Trellix

DATA SHEET

Cybersecurity Framework Development & Review

Build Security with Purpose. Govern with Confidence.

Benefits and Outcome

- Holistic understanding of your cybersecurity maturity
- Reduced risk through structured, measurable controls
- Improved audit-readiness and compliance coverage
- Alignment between IT, security, and business priorities
- Increased board and stakeholder confidence

When Should Companies Consider This Service

- No formal cybersecurity framework exists
- Existing framework is fragmented, outdated, or non-compliant
- Regulatory obligations require structured cybersecurity controls
- Preparing for audits, certifications, or third-party assessments
- Undergoing digital transformation, mergers, or cloud migration
- Seeking to mature from reactive to proactive cybersecurity posture

Framework Development & Review

Overview

Cybersecurity frameworks provide the strategic backbone for securing digital assets, aligning risk with business objectives, and maintaining regulatory compliance.

Trellix Guardians Frameworks Development & Review service helps organizations adopt, tailor, or optimize cybersecurity frameworks that align with international standards (e.g., NIST, ISO/IEC 27001, CIS Controls) and industry-specific regulations. Whether building from the ground up or refining an existing structure, we ensure your security posture is measurable, scalable, and defensible. This services can be customized to fit your needs.

Key Deliverables

We help organizations build or refine cybersecurity frameworks tailored to their business, regulatory, and risk environments. Our service delivers a practical control structure, maturity assessment, and roadmap aligned to global standards like NIST and ISO 27001. The result is a clear, defensible cybersecurity posture that supports strategic and compliance goals. Below is a summary of these key deliverables:

- Current framework gap analysis and benchmarking
- Tailored cybersecurity framework design or refinement
- Policy, control, and standard alignment to selected frameworks
- Mapping controls to compliance requirements (e.g., GDPR, PCI DSS)
- Maturity model integration (e.g., CMMI, NIST CSF tiers)
- Executive summary report and implementation roadmap
- Stakeholder alignment and advisory workshops

Our Methodology

The Guardian approach begins with understanding your business context and assessing existing cybersecurity practices against recognized frameworks. We then identify gaps, design or enhance your framework, and map controls to compliance and risk priorities.

Finally, we deliver a practical roadmap and validate alignment through stakeholder workshops and documentation handover. Below is a summary of our methodology:

1. **Discovery & Scoping**
   - Understand business context, threat landscape, and compliance drivers
   - Identify current frameworks, policies, and security controls

2. **Gap & Maturity Assessment**
   - Conduct a structured assessment against selected framework(s)
   - Leverage industry benchmarks to assess coverage and maturity

3. **Framework Development or Enhancement**
   - Tailor controls, policies, and processes to business needs
   - Align controls to regulations and risk appetite

4. **Control Mapping & Documentation**
   - Produce control mappings and crosswalks (e.g., NIST to ISO 27001 etc)
   - Define implementation of guidance and responsibilities

5. **Validation & Roadmap Delivery**
   - Present findings, implementation roadmap, and quick wins
   - Conduct workshops to validate alignment and handover artifacts

For more information or to schedule a consultation, please contact us at Guardians@Trellix.com