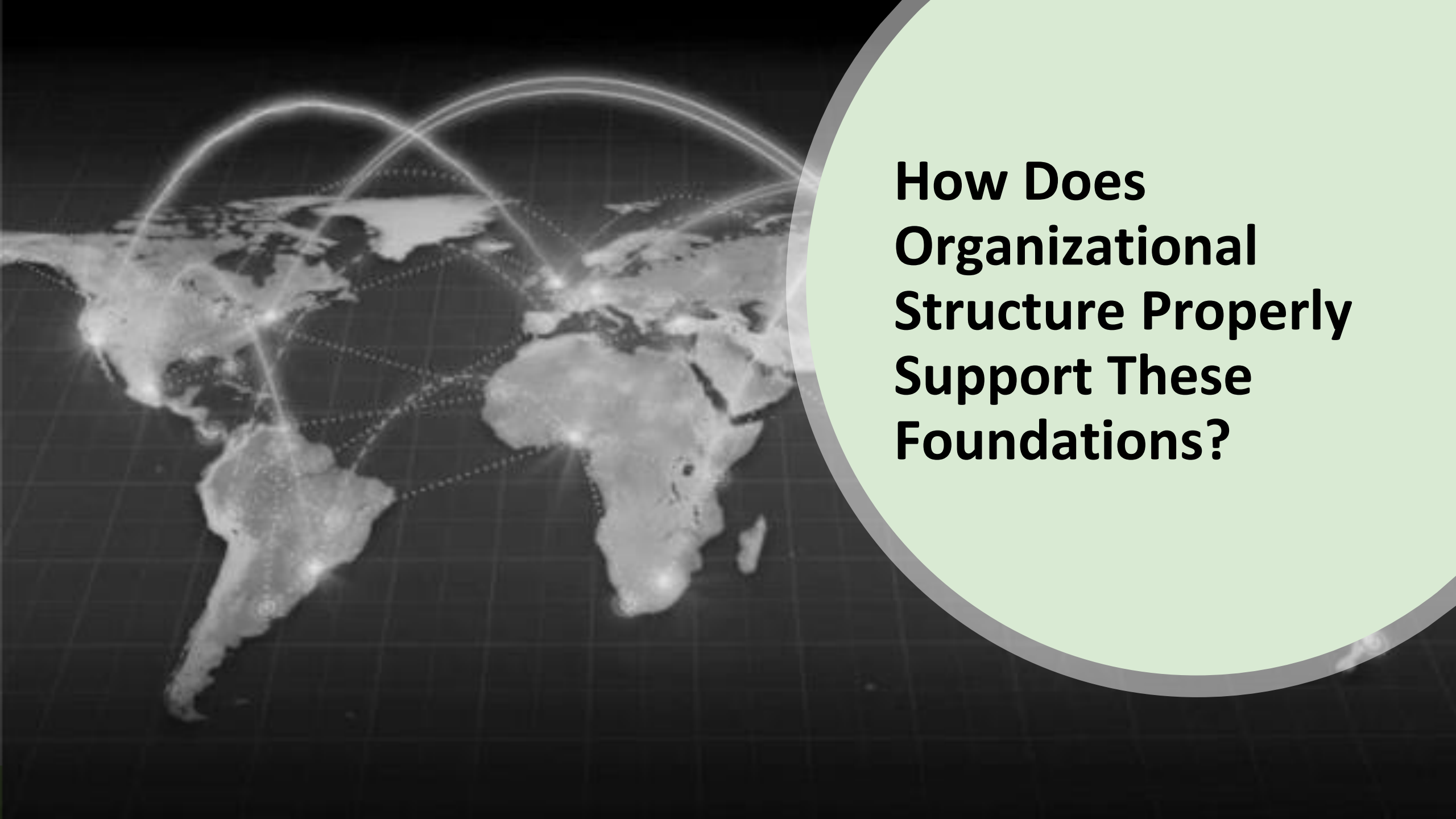
# Transparency

- ESRM provides transparency of:
  - Risk
  - Process


# Governance

Governance Sets Tolerance, Authority, and Scope of Security

- Organizational
  - Role of Executives, decisions, etc.
- ESRM
  - Security Council / Committee



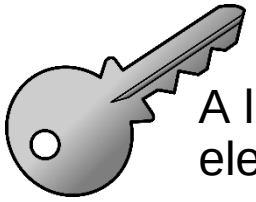
# How Does Organizational Structure Properly Support These Foundations?

# Reporting and Organization Structures Must Avoid Conflicts of Interest to Be Truly Effective

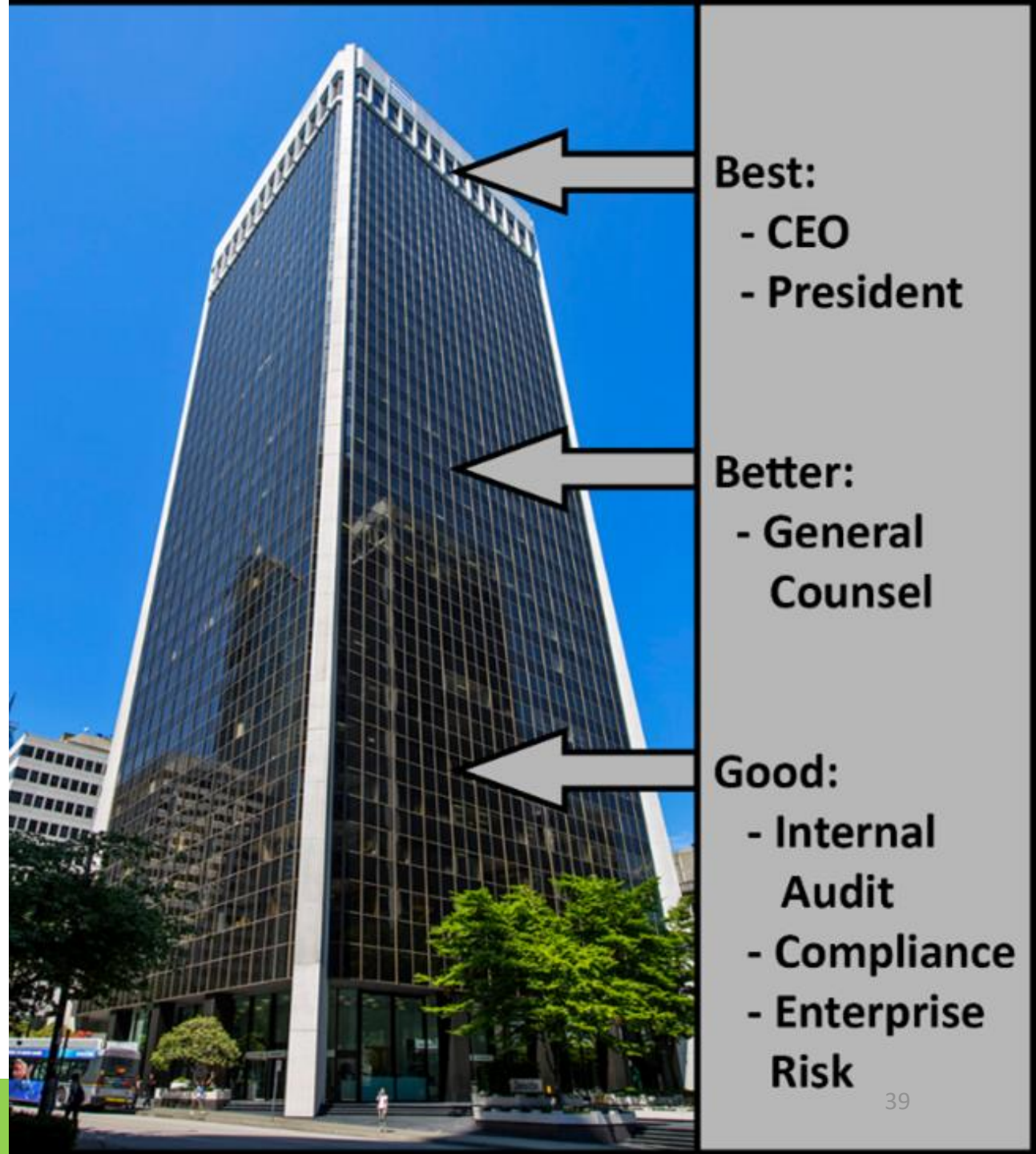
- Can a security team that reports into finance investigate the possibility of fraud or misconduct in its own chain of command?
- Does a Security team that reports to IT risk being shut out if they find a risk that makes the IT leaders look bad?
- Can a security director that reports into operations recommend a program that might impede important business operations?
- Does a security group siloed under facilities have scope to investigate security risks in other lines of business?

# What Are Your Organization's Options?

- Does the Enterprise Have Departments for
  - Compliance?
  - Enterprise Risk Management?
  - Internal Audit?
- Greatest Success Comes with the Greatest Independence



A leader who can ensure the essential elements for security success.



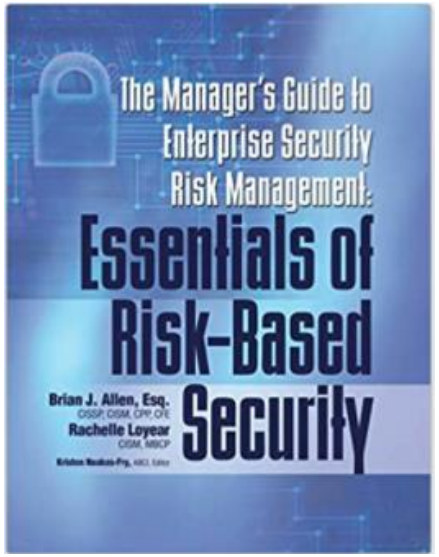
# ESRM Toolbox

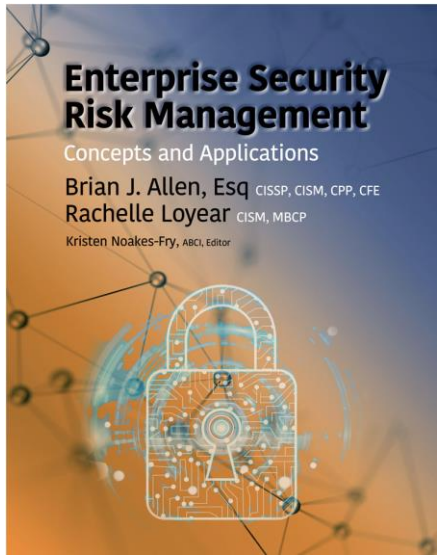
# Articles

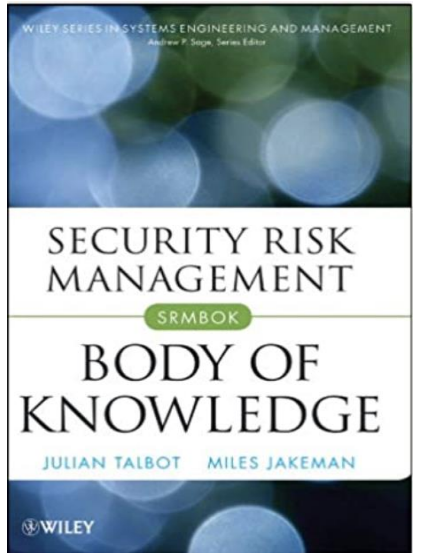
1. A brief guide to ESRM implementation 2019 – Dave Feeney
2. Time to pivot – Applying ESRM after Covid 19 2021 – Claire Meyer
3. Five Insights into ESRM 2017 – Rachelle Loyear & Brian Allen
4. How to implement ESRM 2018 - Art Fiero

# ESRM Toolbox

# Books



# Questions…?


# 5 Minute Break