SILICON LABS

CONNECTED INTELLIGENCE

Security Overview

Information Security Management System (ISMS)
Enterprise and Product Security

Overview Topics

Information Security Management System (ISMS)

Secure SDLC Maturity Framework (SSMF)

Incident Response

- Vulnerability Disclosure Program (VDP)
- Product Security Incident Response Process (PSIRP)

Secure Suppliers

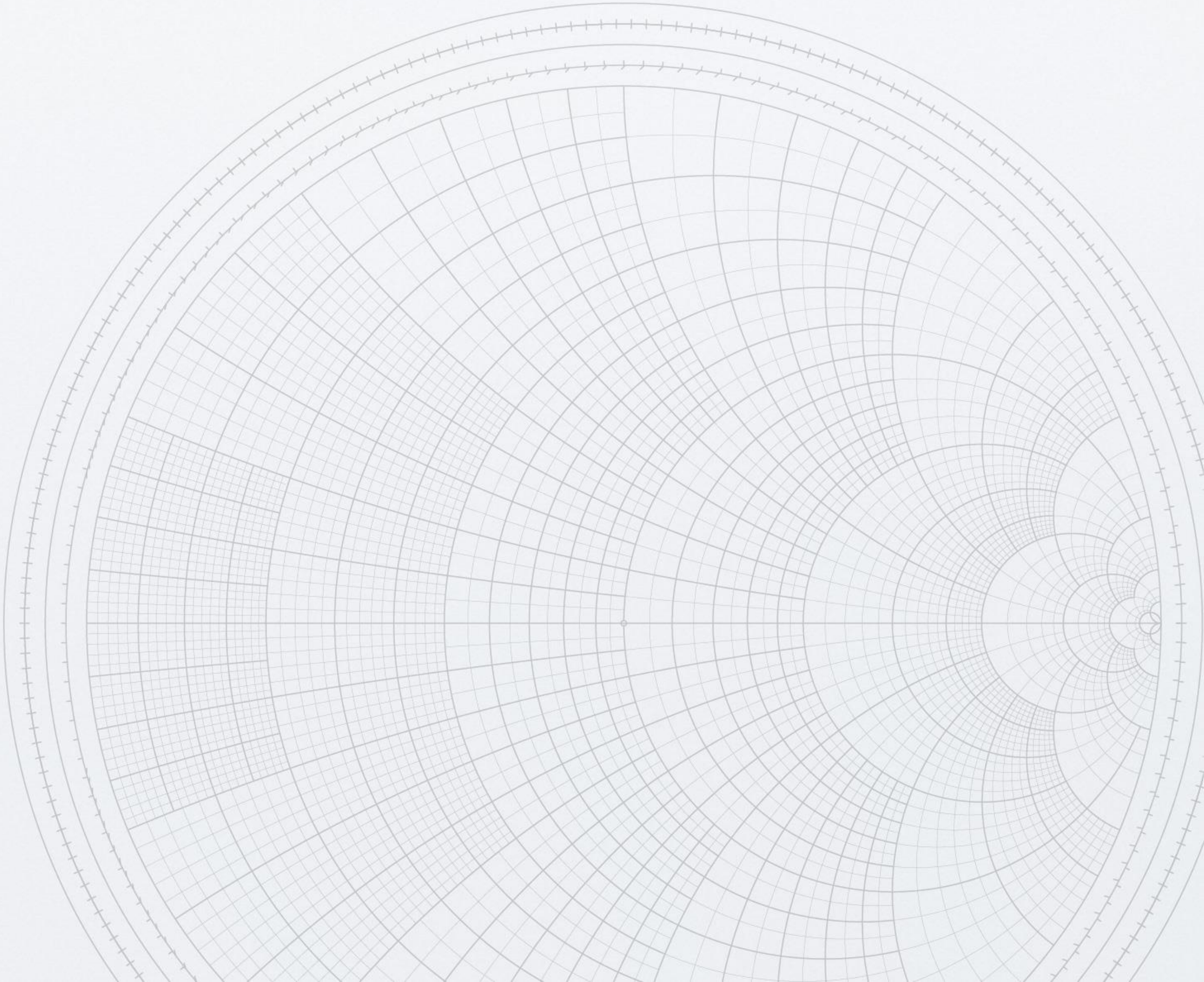
Commitment to Security

Security @ Silicon Labs

At Silicon Labs, protecting our products, data, and customers is central to how we do business. Security is not an afterthought – it's built into every layer of our operations and product lifecycle. Our commitment to security is validated by our ISO 27001:2022 certification. This certification confirms that our security practices comply with one of the world's most rigorous international standards for information security management.

SILICON LABS
CONNECTED INTELLIGENCE

Information Security Management System (ISMS)



SILICON LABS

CONNECTED INTELLIGENCE

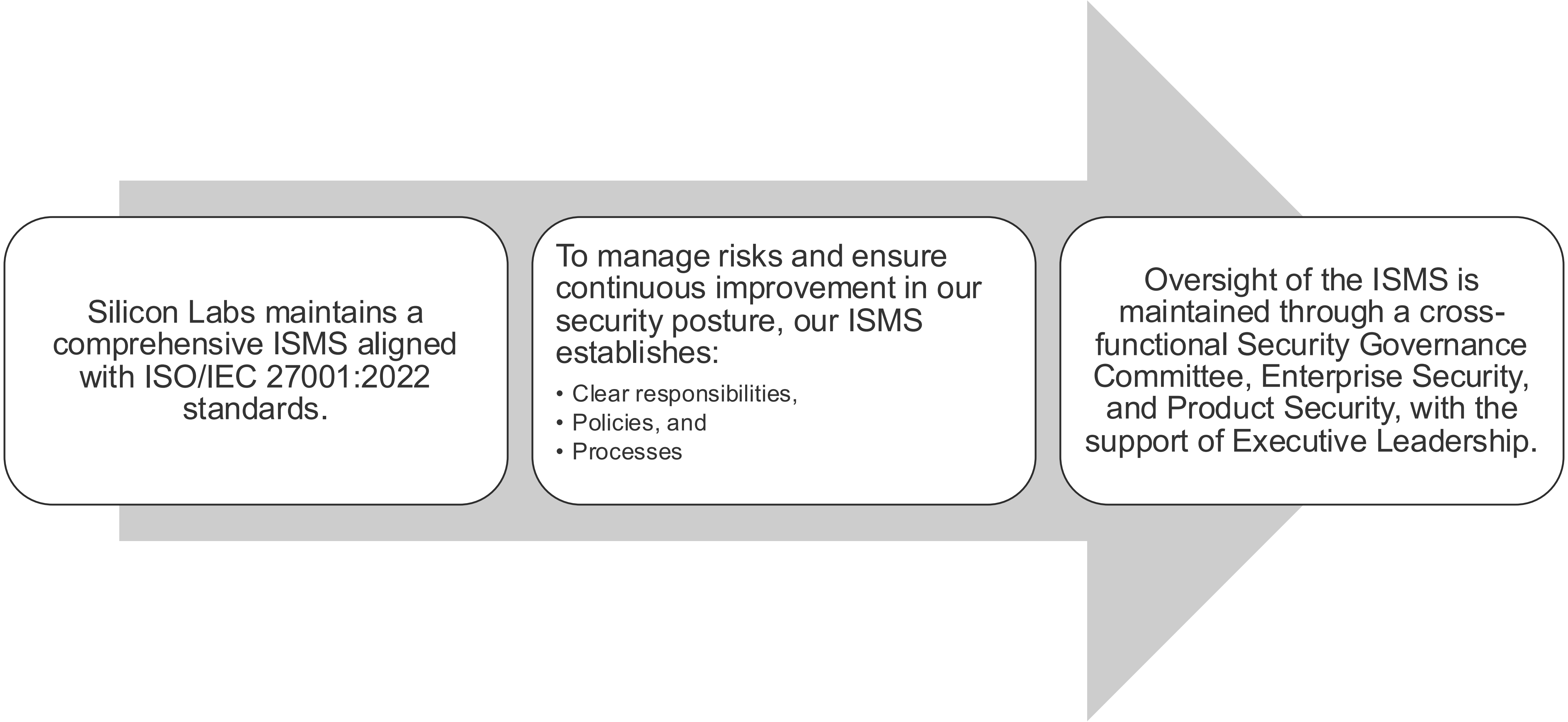
Information Security Management System (ISMS)

Our ISMS governs how we safeguard information assets and ensure the resilience of our systems, services, and intellectual property.

Further, the ISMS:

- ❑ Provides the framework for safeguarding information assets, managing risk, and driving continual improvement
- ❑ Aligns with ISO 27001:2022, ensuring consistent application of security policies, procedures, and controls across all business units, products, and regions
- ❑ Built around four core principles:
  - Confidentiality – Ensuring information is accessible only to authorized parties.
  - Integrity – Protecting information accuracy and reliability.
  - Availability – Maintaining access to systems and data when needed.
  - Continuous Improvement – Regularly assessing and strengthening our security posture.

Security Governance



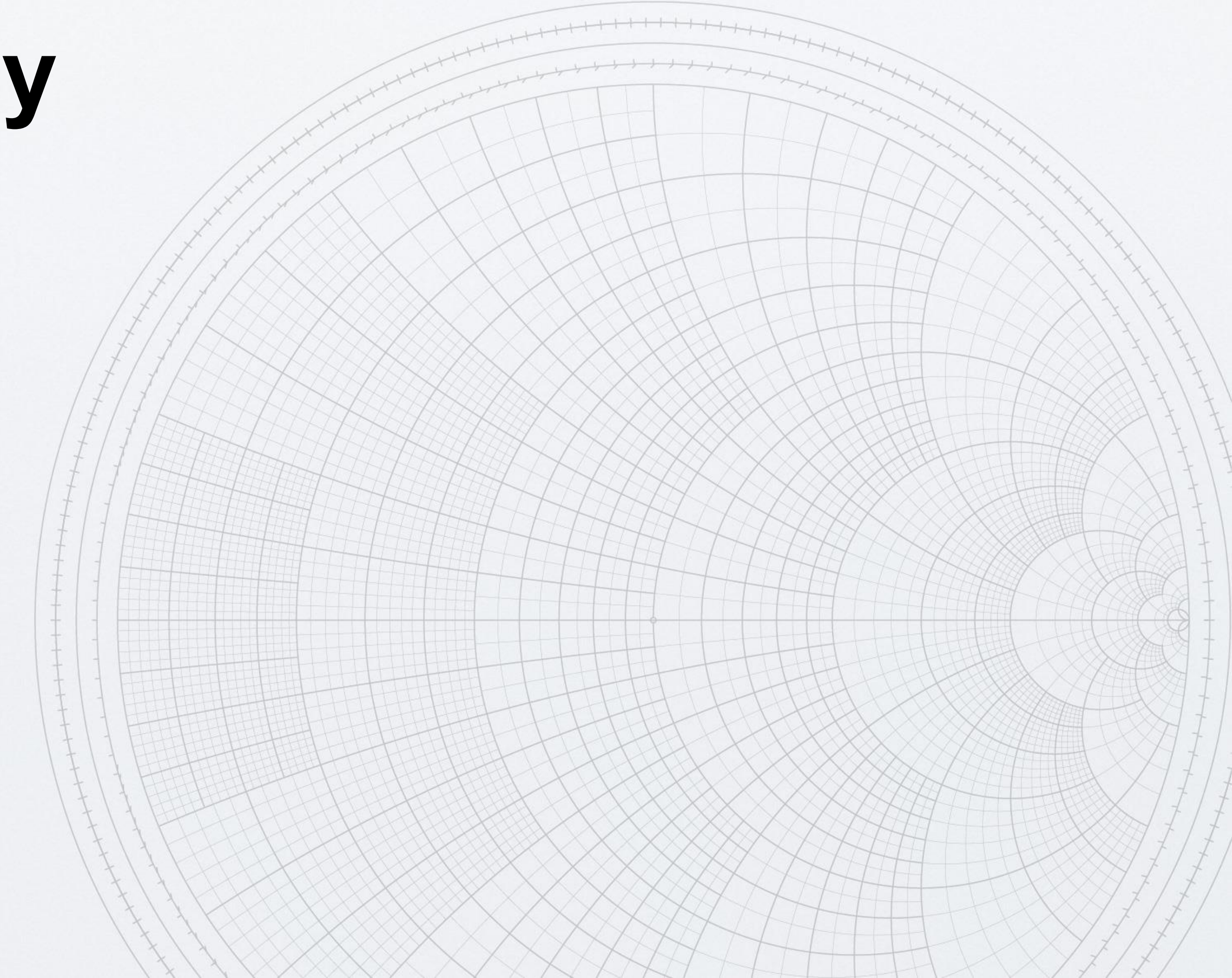
Silicon Labs maintains a comprehensive ISMS aligned with ISO/IEC 27001:2022 standards.

To manage risks and ensure continuous improvement in our security posture, our ISMS establishes:

- Clear responsibilities,
- Policies, and
- Processes

Oversight of the ISMS is maintained through a cross-functional Security Governance Committee, Enterprise Security, and Product Security, with the support of Executive Leadership.

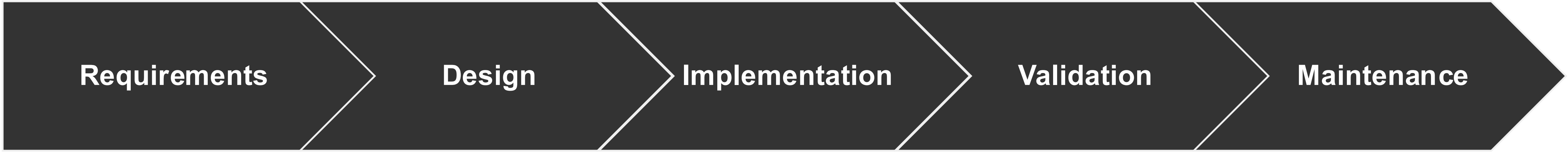
Secure SDLC Maturity Framework (SSMF)



SILICON LABS

CONNECTED INTELLIGENCE

Secure Development Lifecycle

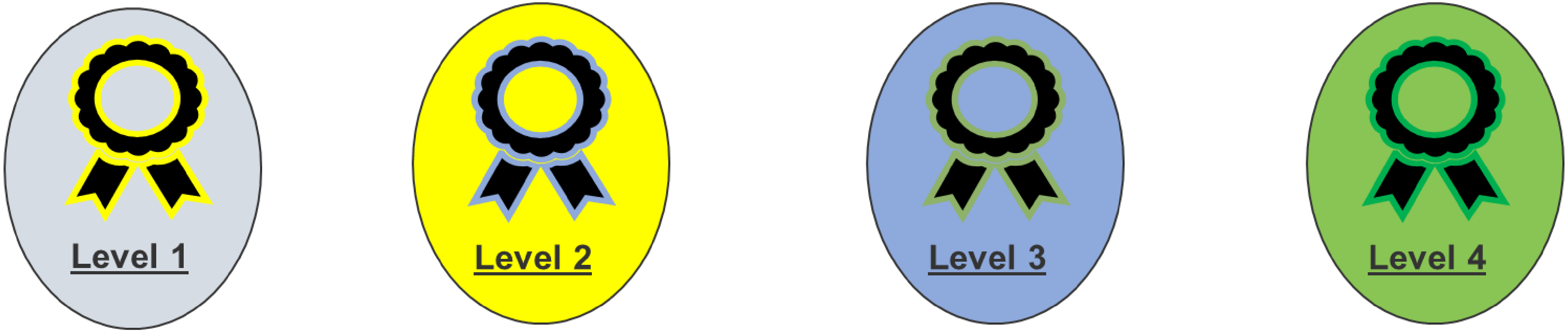


Requirements → Design → Implementation → Validation → Maintenance

- **Secure Design**
  - Hardware Design with security in mind by creating innovative solutions such as Secure Vault™
  - Software Developers follow industry-recognized secure-coding standards and internal guidelines that emphasize code safety, input validation, and prevention of common vulnerabilities.
- **Vulnerability Management**
  - Potential vulnerabilities are tracked through a centralized system that ensures prompt triage, remediation, and documentation. Both internal testing and external feedback – including coordinated disclosure from the research community – feed into a continuous improvement cycle to strengthen product resilience.
- **Continuous Testing**
  - Security testing is performed throughout the product lifecycle, not just before release. This includes threat modeling, fuzz testing, regression testing, and periodic penetration assessments to validate that new features or updates do not introduce risk. Lessons learned from testing inform future design and development practices.

Secure SDLC Maturity Framework (SSMF)

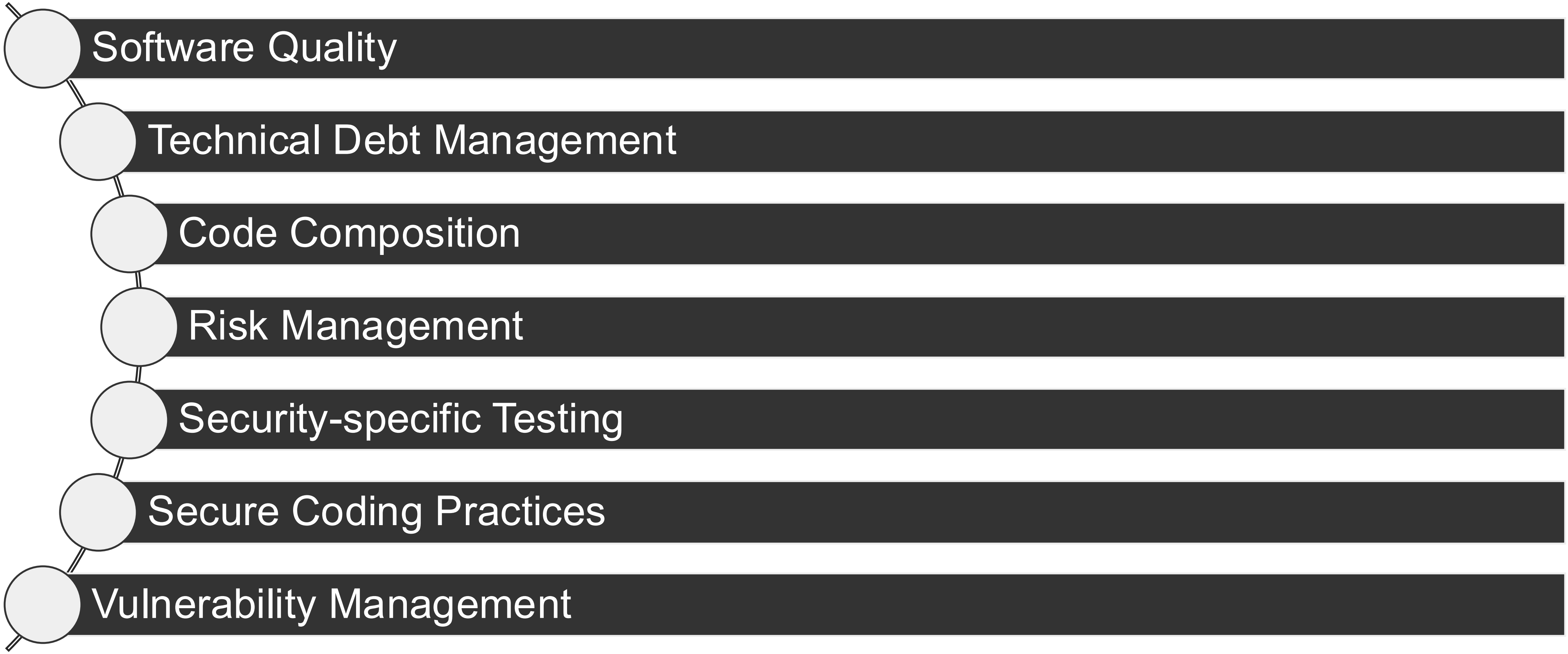
- Silicon Labs uses an in-house 4-level maturity-based framework to drive development practices
- Teams are required to pursue a targeted level based on risk tied to a proprietary criteria matrix
- Activities involved are mapped to various industry standards
- The program is reviewed annually for needed updates



Secure-SDLC Maturity Framework (SSMF)

Topics Covered under SSMF

The maturity framework contains aspects from multiple security and software development standards. This includes processes and practices related, and not limited to:

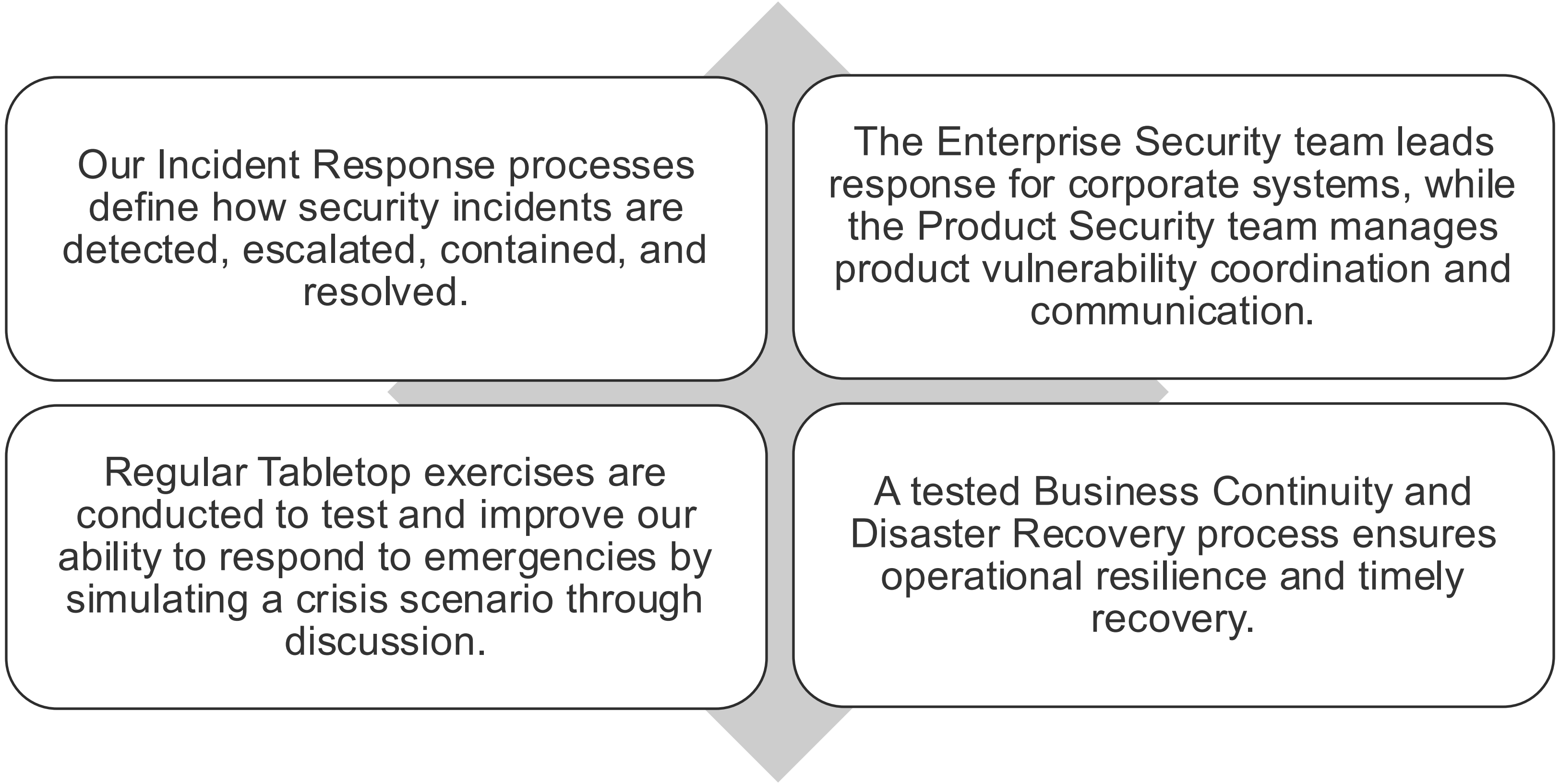


- Software Quality
- Technical Debt Management
- Code Composition
- Risk Management
- Security-specific Testing
- Secure Coding Practices
- Vulnerability Management

Incident Response

SILICON LABS
CONNECTED INTELLIGENCE

Incident Response and Business Continuity



Our Incident Response processes define how security incidents are detected, escalated, contained, and resolved.

The Enterprise Security team leads response for corporate systems, while the Product Security team manages product vulnerability coordination and communication.

Regular Tabletop exercises are conducted to test and improve our ability to respond to emergencies by simulating a crisis scenario through discussion.

A tested Business Continuity and Disaster Recovery process ensures operational resilience and timely recovery.

Visit our Security Vulnerability FAQs to get guidance on how to report potential security issues, what to expect during the disclosure process, and how we handle vulnerability disclosures.

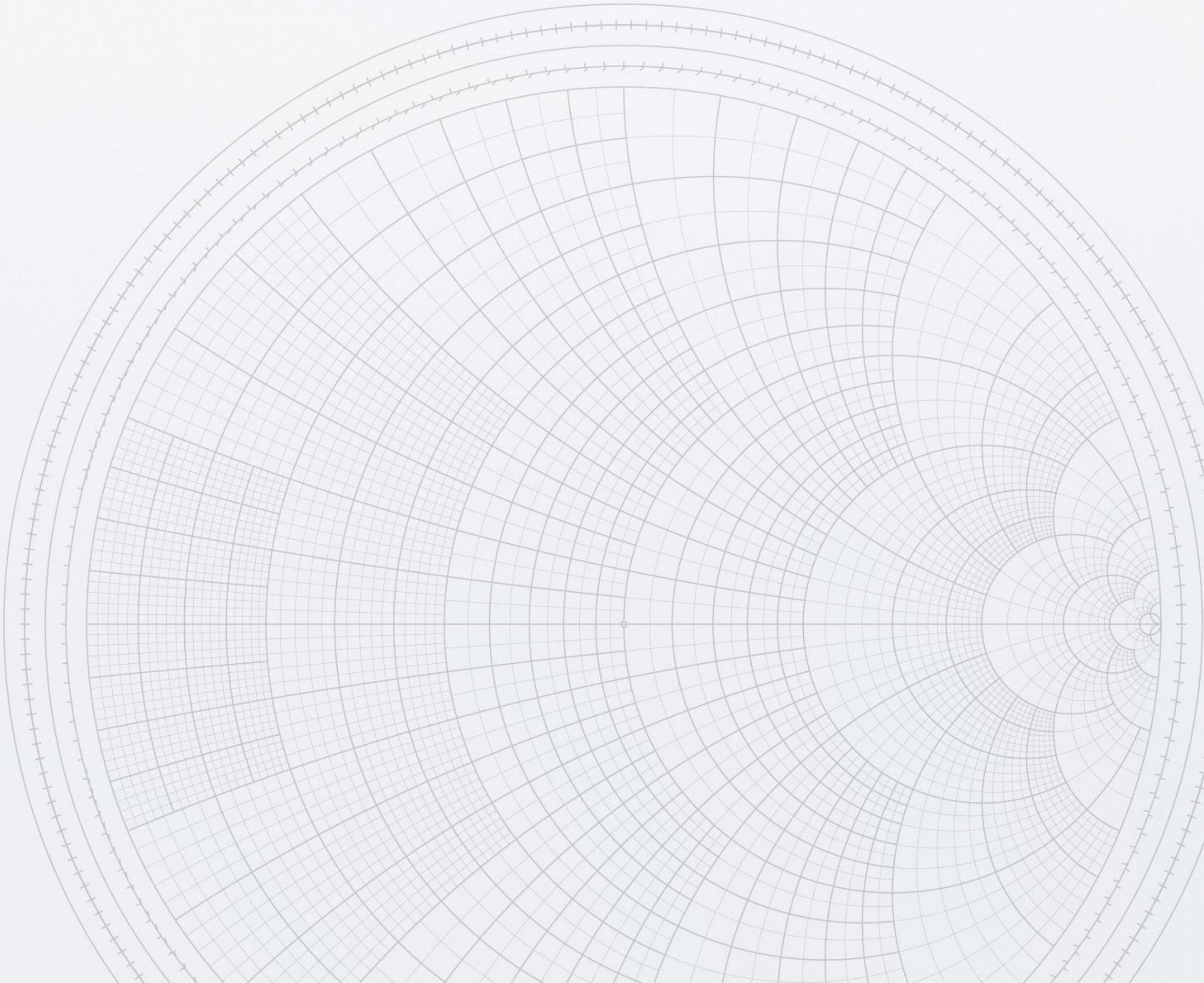
Vulnerability Disclosure

We take inputs on security vulnerabilities from external sources

- Security vulnerabilities can be reported via https://www.silabs.com/security/report-security-vulnerability
- We assess updates from 3rd party partners, and/or national, or regulatory bodies (e.g., MITRE, VINCE, etc.)

Any confirmed vulnerability in our software and products is assigned a CVE by Silicon Labs, as we are a CVE Numbering Authority (CNA)

Secure Suppliers

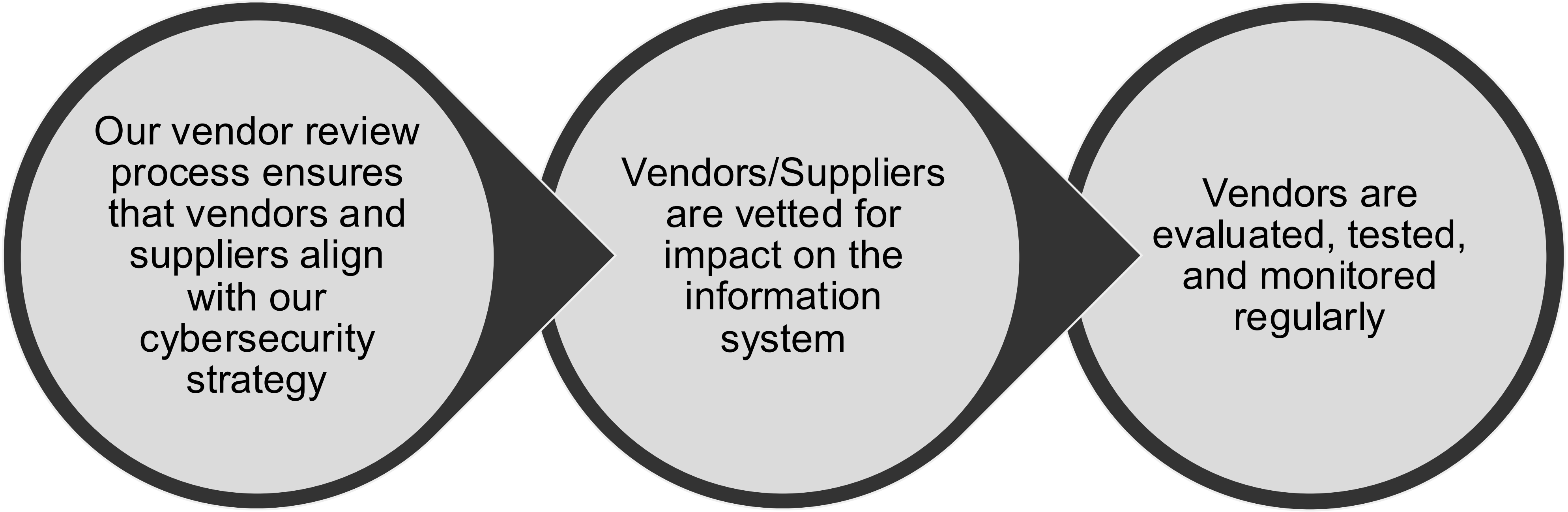


SILICON LABS

CONNECTED INTELLIGENCE

Silicon Labs and Vendor Security

Silicon Labs takes vendors and suppliers very seriously.

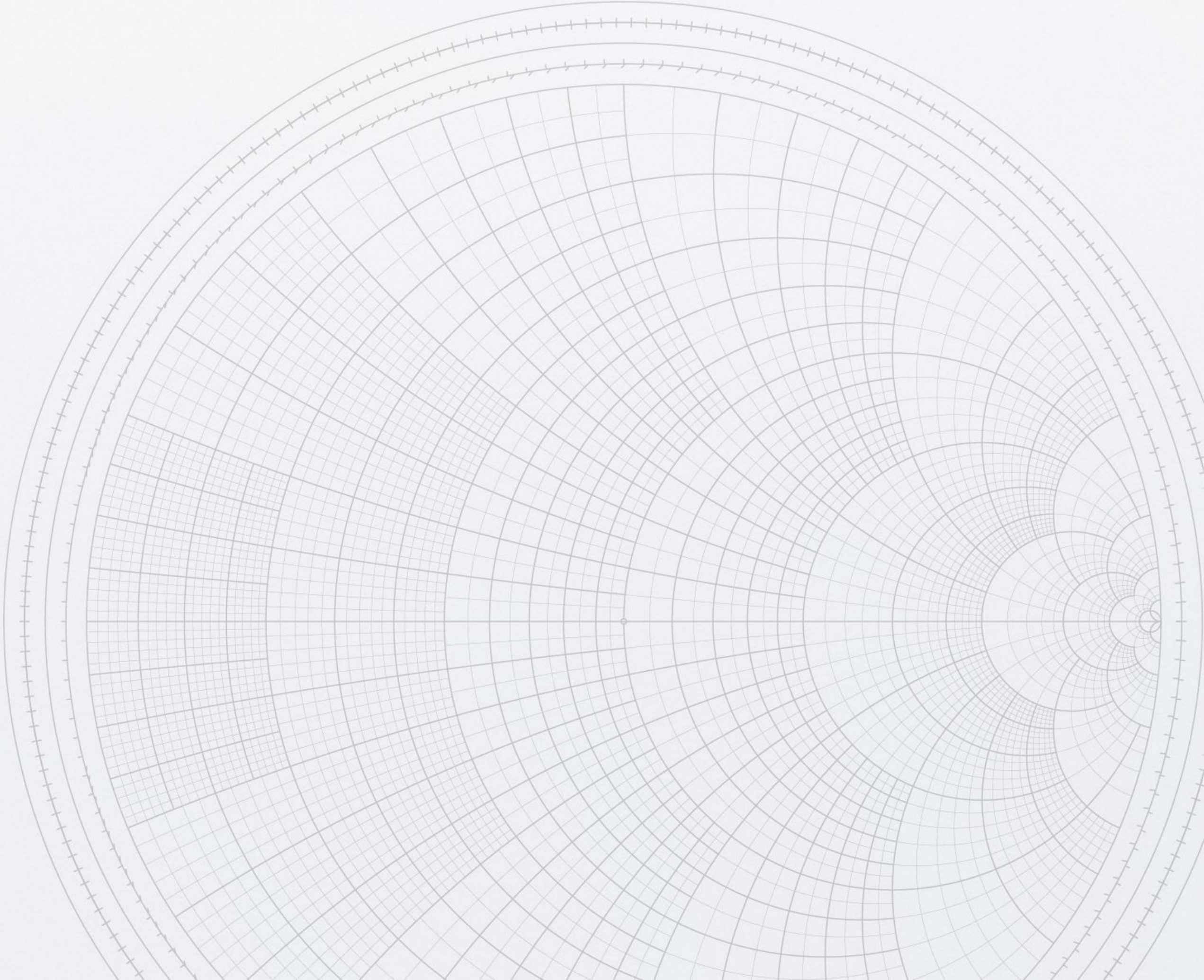


Our vendor review process ensures that vendors and suppliers align with our cybersecurity strategy

Vendors/Suppliers are vetted for impact on the information system

Vendors are evaluated, tested, and monitored regularly

Commitment to Security



SILICON LABS

CONNECTED INTELLIGENCE

Risk Management

Our approach to risk management integrates **identification**, **evaluation**, **mitigation**, and **monitoring** of threats across both enterprise and product domains.

Security risks are reviewed regularly to account for changing technologies and global threat landscapes, and preventive controls are updated to ensure compliance with ISO 27001:2022 requirements.

Preventive and detective controls are continuously updated to maintain the confidentiality, integrity, and availability of our systems and data.

Data Protection and Privacy

Silicon Labs enforces strict controls to protect customer, partner, and employee data in alignment with global data protection laws and frameworks such as the General Data Protection Regulation (GDPR).

Data access follows least-privilege and need-to-know principles, backed by encryption and strong authentication.

Privacy protection is a cornerstone of customer trust and a key element of our ISMS.

Industry Collaboration

We actively participate in standards bodies, security alliances, and research initiatives to advance secure IoT practices.

Collaboration ensures that Silicon Labs products meet the highest benchmarks of trust, reliability, and long-term resilience.

Continuous Improvement

Security at Silicon Labs is a dynamic and continuously improving program with inputs from:

- Customers
- Regulations
- External assessments, and
- Employee awareness programs

The recent ISO 27001:2022 audit outcome reflects a well-managed and continuously improving security culture – one that prioritizes prevention, transparency, and learning.

Security Policy

Silicon Labs is committed to total customer satisfaction by continually improving our Information Security Management System (ISMS) while providing secure, connected devices to improve lives.

SILICON LABS

CONNECTED INTELLIGENCE