

2022 ESRM Maturity Model

*Developed by the ESRM Community's
Maturity Model Team*



Table of Contents

Introduction	3
How to use this Maturity Model.....	4
Phase 2: Maturity model questions	5-14
Culture.....	5-6
Context	7-8
Stakeholders.....	9-10
Risk Management.....	11-12
ESRM Governance	13-14
Maturity Model Table	15-17
Recommended Reading	18

Introduction

The new ESRM Maturity Model has been designed to provide adopters of ESRM philosophy an easy to use reference to establish an organization’s current level of maturity and guidance on how to progress to the next level of maturity. It follows two years of research by the ESRM Steering Committee and builds on the excellent work to produce the initial maturity model in 2019.

ESRM philosophy is suited equally to public and private enterprises, large and small. Smaller organizations may establish ESRM processes and governance using an existing management group or committee.

Throughout this document, the terms ‘security leadership’ and ‘security professional’ refer to those responsible for all aspects of security, including PhysSec, CyberSec, Infosec, Business Continuity, Background Investigations, Access Management, Intelligence, Security Governance, and Security Compliance. In addition, the term ‘Asset Owner’ refers to business managers with overall responsibility for business assets, including facilities management, manufacturing and supply chain, and the term stakeholder refers to any person or organization with an interest or concern in security, including suppliers and service providers.

Elements of Maturity/ Maturity Level	Level 1 (Initial)	Level 2 (Repeatable)	Level 3 (Defined)	Level 4 (Managed)	Level 5 (Optimized)
Culture					
Context					
Stakeholders					
Risk Management					
ESRM Governance					

How to Use this Maturity Model

- 1** Review your report from the Maturity Model tool.
- 2** Your maturity level assumes you would be able to answer Yes to all lower level questions. Please review the questions at the lower maturity level to ensure alignment. If you cannot answer Yes to all lower level questions, adjust your level accordingly.
- 3** Once you have confirmed your maturity level, browse the [ESRM resource page](#). Resources listed here will assist you in achieving the next maturity level.

Elements of Maturity/ Maturity Level	Level 1 (Initial)	Level 2 (Repeatable)	Level 3 (Defined)	Level 4 (Managed)	Level 5 (Optimized)
Culture					
Context					
Stakeholders					
Risk Management					
ESRM Governance					

Phase 2: Maturity Model Questions

CULTURE LEVEL 1 – INITIAL

Security leaders representing all security functions have partnered with asset owners and proposed policies and procedures to align ESRM with organizational strategies.

Questions

- | | | |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Do you know who all of the leaders are who perform or represent security activities? (Physical, IT, Cyber, Fraud, Privacy, Etc.) |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Has the security department identified the appropriate asset owner for all prioritized assets who are most accountable for all security risks? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Has the security leadership established relationships with function/department business leaders across the enterprise? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 4. Have you discussed the fundamental partnership and risk philosophies of ESRM with all identified asset owners/ partners responsibility? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 5. Have you discussed and gotten an agreement on how to align existing security policies and procedures with all responsible leaders identified in questions 1 and 2? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |

CULTURE LEVEL 2 – REPEATABLE

The tenets of ESRM have been socialized with security professionals across all security functions in the organization through training/education.

Questions

- | | | |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Have you trained/presented all security personnel on the basic tenets of ESRM as it relates to their position in the organization? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Have you documented the ESRM cycle and approach as the foundation/charter for all security functions in the organization? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |

CULTURE LEVEL 3 – DEFINED

Security leaders representing all security functions have reached a partnership agreement with asset owners to manage security risks in the ESRM model.

All security policies and procedures relevant to asset owners are documented and aligned with ESRM appropriately and updated on a routine basis.

Questions

- | | | |
|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Have security leaders representing all security functions jointly reached a partnership agreement with asset owners to manage security risks? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Have all security policies & procedures relevant to asset owners been documented and aligned with ESRM appropriately? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Have all security policies & procedures relevant to asset owners been reviewed, agreed upon, and updated within the past year? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |

Phase 2: Maturity Model Questions

CULTURE LEVEL 4 – MANAGED

Security professionals are unified across all security functions and actively manage security risks with asset owners and stakeholders according to established & documented ESRM processes enterprise-wide.

Questions

- | | | |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Are security professionals, across all security functions, successfully supporting security risk management with asset owners? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Are security professionals supporting the management of security risk in a unified manner with asset owners? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Is security risk being managed in accordance with established & documented ESRM processes enterprise-wide? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |

CULTURE LEVEL 5 – OPTIMIZED

ESRM has been fully adopted as the organization's integrated approach to security risk management. Top management, asset owners, stakeholders and security professionals are unified across the enterprise, routinely work together to manage/control security risk and drive continuous improvement.

Questions

- | | | |
|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Has a documented ESRM approach been successfully & universally adopted across the entire organization? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Do security professionals across all security functions operate in a unified manner, to collectively identify, manage and control security risks in support of asset owners who own the risk? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Does top management support security professionals and asset owners to drive continuous improvement of the organization's approach? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |

Phase 2: Maturity Model Questions

CONTEXT LEVEL 1 – INITIAL

Security leaders representing all security functions clearly understand ESRM within the context of the organization's on, values, business processes, regulations, stakeholder responsibilities, and operating environment.

Questions

- | | | |
|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Do security leaders understand the mission and goals of the overall enterprise and the industry in which it operates? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Do security leaders understand the ESRM philosophy and approach? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Do security leaders have a general understanding of the security risks impacting the organization? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 4. Do security leaders understand the context of the security risks to the organization and how the same risk impacts other functions and areas of the organization differently? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |

CONTEXT LEVEL 2 – REPEATABLE

Security leaders representing all security functions can articulate how ESRM can support all business functions through socialization of ESRM and appropriate strategy outlines for implementation.

Questions

- | | | |
|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Do security leaders have adequate knowledge and training on ESRM topics to convey to business functions the potential impact of security risks? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Do security leaders have adequate access to engage in security risk management decisions with business functions? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Do security leaders have adequate knowledge of business functions to express security risks in terms that will resonate with business function leaders? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |

CONTEXT LEVEL 3 – DEFINED

Security professionals representing all security functions can demonstrate how their functions can help asset owners and stakeholders manage security risk across the organization in line with ESRM processes.

Questions

- | | | |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Do security professionals actively engage asset owners when new security risks arise? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Do security professionals provide asset owners with risk treatment options and recommendations? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Do asset owners sign off on the security recommendations/options presented by enterprise security professionals? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 4. Do security professionals provide sufficient awareness to asset owners of the security issues they may face? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |

Phase 2: Maturity Model Questions

CONTEXT LEVEL 4 – MANAGED

Security professionals are unified across all security functions and working with their teams, asset owners, and stakeholders to monitor and review any changes that might impact the enterprises' profile.

Questions

- | | | |
|------------------|-----------------|---|
| <hr/> YES | <hr/> NO | 1. Are risk assessments shared across disciplines and leveraged to identify assets and risks to ensure all are considered in the ESRM process? |
| <hr/> YES | <hr/> NO | 2. Are security risk monitoring activities performed and shared across all disciplines and leveraged to identify new or emerging security risks in the enterprise proactively? |
| <hr/> YES | <hr/> NO | 3. Do asset owners actively engage security professionals to discuss security risks? |
| <hr/> YES | <hr/> NO | 4. Do security professionals coordinate with asset owners to develop risk treatment options and recommendations? |
| <hr/> YES | <hr/> NO | 5. Do asset owners actively affirm a risk treatment option? |
| <hr/> YES | <hr/> NO | 6. Are security risks included on the enterprise risk register? |
| <hr/> YES | <hr/> NO | 7. Do asset owners engage their key staff in supporting effective security risk management throughout the organization? |
| <hr/> YES | <hr/> NO | 8. Do security leaders ensure that effective post-incident reviews and root cause analysis is carried out after any significant event? |

CONTEXT LEVEL 5 – OPTIMIZED

The organization conducts ESRM proactively. Security leaders are unified across all security functions and work with asset owners who take ownership of their own security risk. Security professionals & asset owners work together to continuously improve ESRM through open, real-time communication with the top management, asset owners, and other stakeholders.

Questions

- | | | |
|------------------|-----------------|--|
| <hr/> YES | <hr/> NO | 1. Does an ongoing training program exist to ensure all employees are trained to promote and improve a dynamic ESRM security culture? |
| <hr/> YES | <hr/> NO | 2. Is the risk register actively managed across business functions, prioritized according to the organization values, business processes, regulations, stakeholder responsibilities, and operating environment? |
| <hr/> YES | <hr/> NO | 3. Are you able to achieve near real-time ESRM capability? |

Phase 2: Maturity Model Questions

STAKEHOLDERS LEVEL 1 – INITIAL

Security leaders representing all security functions have identified asset owners and key stakeholders across the enterprise and have begun socializing ESRM philosophy.

Questions

- | | | |
|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Has the Security Department identified all enterprise assets (tangible and intangible) considered in the ESRM program? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Do you know who all the different stakeholders are who have responsibility for the enterprise? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Do these stakeholders include the Board, the C-suite, IT, Audit, Legal, Finance, Privacy, Health and Safety, Cybersecurity, Facilities, HR? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 4. Have you engaged with these stakeholders and begun a discussion around the security risks to their assets? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 5. Are all your security colleagues across the enterprise similarly engaged with these stakeholders? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 6. Have you established a plan/method to introduce ESRM across the enterprise through emails, conference calls, coffee and lunch meetings? |
| YES | NO | |

STAKEHOLDERS LEVEL 2 – REPEATABLE

Security leaders representing all security functions have identified, understood, and documented ESRM stakeholder relationships and defined and agreed on roles and responsibilities concerning security risk management support to asset owners.

Questions

- | | | |
|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Has your engagement with stakeholders enabled you to understand their roles regarding ESRM? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Have you documented these roles and agreed on their responsibilities regarding ESRM? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Have you agreed and documented the security team's management support for these asset owners? |
| YES | NO | |

STAKEHOLDERS LEVEL 3 – DEFINED

Security professionals representing all security functions and asset owners have documented the identification, prioritization and mitigation of security risks.

Questions

- | | | |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Have you worked with stakeholders to identify and document the key security risks to the enterprise and individual assets and functions within the enterprise? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Have you worked with all your security colleagues to prioritize and document security risks? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Have you agreed to a collaborative and documented response to mitigate these risks? |
| YES | NO | |

Phase 2: Maturity Model Questions

STAKEHOLDERS LEVEL 4 – MANAGED

Security leaders are unified across all security functions enterprise-wide and have implemented documented processes to ensure stakeholder engagement continuity. Partnerships continue to progress as personnel change among asset owners and other stakeholders.

Questions

- | | | |
|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Are all security leaders and functions working closely together on all security risks? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Are internal and external security threats and risks managed holistically in partnership with all impacted groups? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Are your security teams engaging with the stakeholders in a collaborative approach that is reviewed and updated annually? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 4. Are you notified regularly on changes in personnel and responsibility for asset ownership and security risk management? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 5. Are you notified on a six-monthly basis of new stakeholders or changes in their functions, personnel and policies? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 6. Is all of the above documented? |
| YES | NO | |

STAKEHOLDERS LEVEL 5 – OPTIMIZED

Security leaders are unified across all security functions enterprise-wide and working directly with top management to ensure an integrated and proactive approach in preparing for anticipated changes in asset owners and key stakeholders and are planning for continuity of operations in the event of unanticipated changes.

Questions

- | | | |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Are you and all security leaders actively working with the Board and senior management to ensure ESRM is fully integrated into the organization's strategy and policies? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Are you and all security leaders, the Board and senior management planning to progress ESRM and prepare for changes in asset owners? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Are all stakeholders planning for continuity of operations and forecasting unanticipated changes? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 4. Are Risk mitigation plans and activities and associated roadmaps updated regularly to account for changing risk environments? Original (1. 5.10) |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 5. Does an independent 3rd party audit all of the above? |
| YES | NO | |

Phase 2: Maturity Model Questions

RISK MANAGEMENT LEVEL 1 – INITIAL

Security leaders representing all security functions have engaged with asset owners and stakeholders to document existing security risks across the enterprise and align ESRM with the organization's arching risk management approach.

Questions

- | | | |
|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Has the security department discussed & agreed to a security risk management approach with top management aligned with the organization's arching risk management approach? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Has the security department identified all asset owners within the organization with appropriate authority to discuss & agree on security risks to their assets? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Has the security department identified all stakeholders relevant to the organization who may play a role in determining effective mitigation of security risk to the enterprise's critical asset? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 4. Has the security department documented risk identified with each asset owner? |
| YES | NO | |

RISK MANAGEMENT LEVEL 2 – REPEATABLE

Security leaders representing all security functions have agreed with asset owners and codified/ documented security risk management methodologies aligned to the organization's arching risk management approach. These methodologies outline the method of prioritization of the protection of assets, identifying and evaluating security risk, and determining the appropriate risk mitigation strategy.

Questions

- | | | |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Has the security department codified/documentated a security risk management approach with asset owners? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Are security professionals across all security functions unified in a standard and integrated approach to security risk assessment? Do they work together to develop suitable mitigation strategies with asset owners? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Does the agreed-upon security risk management methodology consider the prioritization of assets and a means of identifying and evaluating risk? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 4. Is the assignment of appropriate mitigation linked directly to risks identified against each asset? |
| YES | NO | |

Phase 2: Maturity Model Questions

RISK MANAGEMENT LEVEL 3 – DEFINED

Asset owners have taken ownership of and understand their security risk.

Questions

- | | | |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Are Security professionals representing all security functions, working directly with asset owners in an integrated manner to monitor & manage security risks to their assets? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Have asset owners defined their own risk tolerance, and do the security professionals supporting each asset owner understand these risk tolerances in relation to a security risk? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Have asset owners acknowledged ownership of risk to their assets and actions for mitigations of those risks? |
| YES | NO | |

RISK MANAGEMENT 4 – MANAGED

Security leaders unified across all security functions actively monitor the security risk management strategy's effectiveness. Security leaders engage with top management, asset owners, and other stakeholders to measure and improve effectiveness across the enterprise.

Questions

- | | | |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Have security leaders across all security functions adopted the security risk management methodology agreed upon with top management? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Do security leaders across all security functions monitor the progress of an integrated security risk management approach? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Do security leaders across all security functions engage with asset owners & relevant stakeholders as an integrated security function to measure and improve the enterprise's security risk management approach? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 4. Do all security leaders across all security functions engage with top management as an integrated security function to report the effectiveness of the security risk management approach across the enterprise? |
| YES | NO | |

RISK MANAGEMENT LEVEL 5 – OPTIMIZED

Security leaders are unified across all security functions and work routinely with asset owners and stakeholders to mitigate security risks across the enterprise proactively.

Questions

- | | | |
|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Are security leaders across all security functions working routinely with asset owners/stakeholders to proactively mitigate security risks across the enterprise? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Has ESRM been adopted consistently across the entire enterprise? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Has ESRM been successfully aligned with the organization's overarching risk management process? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 4. Has the adoption of a fully mature ESRM philosophy enhanced real-time decision making across the organization? |
| YES | NO | |

Phase 2: Maturity Model Questions

ESRM GOVERNANCE LEVEL 1 – INITIAL

Security leaders representing all security functions have agreed on an ESRM Governance requirement with top management, aligned to broader organizational governance processes.

Questions

- | | | |
|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Is there policy guidance or other documentation of organizational top managements' commitment to ESRM and its intended relationship to other organizational functions and governance processes? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Does the security departments goals clearly align with and commit to an ESRM philosophy and approach? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Have security department leadership and all function/department business leaders across the enterprise drafted a foundation for the development of ESRM policy? |
| YES | NO | |

ESRM GOVERNANCE LEVEL 2 – REPEATABLE

A documented security governance charter has been established, an ESRM governing body / Security council has been formed, aligned to the organization's and structure, and all members understand their roles.

Questions

- | | | |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Has an ESRM governing body/security council been formed to govern security risk and the security program?? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Top management formally approved a security governance charter establishing an ESRM governing body/security council? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Is the ESRM governance structure aligned with organizations and structure? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | 4. Do the actions and activities of the security council demonstrate an understanding of their roles in regards to ESRM governance? |
| YES | NO | |

Phase 2: Maturity Model Questions

LEVEL 3

ESRM GOVERNANCE LEVEL 3 – DEFINED

An ESRM governing body is actively overseeing ESRM and tracking positive outcomes of the ESRM approach.

Questions

- | | | |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Has the ESRM governing body defined goals and objectives for implementing ESRM in the organization? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Is there evidence that ESRM governance procedures/processes and activities of the governing body support positive outcomes of the ESRM approach? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Does the ESRM governing body actively document risk management decisions? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 4. Does the ESRM governing body execute a structured framework/process to regularly review risk assessments? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 5. Does the ESRM governing body execute a structured framework/process for regularly evaluate the effectiveness of risk mitigation strategies? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |

LEVEL 4

ESRM GOVERNANCE LEVEL 4 – MANAGED

An ESRM governing body has developed a formal agenda, discussed it at recurring meetings, and reported it to top management.

Questions

- | | | |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Does the ESRM governing body routinely work with all security leaders to prepare and present relevant status reports to the organization's management? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Is there documented evidence that risk across all security functions is regularly reviewed and managed (in accordance with principles of ESRM)? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |

LEVEL 5

ESRM GOVERNANCE LEVEL 5 – OPTIMIZED

Periodically, reports are compiled concerning ESRM and ESRM governance by the ESRM governing body, with input from relevant subcommittees as required, and delivered to top management.

Questions

- | | | |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | 1. Is the ESRM governing body continuously ensuring that risk across all security functions is dynamically identified, assessed, and effectively managed (in accordance with principles of ESRM)? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 2. Is there evidence that the organization's approach is effective regardless of the asset at risk or the threat vector? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | <input type="checkbox"/> | 3. Is there evidence that the organization's approach is effective regardless of the asset at risk or the threat vector? |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |
| YES | NO | |
| <input type="checkbox"/> | <input type="checkbox"/> | |

Maturity Model

Culture

Level 1	Level 2	Level 3	Level 4	Level 5
<p>Security leaders representing all security functions have partnered with asset owners and proposed policies and procedures to align ESRM with organizational strategies.</p>	<p>The tenets of ESRM have been socialized with security professionals across all security functions in the organization through training/ education.</p>	<p>Security leaders representing all security functions have reached a partnership agreement with asset owners to manage security risks in the ESRM model. All security policies and procedures relevant to asset owners are documented and aligned with ESRM appropriately and updated on a routine basis.</p>	<p>Security professionals are unified across all security functions and actively manage security risks with asset owners and stakeholders according to established & documented ESRM processes enterprise-wide.</p>	<p>ESRM has been fully adopted as the organization integrated approach to security risk management. Security professionals, unified across the enterprise, routinely work together to manage/ control security risk and drive continuous improvement.</p>

Context

Level 1	Level 2	Level 3	Level 4	Level 5
<p>Security leaders representing all security functions have a clear understanding of ESRM within the context of the organization's values, business processes, regulations, stakeholder responsibilities and operating environment.</p>	<p>Security leaders representing all security functions can articulate how ESRM can support all business functions through the socialization of ESRM and appropriate documentation outlining a strategy for implementation.</p>	<p>Security professionals representing all security functions can demonstrate how their security function can help asset owners and stakeholders manage security risk across the organization in line with ESRM processes.</p>	<p>Security professionals are unified across all security functions and working with their teams, asset owners, and stakeholders to monitor and review any changes that might impact the enterprise's profile.</p>	<p>The organization conducts ESRM proactively. Security leaders are unified across all security functions and work with asset owners who take ownership of their own security risk. Security professionals & asset owners work together to continuously improve ESRM through open, real-time communication with the top management, asset owners, and other stakeholders.</p>

Stakeholders

Level 1	Level 2	Level 3	Level 4	Level 5
<p>Security leaders representing all security functions have identified asset owners and key stakeholders across the enterprise and have begun socializing ESRM philosophy.</p>	<p>Security leaders representing all security functions have identified, understood, and documented ESRM stakeholder relationships and defined and agreed on roles and responsibilities concerning security risk management support to asset owners.</p>	<p>Security professionals representing all security functions and asset owners have documented the identification, prioritization and mitigation of security risks.</p>	<p>Security leaders are unified across all security functions enterprise-wide and have implemented documented processes to ensure stakeholder engagement continuity. Partnerships continue to progress as personnel change among asset owners and other stakeholders.</p>	<p>Security leaders are unified across all security functions enterprise-wide and working directly with top management to ensure an integrated and proactive approach in preparing for anticipated changes in asset owners and key stakeholders and are planning for continuity of operations in the event of unanticipated changes.</p>

Risk Management

Level 1	Level 2	Level 3	Level 4	Level 5
<p>Security leaders representing all security functions have engaged with asset owners to document existing security risks across the enterprise and align ESRM with the organization's overarching risk management approach.</p>	<p>Security leaders representing all security functions have agreed with asset owners and codified/ documented security risk management methodologies aligned to the organization's overarching risk management approach. These methodologies outline the prioritization of the protection of assets, identifying and evaluating security risk, and determining the appropriate risk mitigation strategy.</p>	<p>Asset owners have taken ownership of and understand their security risk.</p>	<p>Security leaders are unified across all security functions and actively monitor the security risk management strategies and effectiveness. Security leaders engage with top management, asset owners, and other stakeholders to measure and improve effectiveness across the enterprise.</p>	<p>Security leaders are unified across all security functions and work routinely with asset owners and stakeholders to mitigate security risks across the enterprise proactively. The ESRM methodology is the standard approach to security risk management, aligned with the organization's overarching risk management process enabling real-time decision making across the enterprise.</p>

ESRM Governance

Level 1	Level 2	Level 3	Level 4	Level 5
<p>Security leaders representing all security functions have agreed on an ESRM Governance requirement with top management, aligned to broader organizational governance processes.</p>	<p>A documented security governance charter has been established, an ESRM governing body / Security council has been formed, aligned to the organization's structure, and all members understand their roles.</p>	<p>An ESRM governing body is actively overseeing ESRM and tracking positive outcomes of the ESRM approach.</p>	<p>An ESRM governing body has developed a formal agenda, discussed it at recurring meetings, and reported it to top management.</p>	<p>Periodically, reports are compiled concerning ESRM and ESRM governance by the ESRM governing body, with input from relevant subcommittees as required, and delivered to top management.</p>



Recommended Reading

It is strongly recommended that users educate themselves on the basic tenets of ESRM philosophy before using this maturity model.

Below is a list of suggested reading material available which will support a working understanding of ESRM philosophy and the benefits to both the enterprise and the security professional:



[Enterprise Security Risk Management Guideline, 2019](#)

E-BOOK



[A brief guide to ESRM implementation 2019 – Dave Feeney](#)



[Time to pivot – Applying ESRM after Covid 19 2021 – Claire Meyer](#)




[Five Insights into ESRM 2017 – Rachelle Loyear & Brian Allen](#)



[How to implement ESRM 2018 - Art Fiero](#)

In addition, the following publications may also be of interest:

- 
- The Managers Guide to Enterprise Security Risk Management, Essentials of Risk-Based Security 2018 - Rachelle Loyear & Brian Allen
 - Enterprise Security Risk Management, Concepts and Applications 2017 - Rachelle Loyear & Brian Allen
 - Security Risk Management Body of Knowledge 2011 - Julian Talbot & Miles Jakeman