RESILIENT SAGE

ESRM IMPLEMENTATION PROGRESSION

Eighteen tasks. *One clear progression.*

Resilient Sage's synthesis of how to implement the ASIS ESRM Guideline and Maturity Model.

About this progression

The 18 tasks in this progression are the core tasks of implementing Enterprise Security Risk Management (ESRM). Considered together, they are the process to implement ESRM.

The tasks do not need to be done precisely in this order. The progression is a generalized flow, based on a logical implementation sequence most organizations may follow. Some tasks are simple; others are intensive.

Four tasks, marked with the circular arrow, are the core four the ASIS ESRM Guideline (2019) provides. The ASIS ESRM Maturity Model (2022) was benchmarked in developing the progression. Not every consideration from the Guideline, or every maturity element, is explicit here; each is addressed by completing these tasks.

Initial implementation, then ongoing ESRM

INITIAL IMPLEMENTATION

All 18 tasks, in order

Work through every task, 01 to 18. All 18 carry equal weight in building the program.

The four groups, Steps 01–05, 06–09, 10–14 and 15–18, match the four cards on the ESRM graphic, read clockwise from "Start here."

ONGOING ESRM

The core four, repeated

05 ↻ 09 ↻ 14 ↻ 18 ↻

Task 18 re-executes tasks 05, 09 and 14 on a set cadence, so protection keeps pace with changes to objectives, assets, the risk environment and compliance requirements.

SOURCES Resilient Sage ESRM Implementation Progression · ASIS ESRM Guideline (2019) · ASIS ESRM Maturity Model (2022)

STEPS 01–05

Tasks 01 to 05

The top-left card on the ESRM graphic, group 1 of 4.

01–05 | 06–09 | 15–18 | 10–14

01 **Engage initial ESRM stakeholders; establish participation and priorities**

Brings preliminary leaders and strategy-setters into the effort from the start so ESRM is built as a multidisciplinary partnership. ESRM is a team sport.

02 **Understand the organization's context**

Establishes how the organization's purpose, objectives, values, culture, operating environment, existing security, and risk management capabilities shape what must be protected.

03 **Align top management on ESRM**

Secures board and executive support for ESRM's objectives and approach. ESRM directly ties into organizational objectives, strategy, etc.

04 **Adopt ESRM Board Statement**

Documents top management's commitment to ESRM, giving the program its mandate, oversight, and defining periodic reporting requirements.

05 **Identify and prioritize assets, and their owners** ↻

Determines what the organization relies on to achieve its objectives, who is accountable for each asset, and which assets warrant priority protection.

↻ Core four from the ASIS ESRM Guideline, repeated for ongoing ESRM

STEPS 06–09

Tasks 06 to 09

The top-right card on the ESRM graphic, group 2 of 4.

01–05 | 06–09 | 15–18 | 10–14

06 Create ESRM Governance Charter

Establishes the governing body and defined roles that direct day-to-day ESRM, set its goals, and make top-level protective decisions.

07 Develop ESRM Policy and Program Document

Codifies the desired result and requirements of ESRM, and how ESRM is implemented and managed.

08 Receive top management approval for the charter, policy, and program document

Gives the charter, policy, and program document formal organizational authority in accordance with the board statement.

09 Perform Security Risk Assessment ↻

Identifies, analyzes, and evaluates security risks to objectives against the organization's risk appetite and tolerance to produce a prioritized risk picture for decision-makers.

↻ Core four from the ASIS ESRM Guideline, repeated for ongoing ESRM

STEPS 10–14

Tasks 10 to 14

The bottom-right card on the ESRM graphic, group 3 of 4.

01–05 | 06–09 | 15–18 | 10–14

10 **Prioritize risk management measures**

Using the Security Risk Assessment (SRA), each treatment and risk acceptance decision is placed with the asset owner who owns the risk and records it. Organizes initial sources for top management reporting.

11 **Develop Strategic Security Plan**

Turns the findings of the SRA into a resourced, sequenced plan in which every investment traces a specific risk against a specific objective. Informs operational and capital spending for security risk management efforts.

12 **Identify and implement training requirements**

Equips asset owners and those responsible for ESRM with the knowledge and skills required.

13 **Establish Asset Protection Radar**

Creates a single source for the ESRM leader to oversee the status of security risk management efforts against organizational objectives.

14 **Implement security risk management measures** ↻

Puts required security risk management measures into operation and keeps them effective through scheduled and event-driven re-assessment, lessons learned, council oversight, and reporting to top management.

↻ Core four from the ASIS ESRM Guideline, repeated for ongoing ESRM

STEPS 15–18

Tasks 15 to 18

The bottom-left card on the ESRM graphic, group 4 of 4.

01–05 | 06–09 | 15–18 | 10–14

15 **Receive independent third-party ESRM audit**

Provides objective verification that the program operates as documented and achieves its intended outcomes.

16 **Perform scheduled review of ESRM system**

Re-validates policies, procedures, and practices each year and sets the council's strategic agenda so the program stays aligned with current objectives, risks, and compliance issues.

17 **Complete ESRM maturity assessment**

Measures the program's current maturity and identifies what is required to reach the next level.

18 **Repeat core ESRM cycle; improve** ↻

Continual monitoring for improvement. Re-executes steps five, nine, and fourteen on a set cadence so protection keeps pace with changes to the organization's objectives, assets, risk environment, and compliance requirements.

↻ Core four from the ASIS ESRM Guideline, repeated for ongoing ESRM