GSX
GLOBAL SECURITY EXCHANGE

FORMERLY ASIS ANNUAL SEMINAR & EXHIBITS

8-12 SEPTEMBER 2019
McCORMICK PLACE | CHICAGO, IL
GSX.ORG | #GSX19

# ASIS Guideline on ESRM: First Look

September 9, 2019

# Introductions

| | |
|---|---|
| | |
| **David Feeney**<br>Manager, Risk & Financial Advisory<br>Deloitte & Touche LLP<br>dafeeney@deloitte.com | **Toby Houchens**<br>Founder & CEO<br>Alpha Recon<br>thouchens@alpharecon.com |

# ESRM: What?

# 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.

# 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

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

- 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

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

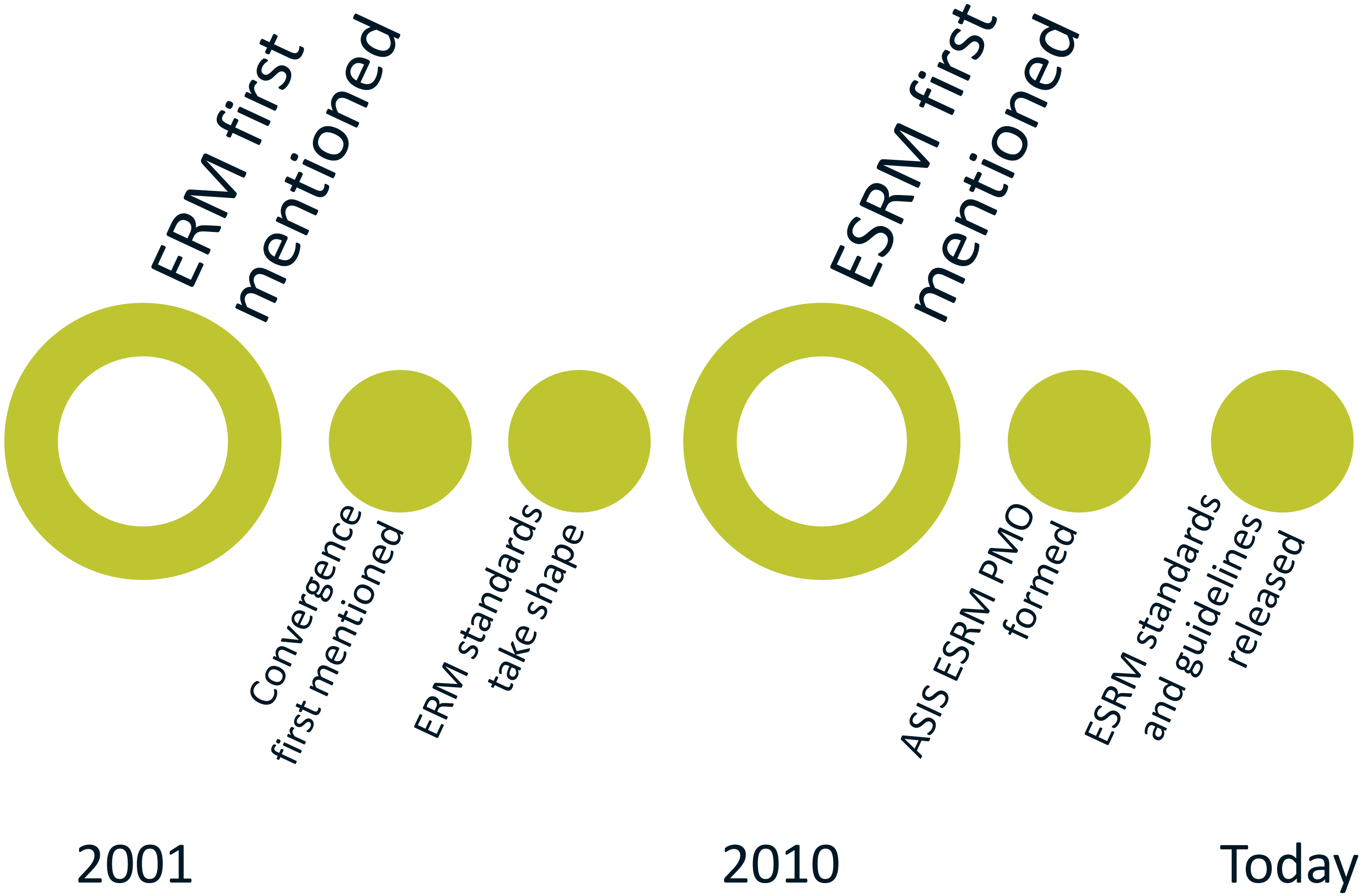
# Specific Roles Within ESRM

| 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.<br>*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)*

# History & Origins of ESRM



ERM first mentioned

Convergence first mentioned

ERM standards take shape

ESRM first mentioned

ASIS ESRM PMO formed

ESRM standards and guidelines released

2001

2010

Today

ASIS INTERNATIONAL

*Advancing Security Worldwide®*

# ESRM: Why?

# 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.

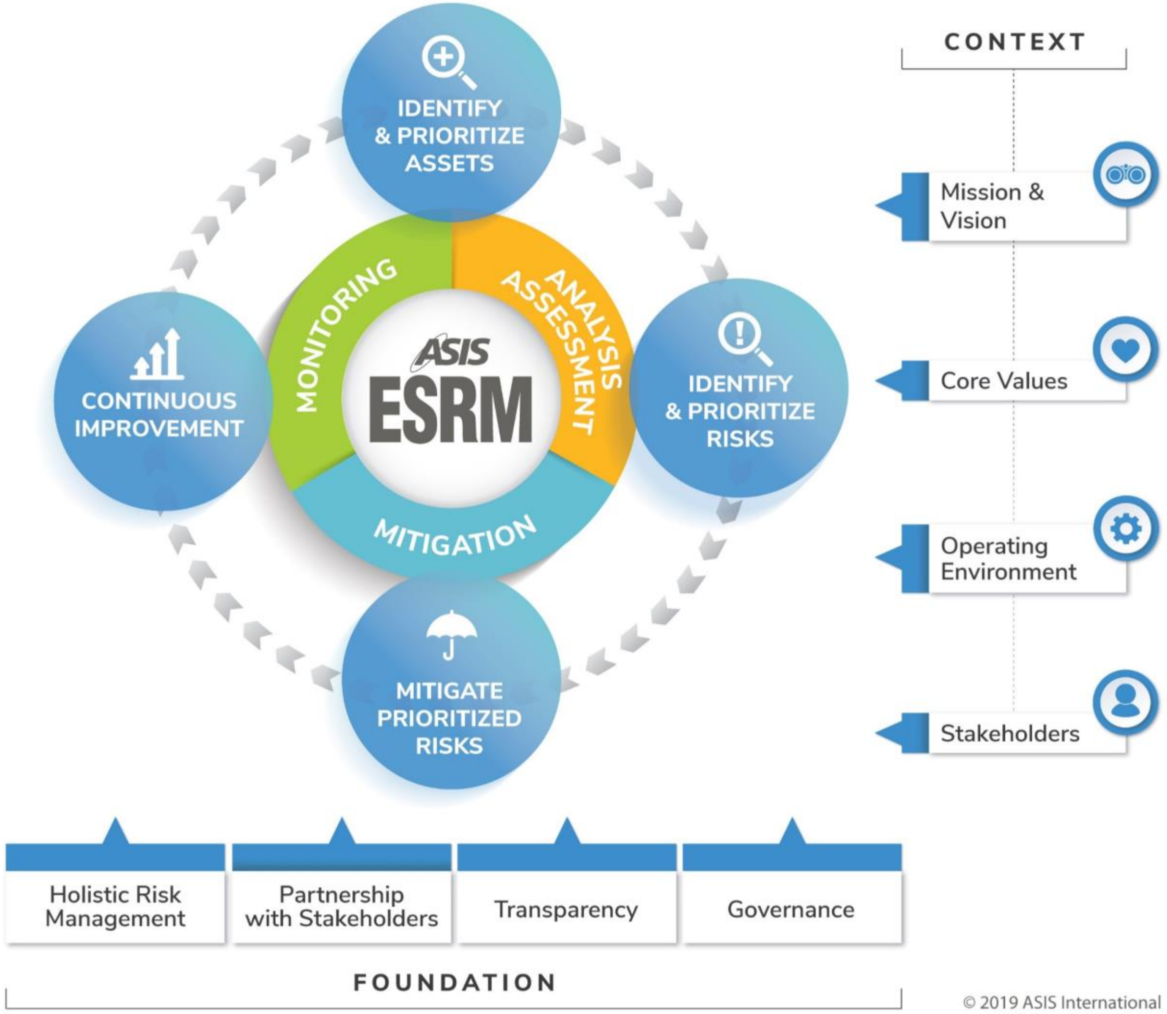
# Potential ESRM Benefits to the Organization

- 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.

ASIS INTERNATIONAL
*Advancing Security Worldwide®*

# ESRM: How?

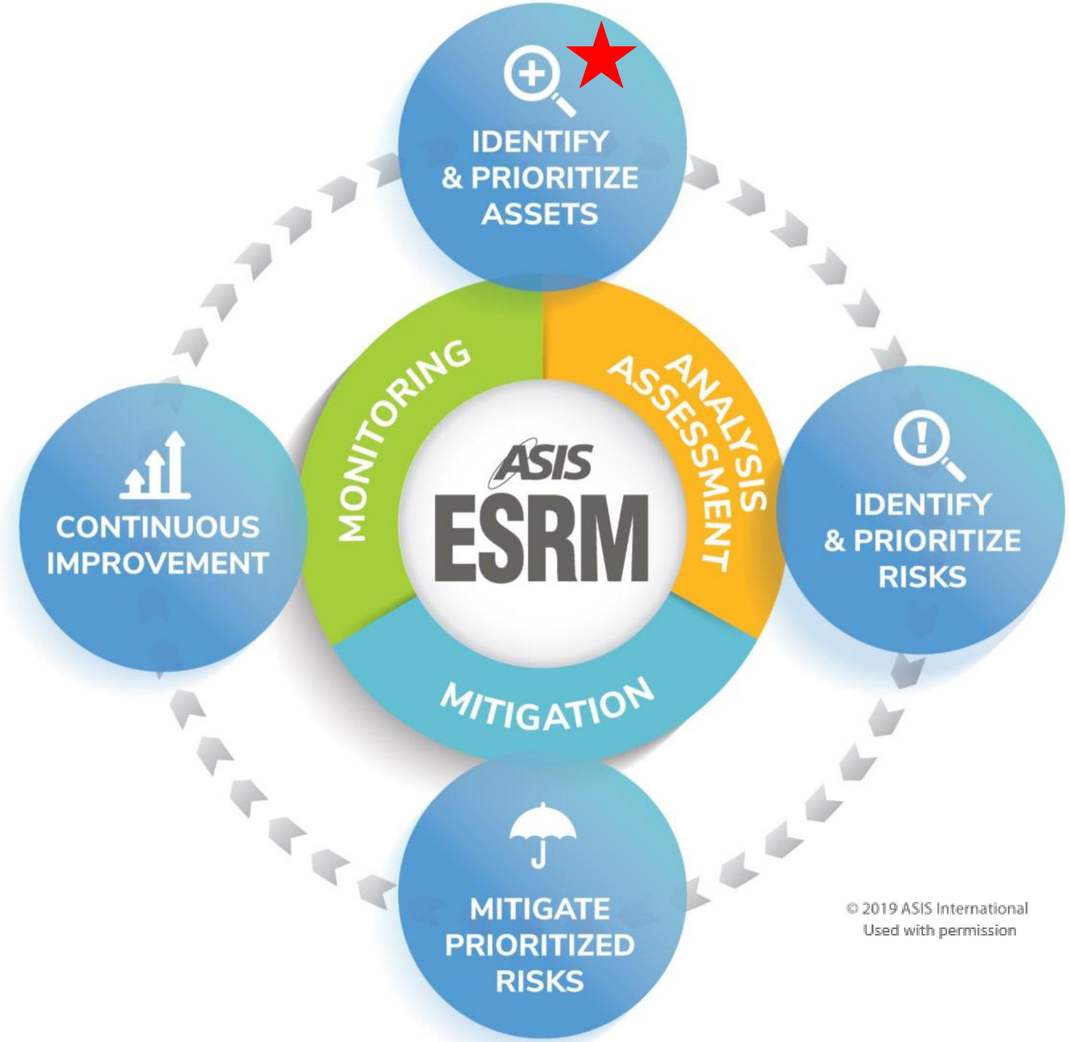
# ESRM Strategic Approach



© 2019 ASIS International
Used with permission

- 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

# ESRM Cycle


IDENTIFY & PRIORITIZE ASSETS
IDENTIFY & PRIORITIZE RISKS
MITIGATE PRIORITIZED RISKS
CONTINUOUS IMPROVEMENT
MONITORING
ANALYSIS ASSESSMENT
MITIGATION
ASIS
ESRM

© 2019 ASIS International
Used with permission

## 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.

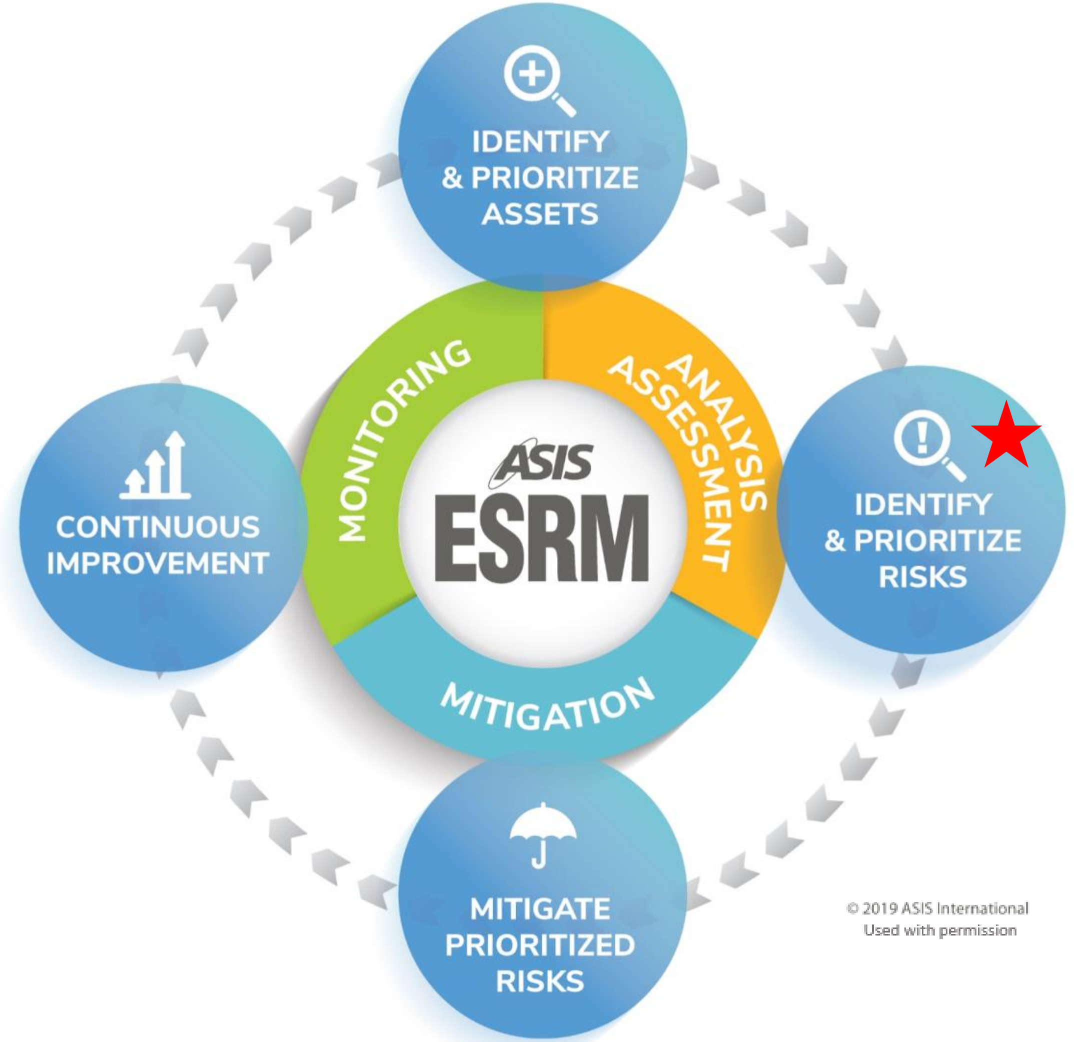
The **Security Manager** helps guide the asset owner through the security risk decision-making process.

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

______________________________

*Activities:*
*Analysis & Assessment*

# ESRM Cycle


IDENTIFY & PRIORITIZE ASSETS
IDENTIFY & PRIORITIZE RISKS
MITIGATE PRIORITIZED RISKS
CONTINUOUS IMPROVEMENT
MONITORING
ANALYSIS ASSESSMENT
MITIGATION
ASIS
ESRM

© 2019 ASIS International
Used with permission

## 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

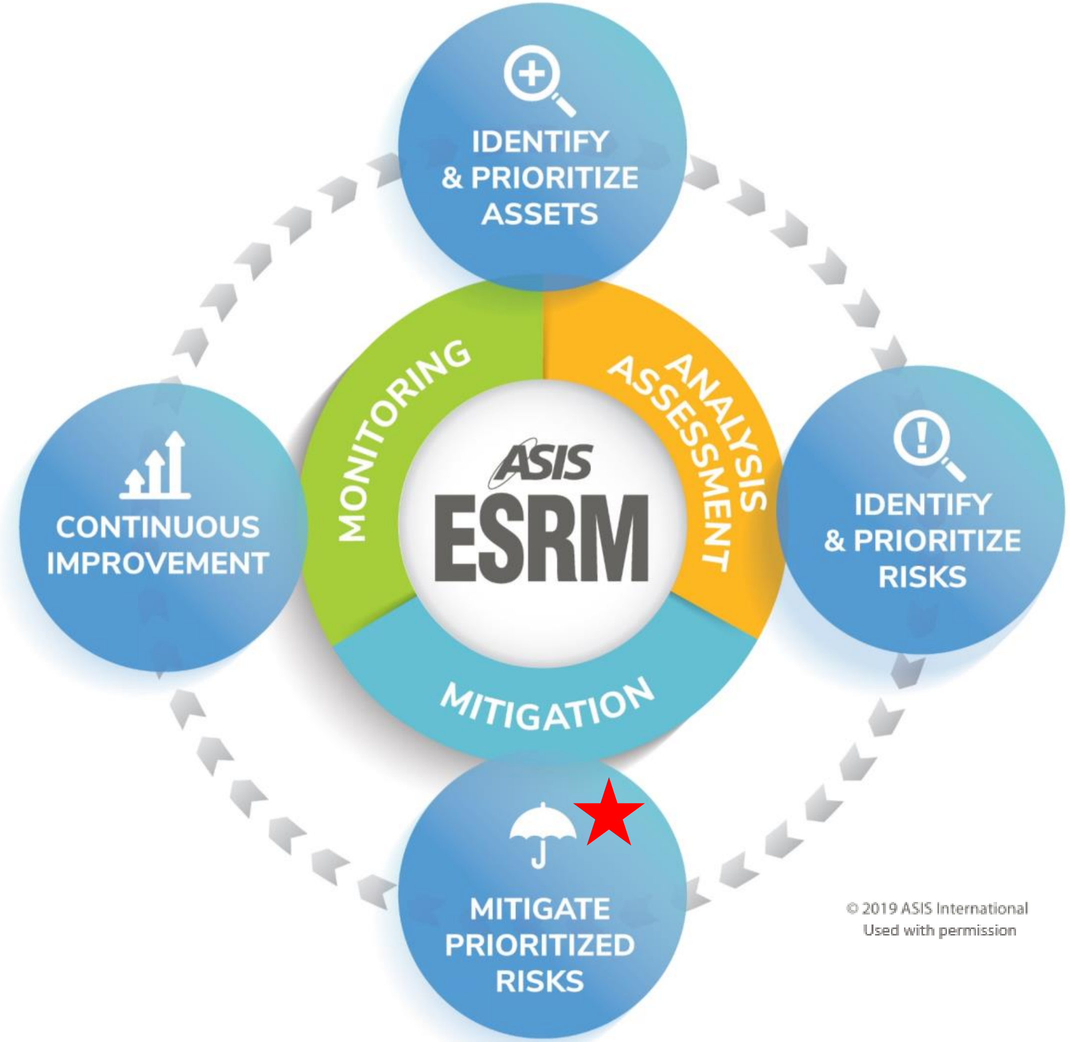
Prioritization is based on guidance from **Senior Management** and input from **Asset Owners**.

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

___________________________________

*Activities:*
*Analysis & Assessment*

# ESRM Cycle


IDENTIFY & PRIORITIZE ASSETS
IDENTIFY & PRIORITIZE RISKS
MITIGATE PRIORITIZED RISKS
CONTINUOUS IMPROVEMENT
MONITORING
ANALYSIS ASSESSMENT
MITIGATION
ASIS
ESRM

© 2019 ASIS International
Used with permission

## Mitigate Prioritized Risks

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

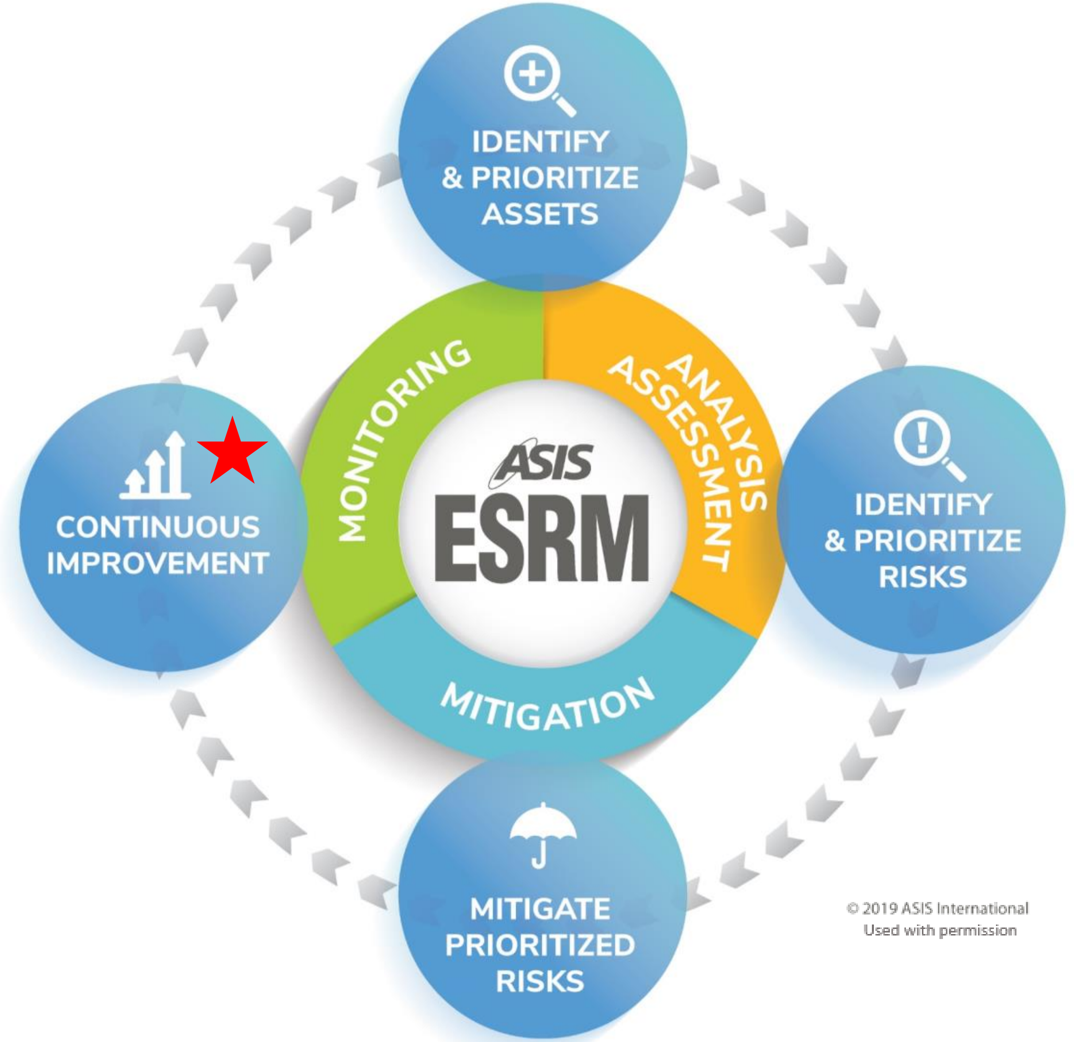
The **Security Risk Management Plan** or **Security Plan** documents the prioritized risks and associated security controls.

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*

# ESRM Cycle


IDENTIFY & PRIORITIZE ASSETS
IDENTIFY & PRIORITIZE RISKS
MITIGATE PRIORITIZED RISKS
CONTINUOUS IMPROVEMENT
MONITORING
ANALYSIS ASSESSMENT
MITIGATION
ASIS
ESRM

© 2019 ASIS International
Used with permission

## 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

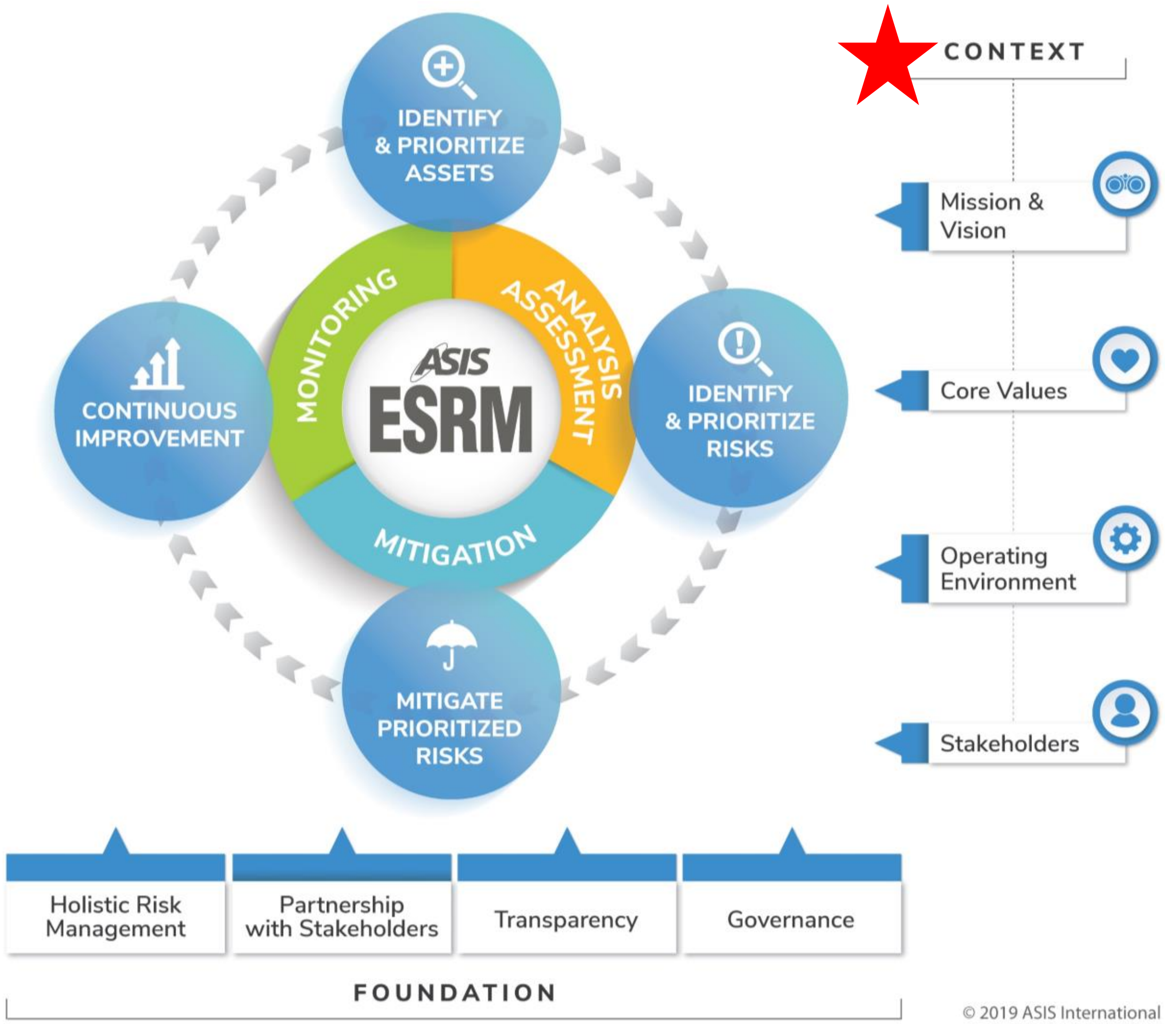
Various **security functions** contribute to continuous improvement of the security program, including but not limited to:

- Incident Response
- Investigations & Analysis
- Information Sharing

______________________________

*Activity:*
*Monitoring*

# The Context of ESRM



# The Context of ESRM

Mission & Vision

- 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

# The Context of ESRM

Core Values

- 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.

# The Context of ESRM

Operating Environment

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.

# The Context of ESRM

Stakeholders

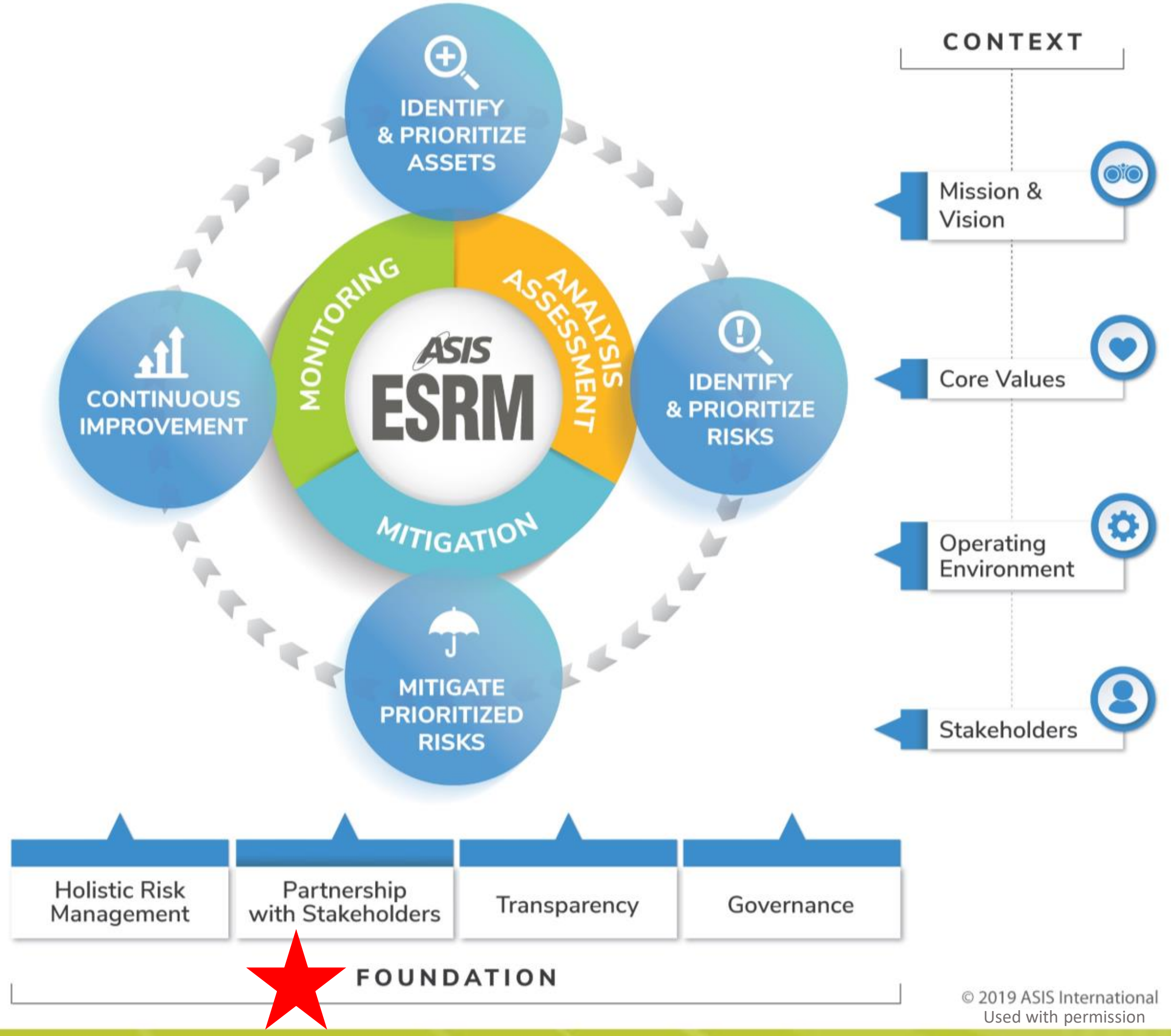
Security professionals should understand the organization's stakeholders and what's important to them.

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.*

# The Foundation of ESRM



© 2019 ASIS International
Used with permission

# The Foundation of ESRM

Holistic Risk Management

- Physical Security | Information Security | Cyber Security
- Crime Prevention | Fraud | Loss Prevention | Executive Protection | Travel Security
- Data Protection | Application Security | Vulnerability Mgmt. | Threat Mgmt. | EDR

- ~~Silos~~
- ~~Boundaries~~

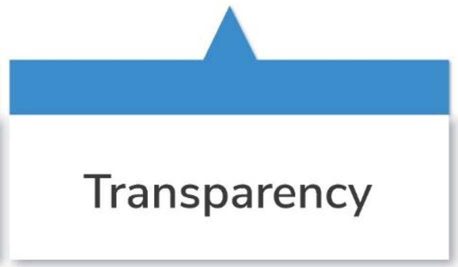
# The Foundation of ESRM

Partnership with Stakeholders

| 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

# The Foundation of ESRM



Transparency

- **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.

# The Foundation of ESRM

Governance

- **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

# ESRM Throughout #GSX19

| Session Date | Session Start | Session End | Title | Session ID |
|---|---|---|---|---|
| 9/9/2019 | 10:30 AM | 11:45 AM | Guiding an Organization Through Digital Transformation | 4115 |
| 9/9/2019 | 1:15 PM | 2:30 PM | Discover Security Program Efficiencies Using an ESRM Approach | 4213 |
| 9/9/2019 | 1:15 PM | 3:15 PM | The Insider: A Significant Threat Which Should Be Addressed | 4217 |
| 9/9/2019 | 2:45 PM | 4:00 PM | Characteristics and Metrics of a Mature Corporate ESRM Program | 4314 |
| 9/9/2019 | 2:45 PM | 4:00 PM | The Importance of Cross-Functional Business Department Collaboration | 4309 |
| 9/10/2019 | 11:00 AM | 12:15 PM | Combining Risk, Response, and Resilience within an ESRM Model | 5113 |
| 9/10/2019 | 2:00 PM | 4:00 PM | Manage Security Risk with ESRM & the NIST Cyber Security Framework | 5216 |
| 9/10/2019 | 3:30 PM | 4:30 PM | How ESRM Is Making a Difference | 5311 |
| 9/11/2019 | 11:00 AM | 12:15 PM | The 2020 Olympics: Red Teaming Enterprise Security Risks | 6114 |
| 9/11/2019 | 2:15 PM | 3:15 PM | The Importance of Risk Literacy in Security | 6212 |
| 9/11/2019 | 3:45 PM | 4:45 PM | Security Incident Insurance: How Does It Help? | 6310 |
| 9/11/2019 | 4:00 PM | 4:15 PM | ESRM Advances in 2019 | HUB-64 |

# Questions and Answers…

# Thank you!

| | |
|---|---|
| **David Feeney**<br>Manager, Risk & Financial Advisory<br>Deloitte & Touche LLP<br>dafeeney@deloitte.com | **Toby Houchens**<br>Founder & CEO<br>Alpha Recon<br>thouchens@alpharecon.com |

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

**About Deloitte**
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.