ASIS School of ESRM

Session 4 - Building Foundational Relationships and a Holistic ESRM Program

ASIS INTERNATIONAL®
JAMAICA CHAPTER

Building Foundational Relationships

Remember:
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.

Remember these?

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?

Doing Security “The Old Way”

Managing a security program was about taking RESPONSIBILITY AND BLAME

- We took a reactive or compliance-based approach
- We decided what the business needed
- We were often activity driven and measured effectiveness in hours and tasks
- We had limited executive level interaction or visibility

When We Transition to ESRM

Managing a security function is about driving
RISK MANAGEMENT IN LINE WITH BUSINESS TOLERANCE

- We take a collaborative approach
- We partner with leaders to decide what the business needs
- We are risk driven and measure effectiveness in incident levels and staying within tolerances
- We are business-focused and require executive level interaction and risk governance

Why is the ESRM Partnership approach important?

- ESRM brings an objective and measurable viewpoint to security decision making
- Partnership links security decisions to business strategies to support business success
- Security has a more proactive posture when driven by the desire of the business to protect its assets

When we embrace partnership with our business leaders… we put the security risk decisions in the hands of the people truly impacted by the risks

What Does an ESRM Partnership Look Like in Real Life?

Security's Role - Trusted Advisor

- Identify and manage security risks to valuable organization assets
- Monitor risks to ensure they stay within defined tolerance levels
- Provide security expertise on mitigation options
- Carry out security tasks to mitigate security risks in support of the security / business partnership.

Business' Role - Decision Owner

- Understand the role of the security department in helping the business carry out its mission
- Define an acceptable level of security risk tolerance to valuable assets
- Make well-educated decisions on security risks and mitigation options
- Support the security team in carrying out functional activities that protect organization assets

Building Partnerships and Trusted Relationships

3. Link security success to business success

- show how you support critical mission activities
- look for ways to leverage security activities to benefit other functions
- continually revisit needs and solutions

1. Position Security Leaders as Trusted Advisors

- identify key line-of-business executives who are critical for success and meet with them
- explain the philosophy of ESRM and the role of security in managing – not owning – security risk.
- reach agreement with your partners that the role of security in the organization is to identify risks to business assets, and to work with the asset owners to respond to those risks or accept them.
- provide quality information and recommendations
- implement mitigations in line with what the business wants

More on these steps in sessions 4 and 5!

2. Demonstrate the immediate value of security to the organization

- report meaningful metrics (impact not “hours”)
- communicate the benefits you are bringing to all aspects of the business

ASIS INTERNATIONAL®
JAMAICA CHAPTER

Holistic ESRM Program

Begin to Build Your Holistic ESRM Program

1. Security Governance
2. Security Charter
3. Security Policy
4. Security Tactical Activity Updates

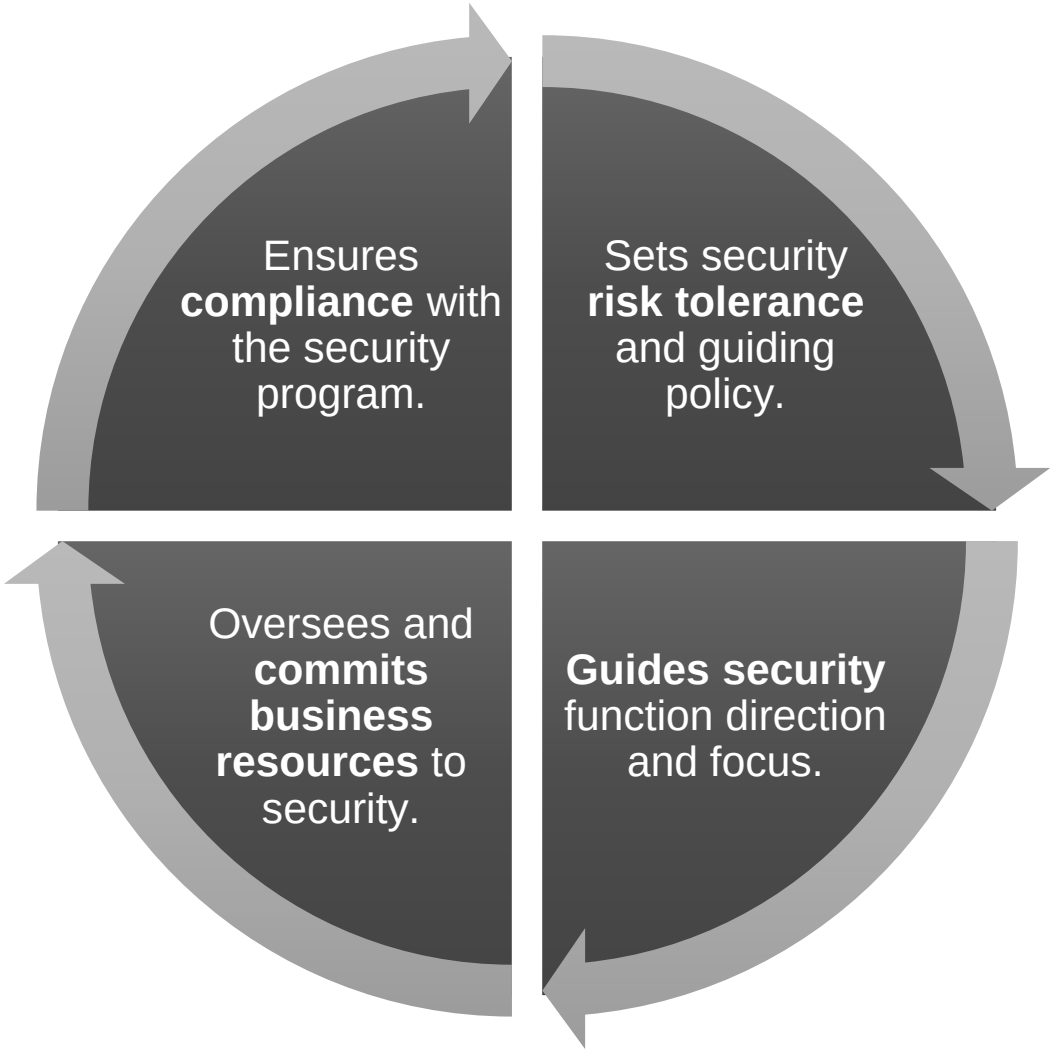
Begin to Build Your Holistic ESRM Program

1. **Security Governance**
2. Security Charter
3. Security Policy
4. Security Tactical Activity Updates

1 - Security Governance

- Governance controls:
  - **How are decisions are made** and carried out?
  - **Who has the authority and responsibility** to do make those decisions?

What Does a Security Governance Council do?

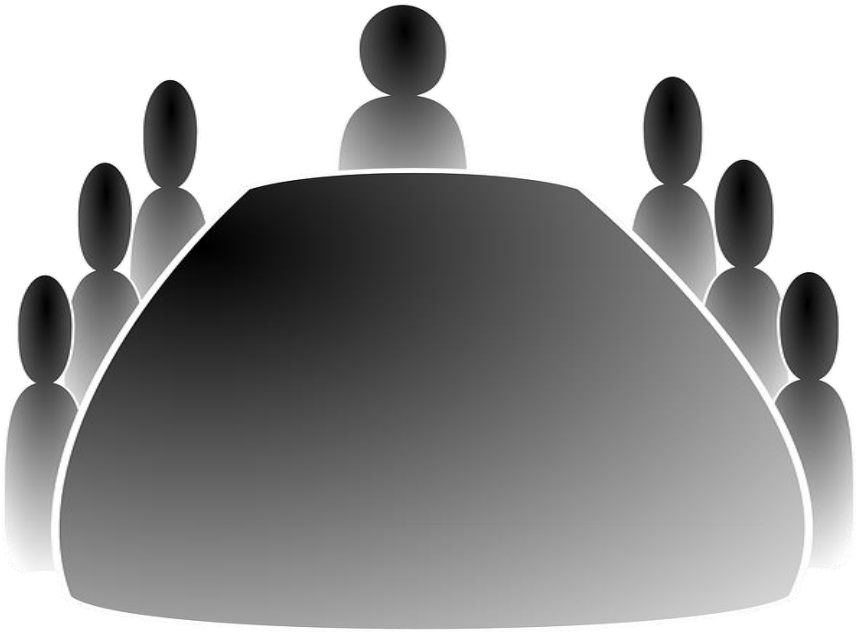


How Do You Set Up A Security Governance Council?

1. Define a Council **structure** that fits the company needs
2. Determine the Security Council **members**
3. Define the **mission and goals** of the Council in a policy or charter
4. Define security **risk tolerances** and key risk indicators
5. **Manage the security risk program** for the organization according to the design

What Does a Security Governance Council Look Like?

- Security Council structure will vary with the needs of your organization
- Security risk management must be **led by the risk owners**
- **Security**, as a stakeholder, should be ON the council, but **not in charge of it**
- D**ecisions must come from the business**



4 - Begin to Build Your Holistic ESRM Program

1. Security Governance
2. **Security Charter**
3. **Security Policy**
4. Security Tactical Activity Updates

4 - Begin to Build Your Holistic ESRM Program

Documents Created and Signed Off By the Security Council

- **Security Council Charter**
  - The need for a**udit and oversight**
  - The r**ights of all stakeholders**
  - The need for **disclosure and transparency** in management
  - The **role of management** in all of these
  - *E-HANDOUT - ASIS School of ESRM - Session 4 - Sample Security Council Charter*

- **Security Policy**
  - Develop a written E**SRM-based security policy** that outlines the agreed upon role of security, and ensure that it is endorsed by the executives in charge.
  - *E-HANDOUT - ASIS School of ESRM - Session 4 - Sample Security Policy*

4 - Begin to Build Your Holistic ESRM Program

1. Security Governance
2. Security Charter
3. Security Policy
4. **Security Tactical Activity Updates**

Phased Development / Updates of Tactical Activities

Start with a program or part of an existing program and develop a strategy on how to implement the ESRM practice. Invite stakeholders into those strategy sessions.

Prototype a Pilot Process

- Involve the **strategic partners who are the most impacted** and brainstorm with them on how to create a program that is satisfactory to all stakeholders.
- Work through a **prototype of one existing function** or task in the program.
- **Document a proposal** for your stakeholders. **Anticipate challenges** and changes.
- Focus on the **long-term benefits**, beyond individual programs or projects. Take and incorporate feedback as necessary.
- Identify potential **ongoing reporting and metrics** for the process.
- Ensure that the model is **repeatable and adaptable.**

Implement Your Updated Tactical Change

1. Pick a **date to start** using the new tactic in daily work.
2. **Announce the change** and ensure that all strategic partners know it is beginning.
3. **Seek (more) feedback** from executives, impacted business units, and security practitioners outside your organization. Continue to iterate the methodology, and practice as needed.

Keep Going!

4. Consistently **reinforce the ESRM principles** through education, conversation, and program maturity.
5. **Expand the practice into strategy**, and more areas of program development.
6. Pick a new process, procedure, or aspect of your program and **begin another round of ESRM implementation**.

ESRM Toolbox

ESRM Maturity Model

ASIS INTERNATIONAL®

Enterprise Security Risk Management (ESRM) Community

MATURITY MODEL (PROOF OF CONCEPT) 2021

By Paul Mercer, Chair of ASIS Maturity Model Team

ASIS ESRM Community

ASIS SUBJECT AREA COMMUNITY

Enterprise Security Risk Management (ESRM)

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

Questions…?

5 Minute Break