Engage. Explore. Empower.

Connecting Visionaries in Radiation Safety, Science and Industry

MIRION Connect 24

Annual Users' Conference

July 29 - August 2 | Omni Dallas Hotel, Dallas, TX

MIRION TECHNOLOGIES

Building a System Roadmap for Security Computer Systems

Key objectives of the session

- ❑ Understanding the components of a system roadmap
  - ❑ Identifying technology obsolescence
  - ❑ Prioritizing upgrades based on risk

Introduction

1. Maintaining a system roadmap is not just about keeping systems running smoothly; it is a tool that enhances security, efficiency, compliance, and overall organizational resilience.
2. By proactively managing technology assets, organizations can avoid disruptions, reduce costs, and stay ahead in an ever-evolving technological landscape.
3. A system roadmap allows you to make decisions and take actions that always build cohesively to achieve your system goals.

What is a System Roadmap?

A system roadmap is a strategic plan that outlines the current state, future goals, and the steps necessary to achieve those goals for a specific system or set of systems.

It serves as a high-level guide for managing and evolving the system over time, ensuring alignment with organizational objectives and adapting to technological advancements.

Benefits: Future-proofing, maintaining security, and ensuring compliance

Engage. Explore. Empower.

System Roadmap Key Elements

Future Vision: Defines the desired future state of the system, including improvements and new capabilities.

Current State Assessment: Evaluates the existing components, performance, and capabilities of the system.

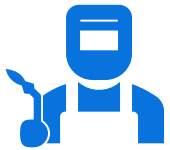
Risk Assessment: Identifies potential risks, such as technology obsolescence, security vulnerabilities, and maintenance challenges.

Action Plan: Details the steps, timelines, and resources needed to transition from the current state to the future vision.

Stakeholder Alignment: Ensures that the roadmap aligns with the needs and expectations of key stakeholders, including Compliance, IT teams, and Security Operations

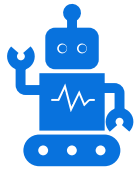
Future Vision

Defines the desired future state of the system, including improvements and new capabilities.



Improvements:

Enhanced performance, security, and reliability.



New Capabilities:

Integration of advanced technologies, scalability, and compliance with future standards.

Innovation:

Adoption of emerging technologies to stay aligned with the industry.

User Experience:

Better user interfaces and more intuitive controls.

Current State Assessment

Evaluates the existing components, performance, and capabilities of the system.

System Infrastructure
- *Networking*
- *Computing*

Subsystems
- *Biometrics*
- *Video Surveillance*
- *Access Control*
- *Intrusion Detection*

Core Software
- *Operating Systems*
- *Database Engine*
- *Hypervisor*
- *Graphics*
- *Reports*

Cyber Security
- *SIEM*
- *Network Intrusion*
- *Boundary Control*
- *Network Monitoring*
- *Endpoint Protection*
- *Backup & Recovery*

Features & Functionality
- *Intrusion Detection*
- *Access Control*
- *Integrated Video Management*
- *Command & Control*
- *Failover, Backup*
- *Emergency Accountability*
- *Badging, Visitor Processing*

MIRION Connect 24
Annual Users' Conference

Engage. Explore. Empower.

Identify Technology Obsolescence

Technology obsolescence refers to the process by which a technology, software, or hardware becomes outdated or no longer useful. This occurs when it is superseded by newer technologies, loses vendor support, or fails to meet current performance or security standards.

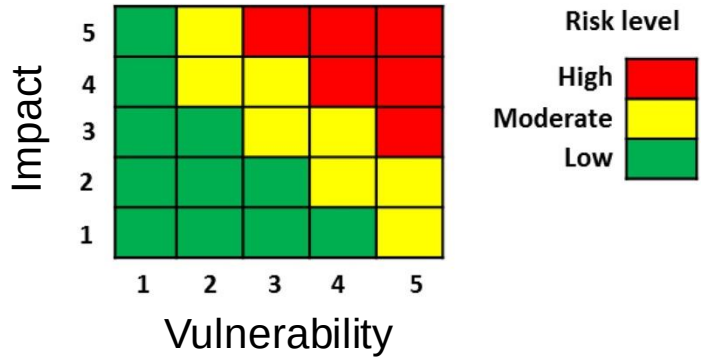
Part of your current state assessment

Key Indicators:

1) **End of Sale (EOSale): A** product is no longer available for purchase from the vendor. After this point, you can no longer replace it.
2) **End of Support (EOS):** No more patches or updates are released, leading to potential security vulnerabilities.
3) **End of Life (EOL):** The point at which a product is no longer supported or updated by the vendor.
4) **Compatibility Issues:** Newer technologies or software are not compatible with the old system, limiting functionality.
5) **Decreased Performance:** The technology no longer meets the performance requirements of current applications or workloads.
6) **Market Trends:** The industry moves towards newer standards and practices, leaving the older technology behind.

Risk Assessment

Identify Risks Related to Security Operations, Compliance, and System Downtime



Risk = Vulnerability (Exposure) × Impact (Criticality)

Where:

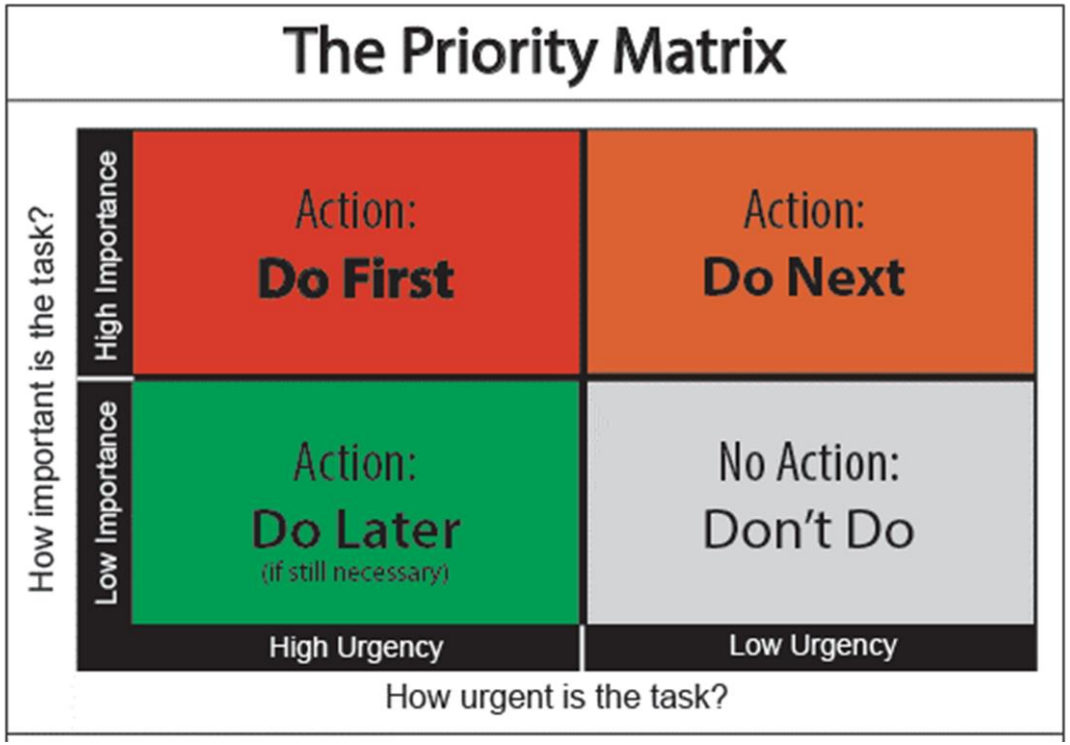
- **Vulnerability (Exposure):** The susceptibility of the system to threats.
- **Impact (Criticality):** The potential consequences or damage that could result from the threat exploiting the vulnerability.

1) **Security Operations:**
   - Unauthorized Access
   - Data Breach
   - Insider Threats
2) **Compliance:**
   - Regulatory Compliance
   - Policy Adherence
   - Audit Findings
3) **System Downtime:**
   - Hardware Failures
   - Software Failures
   - Network Disruptions

Action Plan

Use the risk assessment matrix to prioritize components/features based on their risk scores

1. **Strategy for prioritizing upgrades**
   - *High-Risk Components: Address critical vulnerabilities and end-of-life components immediately.*
   - *Medium-Risk Components: Plan upgrades for components that pose moderate risk.*
   - *Low-Risk Components: Monitor and plan for future updates as needed.*
2. **Balance risk, cost, and operational impact**
3. **Build a plan that strives to meet the defined final state.**
4. **Incorporate New Features and Innovations**
   - Stay aligned with industry by adopting emerging technologies and innovative solutions.



Roadmap Development Summary

Future Vision

Set Goals and Objectives: Define clear, measurable goals for system enhancements and new capabilities.
Identify Specific Improvements: Outline specific improvements in performance, security, and reliability.
Adopt Emerging Technologies: Identify emerging technologies to adopt.

Current State Assessment

Conduct a Comprehensive Audit: Assess all current hardware, software, integrations, and cybersecurity tools.
Document and Analyze Components: Record versions, configurations, and dependencies of each component.
Determine Lifecycle Stages: Identify the lifecycle stage of each component (e.g., in use, nearing end of life, obsolete).

Risk Assessment

Identify Security Risks: Assess risks associated with outdated or unsupported components.
Evaluate Patching and Maintenance: Evaluate the frequency and availability of patches for each component.
Prioritize Risks: Use a risk assessment matrix to prioritize components based on their risk scores (Vulnerability × Impact)

Action Plan

Focus on High-Risk Components: Prioritize and plan for the upgrade or replacement of high-risk components.
Define Key Actions and Milestones: Develop a detailed timeline with clear milestones for each step.
Define Resources: Determine the necessary resources for each action step.

Stakeholder Alignment

Involve Security Operations: Align with security operations to maintain and enhance the security posture of the system.
Collaborate with Vendors: Work with Vendors to ensure technical feasibility and integration.
Engage Compliance: Ensure the roadmap meets regulatory and compliance requirements.

Thank you