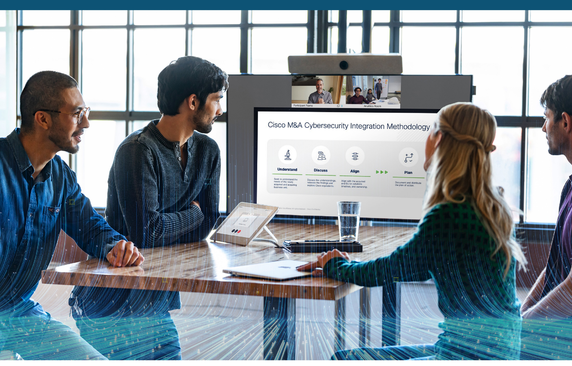
How Cisco Protects its Enterprise throughout the M&A Process



When Cisco acquires a company, it's critical that we consider the security posture of the entity's solutions and infrastructure to meet rigorous cybersecurity standards. Understanding and mitigating risk is essential to establishing trust between Cisco and the acquisition as we move through the Mergers and Acquisitions (M&A) process.

Whether you're a company being acquired or a customer seeking solutions that come from a Cisco acquisition, we are committed to demonstrating transparency throughout this journey.

Learn how Cisco holistically approaches M&A cybersecurity from the initial discovery and diligence phase and through the integration of a new entity.

Our Mission

To investigate and assess risk to Cisco and help define strategic plans for acquisition integration and adoption.

- **Understand**
  We seek to understand an acquisition's mission and environment, first.
- **Discuss**
  We discuss an acquisition's environment and educate them on the Cisco equivalent and standards.
- **Align**
  We seek alignment with acquisitions to ensure their success.

We want to help aquired companies be successful!

Methodology

Understand
Seek to understand the needs of the newly acquired and acquiring business unit.

Discuss
Discuss the needs, reiterate the findings and explore Cisco equivalents.

Align
Align with the acquisition and BU on solutions timelines, and ownership.

Plan
Document and integrate the security plan of action.

Acquisition Anchors

Value Drivers + **Non-Integrated Risks** + **Operating Norms** = **Roadmap Plan**

What are the strategic goals of the acquisition?

What are our immediate security risks?

What are the Cisco security standards?

What is the integration roadmap?

Aquisition Integration

Value Drivers
We have a responsibility to achieve the value that has been defined for each acquisition.

+

Operating Norms
We will drive to Cisco cybersecurity standards in each acquisition.

Rapid Risk Assessment for Offers

Rapid Risk Assessment for Enterprise

Non-Integrated Risks

Goal
To assess and mitigate inherited risk to Cisco in the early stages of aquisition.

CSDL Engagement

Enterprise Standards & Processes

Data Privacy Standards & Processes

ASIG Security Risk Assessment

Operating Norms

Goal
To align the acquired with Cisco standards where applicable.

Operating Norms

- Threat & Vulnerability Management
- Incident & Event Logging
- Identity & Access Management
- Infrastructure & Virtualization Security
- Governance & Risk Management
- Data Security & Privacy
- Crypgography & Enterprise Key Management
- Application Interface Security

Roadmap Plan

Day 1 + 30	Information gathering, cross-functional briefings, schedule risk readiness assessment
Day 1 + 60	Security assessments, mitigation planning
Day 1 + 90	Mitigation plans developed, execution of mitigation work
Day 120+/ Day 180+/ Run the Business	Final deliverables completion, CSDL readiness plan, and transition services to run the business