

Enterprise Security Risk Management
a first introduction

Osaka, 1 June 2020 & Tokyo, 9 Juni 2020

Berndt Rif, MSc, MBA, CPP,

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

Enterprise Security Risk Management (ESRM)

a first introduction

09.00 – 09.30 Meet & Greet
09.30 – 11.00 ESRM
11.00 – 11.30 Coffee Break
11.30 – 12.30 Exercise
12.30 – 13.30 Lunch
13.30 – 14.45 Exercise
14.45 – 15.15 Coffee Break
15.15 – 16.30 Exercise
16.30 – 17.00 Evaluation

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

ESRM: What It Is

Enterprise Security Risk Management (ESRM) is a strategic approach to security management that ties an organization's security practice to its mission and goals using globally established and accepted risk management principles.

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

ESRM: What It Isn't

- It's not Security Convergence:
  - Convergence integrates Physical Information, and/or Cyber Security under one leader
  - The degree of integration identifies the degree of convergence

- It's not Enterprise Risk Management:
  - ERM manages all company risk
  - ESRM is a component of ERM
  - ESRM uses similar philosophy to manage security risks

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

** ESRM does not require an ERM program to be successful, but the presence of an ERM program can ease the process of ESRM adoption.*

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

Specific Roles Within ESRM

Role	Description
Asset Owner	* Member of an enterprise who is most accountable and responsible for the productivity, performance, and overall operation of an asset.
Security Professionals	Security leaders, managers, or workers involved in security and security risk management.
Stakeholders	* Person or organization with an interest or concern. *NOTE: A stakeholder can affect and may be affected by the organization and its achievement of its objectives (real or perceived).*
Top Management	* Person or people responsible and accountable for formulating the goals, objectives, strategies, and policies of an enterprise, and/or who allocate the enterprise's resources.

** = Defined Term in ASIS ESRM Guideline*
(ASIS ESRM-2019, Enterprise Security Risk Management)

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

ESRM: Why?

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

Potential ESRM Benefits to Security Professionals

- Enables security to define its own role as trusted advisors of asset owners, stakeholders, and top management;
- Assists in developing a better understanding of the organization and its overall strategy;
- Can help improve communication and interaction opportunities with diverse stakeholders (internal and external) to learn what they consider important;
- Assists in developing a more timely and comprehensive understanding of security risks;
- Assists in obtaining greater support from asset owners by better aligning security efforts with their needs; and
- Enables innovative problem solving by increasing focus on the concepts of risk as opposed to the specific tactics used to mitigate risk.

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

Potential ESRM Benefits to the Organization

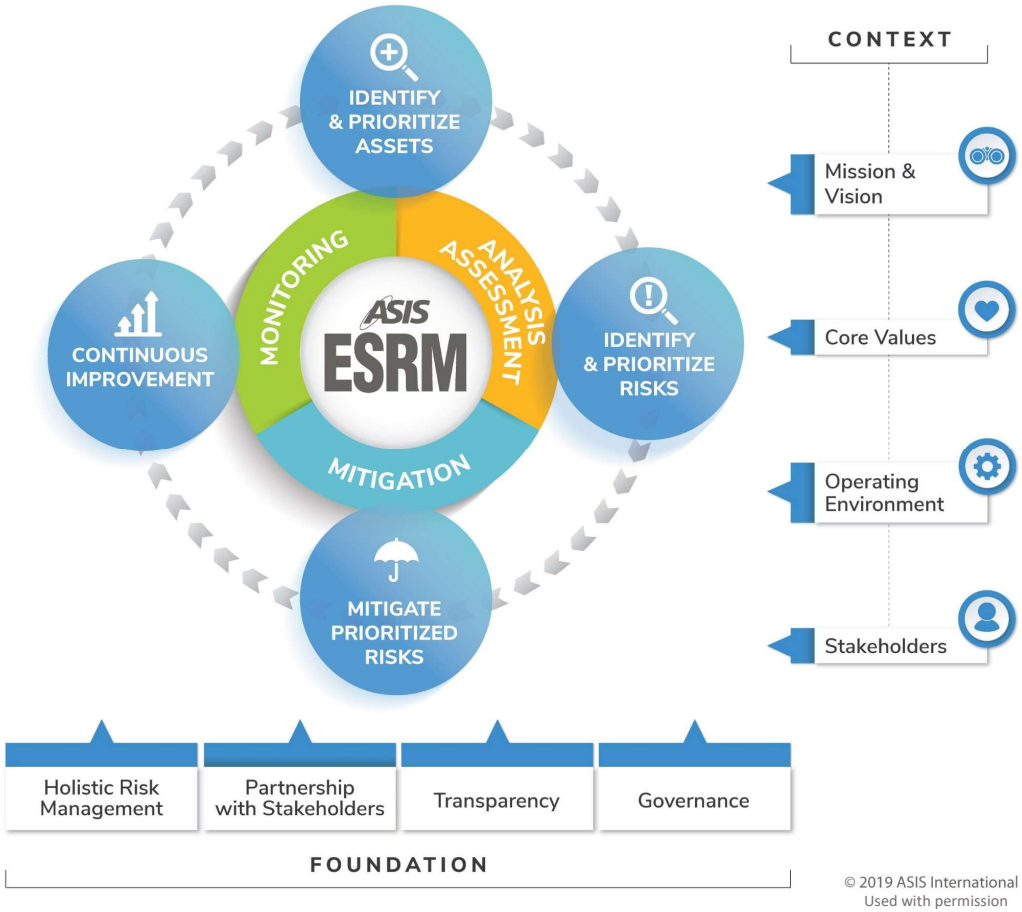
- Enables enterprise-level risk-based decisions, supporting the organization's mission and objectives;
- Enables asset owners & stakeholders to develop a greater, consistent understanding of security's role;
- Provides a mechanism to elevate identified security risks to top management;
- Better alignment of security resources & organizational strategy to effectively manage prioritized risk;
- Can improve effectiveness and efficiency of the security program;
- Early identification and proactive monitoring of threats and vulnerabilities;
- More effective risk prioritization & mitigation based on partnership between security & asset owners;
- Can improve engagement with stakeholders with a vested interest in the security of the organization;
- Better support for the organization's legal, regulatory, contractual, and internal audit responsibilities;
- Integrates security into the culture of the organization; and
- Can enhance organizational resilience & event response capabilities, including crisis management.

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

ESRM: How?

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

ESRM Strategic Approach



- ESRM Cycle:
  - Identify & Prioritize Assets
  - Identify & Prioritize Risks
  - Mitigate Prioritized Risks
  - Continuous Improvement
- ESRM Context:
  - Mission & Vision
  - Core Values
  - Operating Environment
  - Stakeholders
- ESRM Foundation:
  - Holistic Risk Management
  - Partnership with Stakeholders
  - Transparency
  - Governance

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

ESRM Cycle



Identify & Prioritize Assets

The **Asset Owner** is the Risk Owner. The Asset Owner also owns risks to that asset.

The **Security Manager** is the Asset Owner's trusted advisor and security risk subject matter expert.

The **Security Manager** helps guide the asset owner through the security risk decision-making process.

ESRM considers all assets and all security risk – physical, cyber, information, etc. – without segmenting security disciplines.

Activities:
Analysis & Assessment

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

ESRM Cycle



Identify & Prioritize Risks

Prioritization is based on the risk's potential impact on the organization's ability to:

- Execute its mission and vision
- Maintain its core values
- Support its operating environment
- Satisfy its stakeholders

These **strategic priorities** cascade throughout the entire ESRM cycle, helping guide asset owner decisions.

Prioritization is based on guidance from **Top Management** and input from **Asset Owners**.

Activities:
Analysis & Assessment

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

ESRM Cycle



Mitigate Prioritized Risks

Risks are mitigated **in order of priority**, using security controls recommended by the **Security Manager** and approved by the **Asset Owner**.

The **Security Risk Management Plan** or **Security Plan** documents the prioritized risks and associated security controls.

Senior Management and Asset Owners are responsible for the decisions in the Security Plan, and the **Security Manager** is responsible for **executing** it.

_____

Activity:
Mitigation

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

ESRM Cycle



Continuous Improvement

Continuous improvement of the security program occurs as a result of **ESRM outcomes** such as:

- Improved communication
- Greater visibility into security risks
- Effective prioritization & mitigation

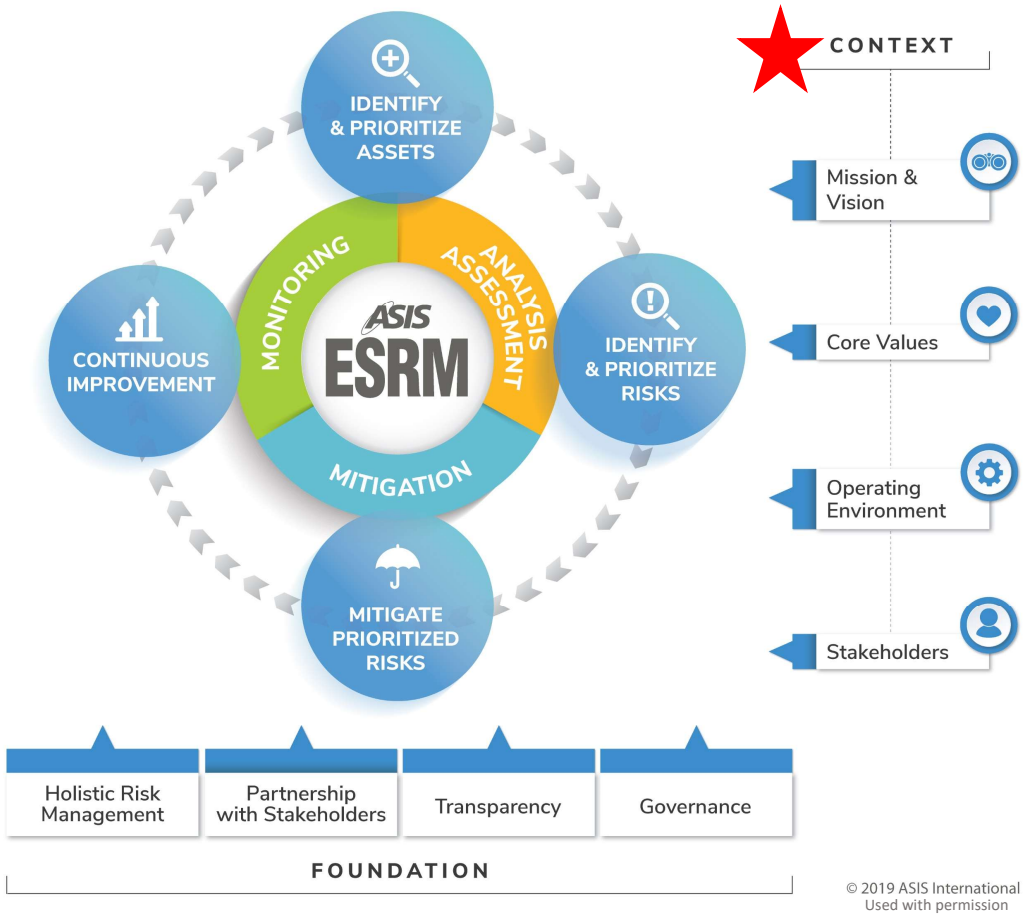
Various **security functions** contribute to continuous improvement of the security program, including but not limited to:

- Incident Response
- Investigations & Analysis
- Information Sharing

Activity:
Monitoring

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

The Context of ESRM



Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

The Context of ESRM



- Understanding the organization's mission & vision enables security professionals to identify risks that could undermine them.

- Consider aspects of the organization's strategy such as:
  - Operating structure
  - Relevant staff & top management
  - Products & services
  - Regulations & legal requirements
  - Strategic goals & objectives

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

The Context of ESRM



- Core values can indicate how well ESRM might be supported by the corporate culture.
- Strategically linking ESRM to the organization's core values can help achieve alignment with the priorities of top management.
- An organization's core values are an integral component and driver of corporate culture.
- That culture may indicate an organization's:
  - Risk tolerance & risk appetite
  - Ability to execute, communicate and handle change
  - Support of communications, transparency, and security.

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

The Context of ESRM

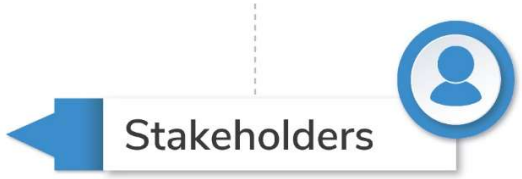


The operating environment consists of three main categories and their interdependencies:

- **Physical**: Factors such as the organization's types and locations of buildings, its surroundings, its infrastructure, its pedestrian or vehicular traffic, the operational technology needed for the organization to operate, and the sensitivity and criticality of on-site processes and assets.
- **Nonphysical**: Factors such as the geo-political landscape, culture, industry pressures, legal, regulatory and compliance requirements, intensity of competition, organizational growth mode, speed of decision-making, and willingness to adopt technology.
- **Logical**: Includes information and digital assets, and the network or digital space that connects them to each other and to their users and stakeholders.

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

The Context of ESRM



Security professionals should understand the organization's stakeholders and what's important to them.

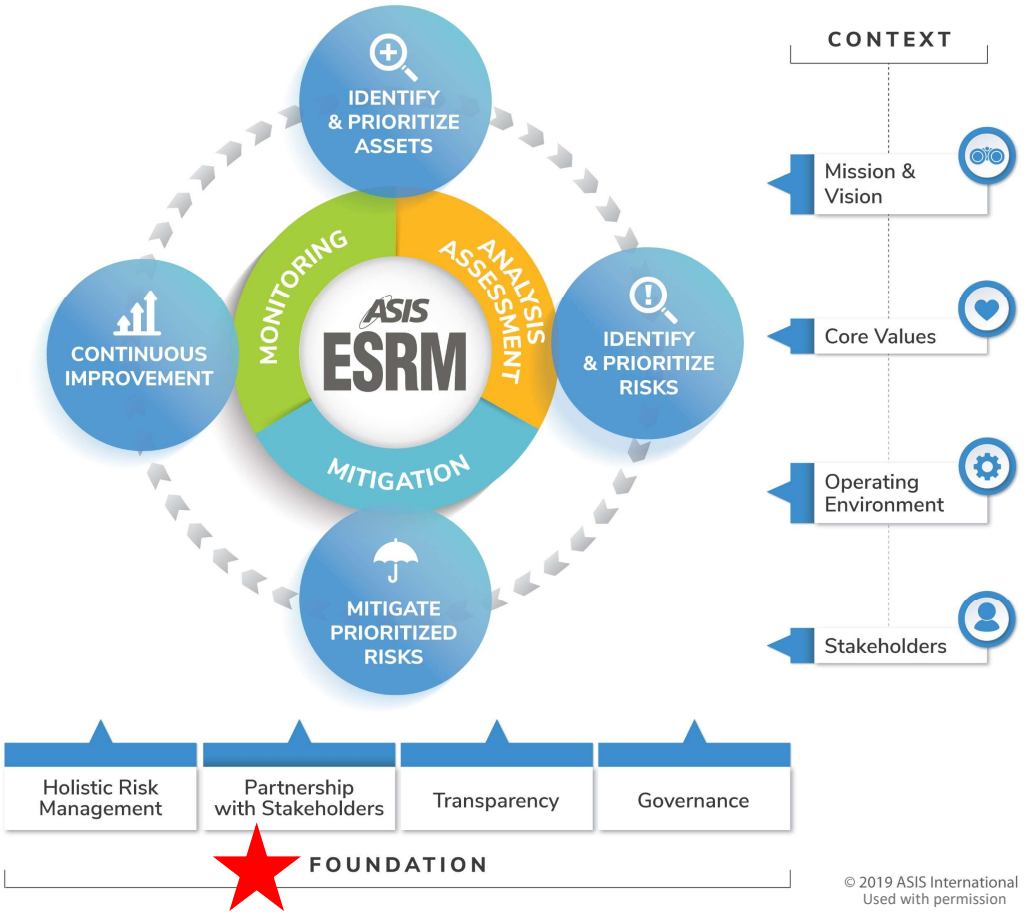
Any individual who interfaces with the organization may be considered a stakeholder, including:

- Top management
- Asset owners
- Employees, contractors, vendors, clients, and visitors
- Persons who may be impacted by the organization and/or the security professional.

Understanding stakeholders does not necessarily mean harmonizing their interests, but rather understanding their needs and their risk insights to better execute the ESRM Cycle.

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

The Foundation of ESRM



Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

The Foundation of ESRM



YES

Physical Security | Information Security | Cyber Security

Crime Prevention | Fraud | Loss Prevention | Executive Protection | Travel Security

Data Protection | Application Security | Vulnerability Mgmt. | Threat Mgmt. | EDR

NO

Silos | Boundaries

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

The Foundation of ESRM



IN	OUT
Partner	Authoritarian
Trusted Advisor	Empowered Officer
Alignment	Enforcement
Risk-Based	Task-Based
Guidance	Compliance
Making Decisions	Following Rules

- Engagement
- Buy-In
- Sense of Ownership
- Understanding of Risk
- Organizational Support

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

The Foundation of ESRM



- **Risk Transparency**:
  - Enables informed decision making.
  - Maintains risk ownership with the Asset Owner.

- **Process Transparency**: Keep stakeholders informed about:
  - Current and planned security measures
  - The reasons for those measures
  - Any other relevant decision-makers
  - Other mitigation options that may be considered
  - Final decisions on risk mitigations.

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

The Foundation of ESRM



- **Organizational Governance**: The system by which an organization is directed and controlled. Addresses:
  - The role of top executives and the board of directors
  - The need for audit, oversight, and transparency
  - The rights and responsibilities of stakeholders
  - Procedures for decision-making

- **ESRM Governance**: The process of setting enterprise security risk policy and direction, allocating resources, and ensuring compliance.
  - A subset of organizational governance
  - Carried out by the organization's security governance body

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

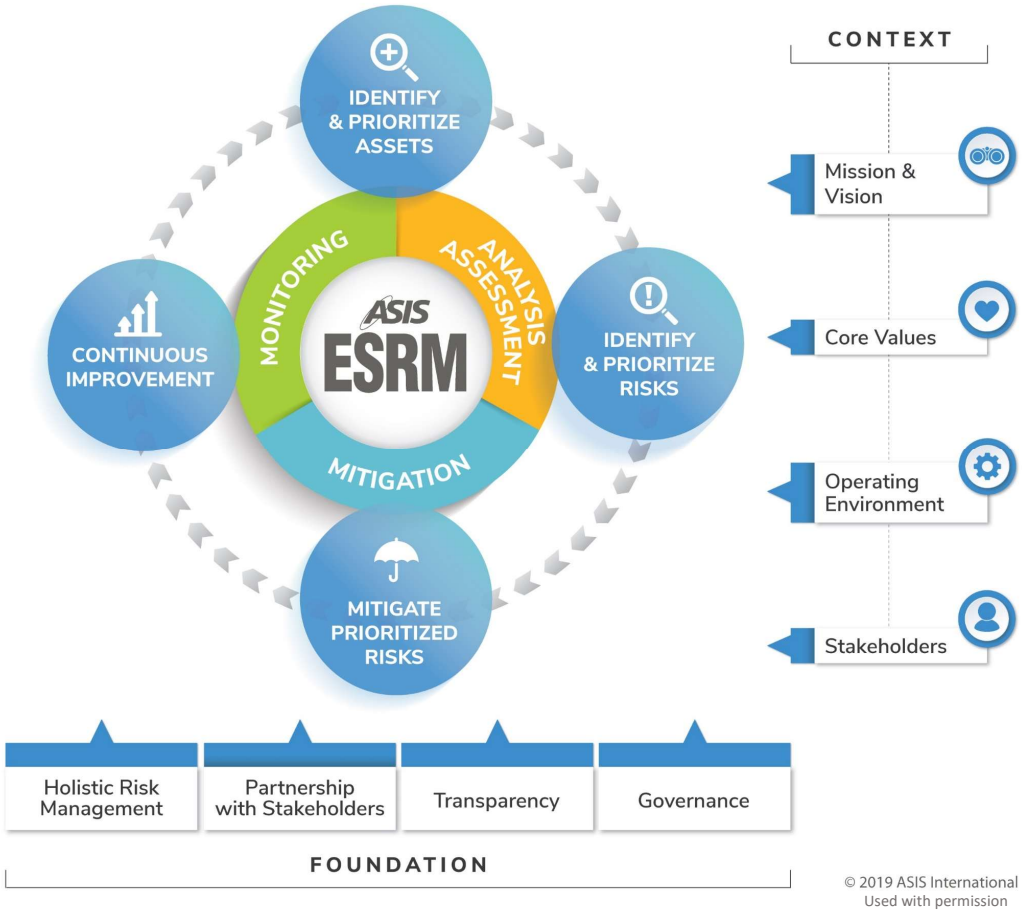
Enterprise Security Risk Management (ESRM)

a first introduction

09.00 – 09.30 Meet & Greet
09.30 – 11.00 ESRM
11.00 – 11.30 Coffee Break
11.30 – 12.30 Exercise
12.30 – 13.30 Lunch
13.30 – 14.45 Exercise
14.45 – 15.15 Coffee Break
15.15 – 16.30 Exercise
16.30 – 17.00 Evaluation

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

ESRM Strategic Approach



- ESRM Cycle:
  - Identify & Prioritize Assets
  - Identify & Prioritize Risks
  - Mitigate Prioritized Risks
  - Continuous Improvement
- ESRM Context:
  - Mission & Vision
  - Core Values
  - Operating Environment
  - Stakeholders
- ESRM Foundation:
  - Holistic Risk Management
  - Partnership with Stakeholders
  - Transparency
  - Governance

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

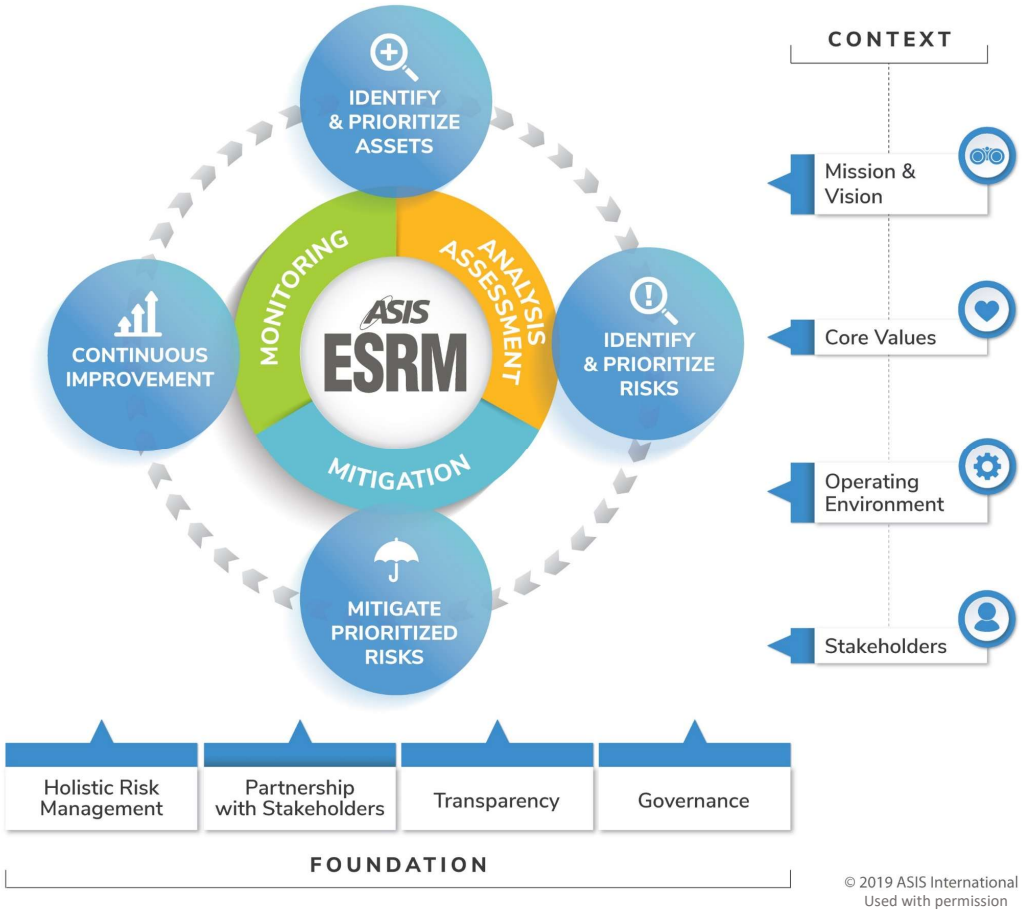
Enterprise Security Risk Management (ESRM)

a first introduction

09.00 – 09.30 Meet & Greet
09.30 – 11.00 ESRM
11.00 – 11.30 Coffee Break
11.30 – 12.30 Exercise
12.30 – 13.30 Lunch
13.30 – 14.45 Exercise
14.45 – 15.15 Coffee Break
15.15 – 16.30 Exercise
16.30 – 17.00 Evaluation

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

ESRM Strategic Approach



- ESRM Cycle:
  - Identify & Prioritize Assets
  - Identify & Prioritize Risks
  - Mitigate Prioritized Risks
  - Continuous Improvement
- ESRM Context:
  - Mission & Vision
  - Core Values
  - Operating Environment
  - Stakeholders
- ESRM Foundation:
  - Holistic Risk Management
  - Partnership with Stakeholders
  - Transparency
  - Governance

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

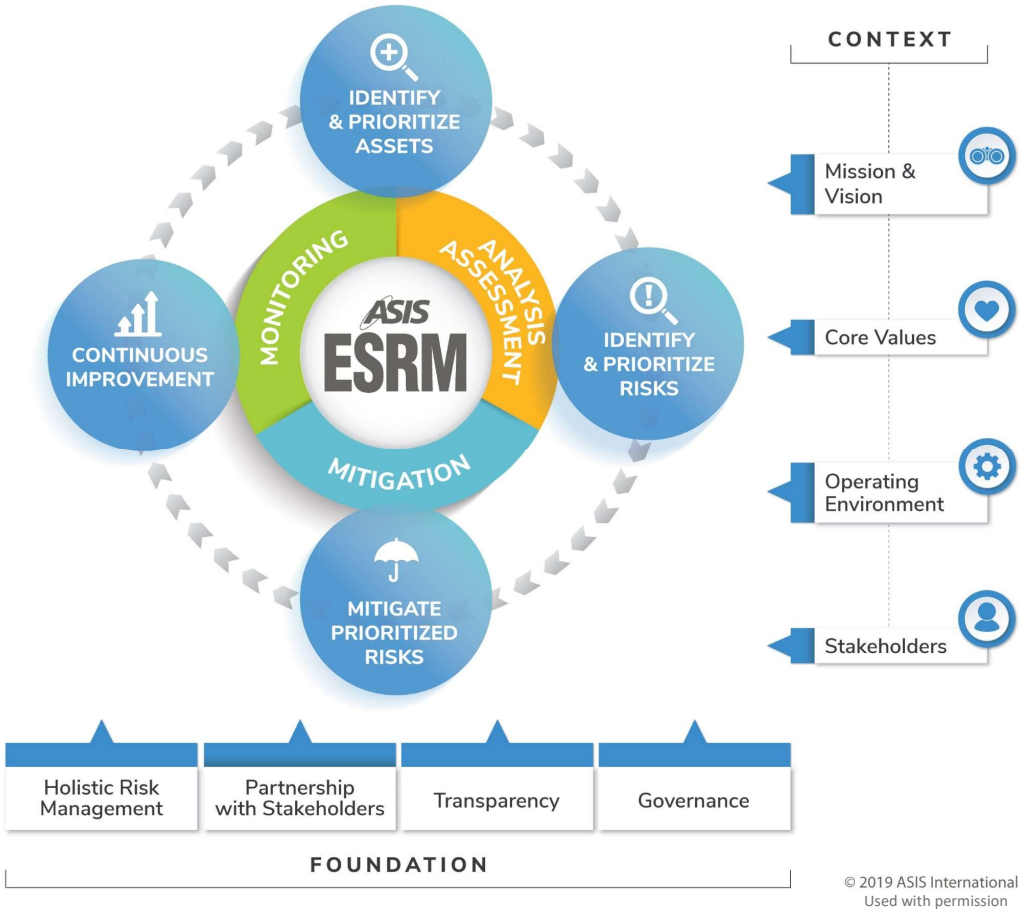
Enterprise Security Risk Management (ESRM)

a first introduction

09.00 – 09.30 Meet & Greet
09.30 – 11.00 ESRM
11.00 – 11.30 Coffee Break
11.30 – 12.30 Exercise
12.30 – 13.30 Lunch
13.30 – 14.45 Exercise
14.45 – 15.15 Coffee Break
15.15 – 16.30 Exercise
16.30 – 17.00 Evaluation

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

ESRM Strategic Approach



- ESRM Cycle:
  - Identify & Prioritize Assets
  - Identify & Prioritize Risks
  - Mitigate Prioritized Risks
  - Continuous Improvement
- ESRM Context:
  - Mission & Vision
  - Core Values
  - Operating Environment
  - Stakeholders
- ESRM Foundation:
  - Holistic Risk Management
  - Partnership with Stakeholders
  - Transparency
  - Governance

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.

Enterprise Security Risk Management (ESRM)

a first introduction

09.00 – 09.30 Meet & Greet
09.30 – 11.00 ESRM
11.00 – 11.30 Coffee Break
11.30 – 12.30 Exercise
12.30 – 13.30 Lunch
13.30 – 14.45 Exercise
14.45 – 15.15 Coffee Break
15.15 – 16.30 Exercise
16.30 – 17.00 Evaluation

Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.



Reprinted with permission from ASIS. Permission to reproduce or transmit in any form or by any means must be obtained in writing from ASIS International. All rights reserved.