ASIS INTERNATIONAL

Advancing Security Worldwide®

ENTERPRISE SECURITY RISK MANAGEMENT

Chapters and Councils

ESRM Initiative – Message to Chapters and Councils

The ESRM strategic initiative is well under way and will publish official trainings and other documents in the coming months.

In the meantime, the below information explains the goals of the workstreams as well as a high level presentation defining ESRM and its importance.

ASIS PROGRAM UPDATE

ESRM Board Initiative

ESRM Board Initiative – Charter Executive Summary

In 2016, the ASIS Board of Directors determined that Enterprise Security Risk Management (ESRM) would be a driving underlying force in the global ASIS, International strategic plan.

The stated goal of the board was “to make ASIS members more effective security professionals and more valuable members of their organizations by enabling them to better identify and manage the various aspects of security risks they face… [leading to a] empowered membership, safer enterprises, a more strategic approach to risk, and a more cost-effective security function”.

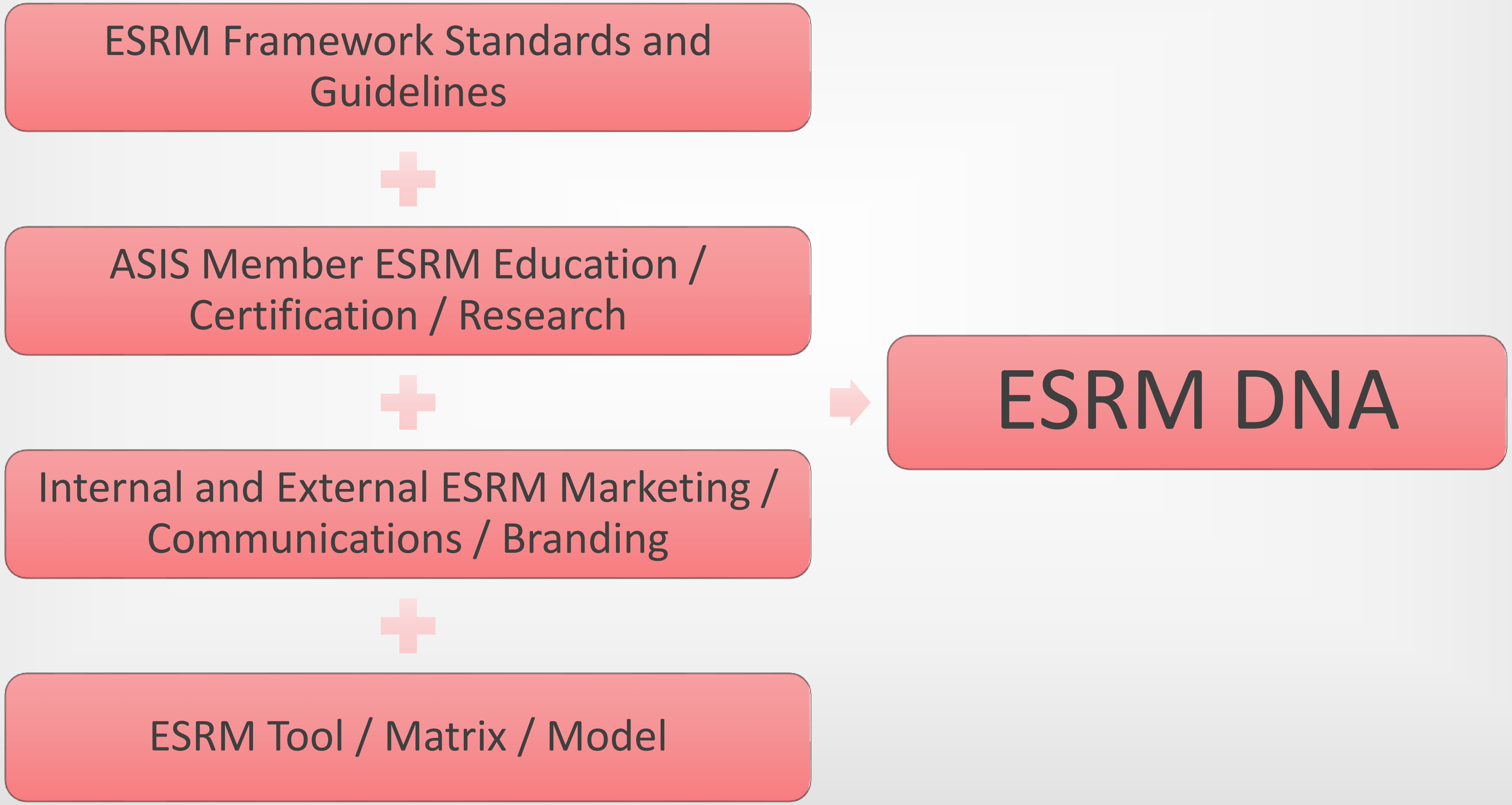
This project will enable that strategic vision through a systematic integration of ESRM principles in ASIS content and education, standards and guidelines, marketing and messaging, certifications, and member support tools.

ESRM Board Initiative – Goals

- Provide educational courses and materials to ASIS membership on ESRM and topics associated with ESRM.
- Educate the security industry at-large on the concepts of ESRM.
- Create an ESRM Standard/Guideline Framework and detailed document set to align existing ASIS standards and recommended practices with the ESRM model.
- Market the ESRM model appropriately and ensure the ASIS brand is tied closely to the ESRM model and methodology.
- Provide tools and collateral to ASIS members to assist them in embracing and implementing ESRM in their security programs

ESRM Board Initiative – Project Scope

The ESRM Board initiative will consist of four working “Value Streams” with deliverables due from each stream.



ESRM Framework Standards and Guidelines

ASIS Member ESRM Education / Certification / Research

Internal and External ESRM Marketing / Communications / Branding

ESRM Tool / Matrix / Model

ESRM DNA

Internal and External ESRM Marketing, Communications, & Branding

The Marketing and Communications Workstream is crafting internal and external ESRM messages that will be presented at GSX in September.

If your Council or Chapter would like to hear more about ESRM messaging, please reach out to Tim Wenzel, CPP and Ray O’Hara, CPP at ESRM@asisonline.org.

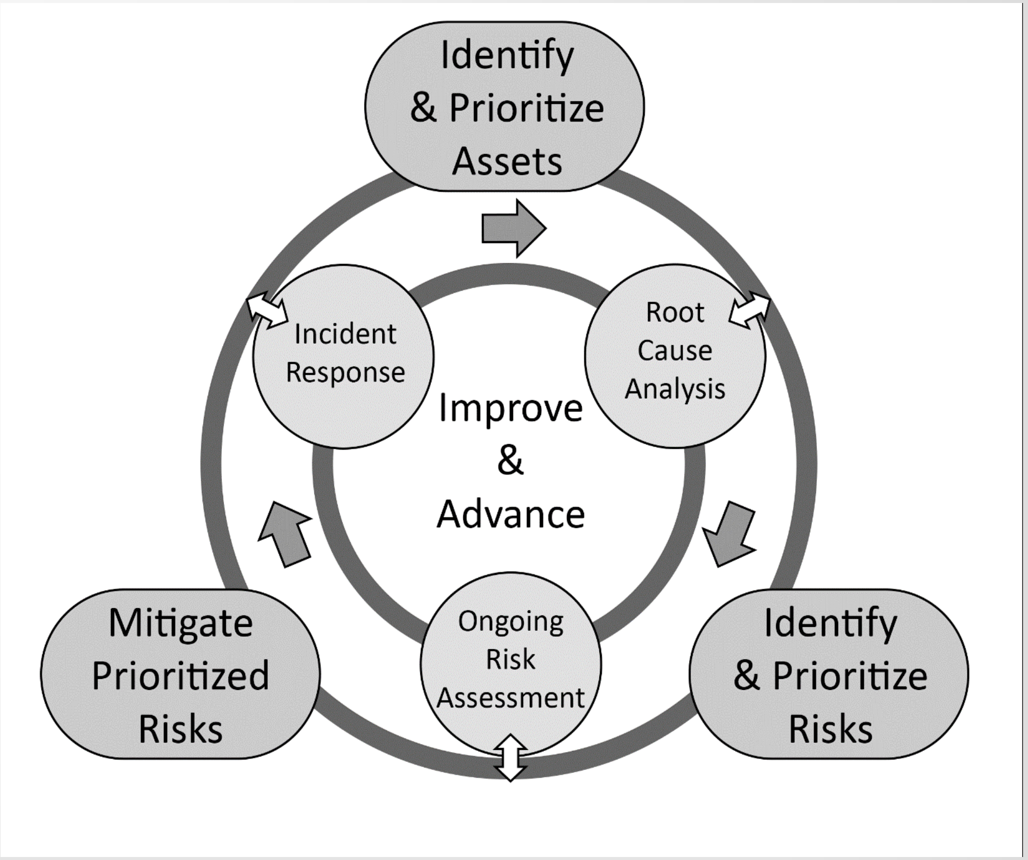
ASIS INTERNATIONAL

Advancing Security Worldwide®

ENTERPRISE SECURITY RISK MANAGEMENT

ESRM DEFINED

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


Identify & Prioritize Assets
Root Cause Analysis
Identify & Prioritize Risks
Ongoing Risk Assessment
Mitigate Prioritized Risks
Incident Response
Improve & Advance

SECURITY IS ABOUT RISK MANAGEMENT

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.

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.

ESRM AND SECURITY

A mature ESRM program encompasses all aspects of security risk mitigation practices: physical security, cyber security, information security, loss prevention, organizational resilience, workplace violence, fraud, threat management, brand protection, travel safety, business continuity, and all other practices undertaken to prevent security risk impacts to the enterprise.

WHAT IS ESRM?

- ESRM is strategic, not tactical
- Creates a link between business objectives and risk management
- Shared responsibility
- Final decision = business
- Security “manages”, in partnership with business
- Covers all aspects/areas of security
- It’s cyclical

WHAT ESRM ISN'T

- It's not ”convergence”:
  - Converged integrates IT and Physical under one team
  - The degree of integration identifies the degree of convergence
  - First efforts were based on budget
- 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

SO, WHY ESRM?

- You gain intimate knowledge of your organization
- You get to speak to diverse stakeholders, and learn what they consider is important to them and the company
- You learn your organization’s business objectives
- You identify risks and help the business achieve objectives
- You support the legal responsibilities of the business

SO, WHY ESRM?

- You become “aware” of your role in the organization:
  - Identify risks to the right executive
  - Provide objective perspective on the risk(s)
  - Let the executive decide
- We don’t “accept” risks – that’s not our job!
- We identify risks, and provide SME during the risk management process

SO, WHY ESRM?

- Organizations have a risk based view of the protection of the business across all relevant fields. Such as, business continuity, cyber risk, personnel vetting
- Provides security structures which are best practice and defensible

REFERENCES

- ISO/Guide 73:2009(en) - Risk management. https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en
- ISO 704, Terminology work — Principles and methods
- ISO 860, Terminology work — Harmonization of concepts and terms
- ISO 3534-1, Statistics — Vocabulary and symbols — Part 1: General statistical terms and terms used in probability
- ISO 9000, Quality management systems — Fundamentals and vocabulary
- ISO 10241, International terminology standards — Preparation and layout
- ISO 31000:2009, Risk management — Principles and guidelines
- ISO/IEC Guide 2, Standardization and related activities — General vocabulary
- ISO/IEC Guide 51, Safety aspects — Guidelines for their inclusion in standards

PLEASE SEND QUESTIONS TO:

ESRM@ASISONLINE.ORG