# Information Security Governance Risk & Compliance (GRC) Management
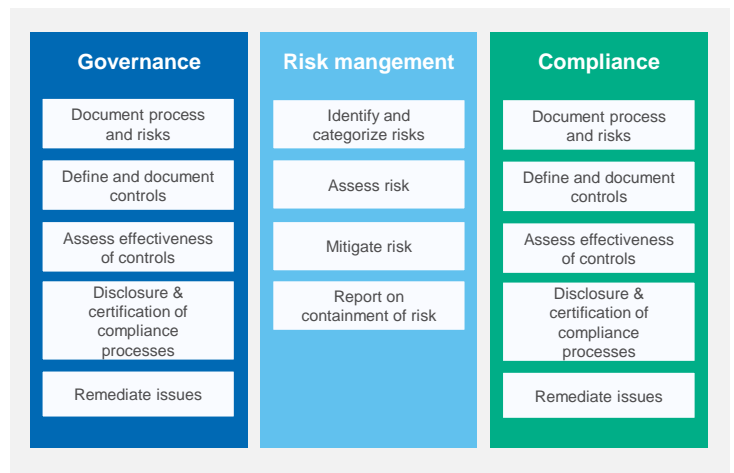
## The challenge

With increasing regulatory requirements, higher business complexity and more focus on accountability, enterprises are forced to pursue a larger scope for governance, risk and compliance initiatives across the organization. However, controls are shared which leads to uncoordinated and unmanaged initiatives or getting planned and managed in silos, potentially increasing the overall business risk for the organization.

Organizations of all sizes are constrained by their available resources; financial, people, and time. To achieve an effective return on investment (ROI) we must prioritize where they will invest. Implementation of security across your organization is also constrained by this, so to achieve an appropriate ROI on security let us first understand and define its security priorities together.

## The solution

Enfo's Information Security GRC Management Service is a managed process towards your organizational IT Security risks.

We will assist you in understanding the business strategy, drivers, strategic risks, risk impacts, risk appetite and management attitude while developing a risk management strategy with better visibility of risks in both business and technical settings.

| Governance | Risk mangement | Compliance |
|---|---|---|
| Document process and risks | Identify and categorize risks | Document process and risks |
| Define and document controls | Assess risk | Define and document controls |
| Assess effectiveness of controls | Mitigate risk | Assess effectiveness of controls |
| Disclosure & certification of compliance processes | Report on containment of risk | Disclosure & certification of compliance processes |
| Remediate issues | | Remediate issues |

## The value

The goal of most organizations is to optimize business value by choosing a level of investments across a portfolio of IT GRC initiatives that support strategic objectives. What is required today is transparency, executive accountability, and tight corporate governance. Key benefits of our Information Security GRC Management service are:

- Continuous Compliance
- Secure your systems
- Enable a responsible workforce
- Risk Focused Decisions
- Improved security posture
- Mitigation of Risk
- Reduce the cost of compliance
- Identify overlaps in controls
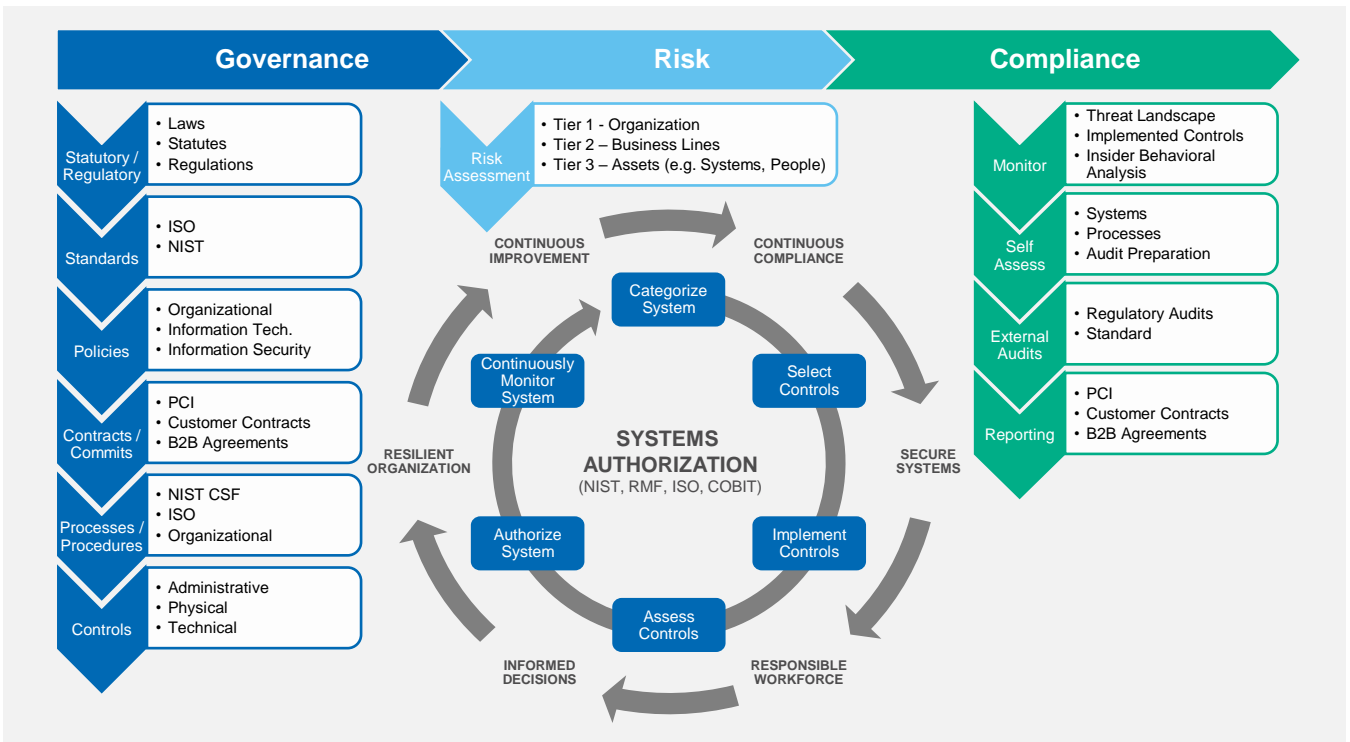- Align your silos

enfo

# Information Security Governance Risk & Compliance (GRC) Management

## The how

The implementation plan and depth of a GRC program varies with each of our partners. Regardless of what level of complexity, there are opportunities to transform or scale your program for the adoption of cloud services, emerging technologies, and other future innovations.

Below is how we can implement an Information Security GRC program for your organization tailored to your business needs. The key objectives in this service are: base governance on objectives and capabilities, include risk context in decision-making, and automate monitoring and response.

### Governance | Risk | Compliance

**Governance**

| Category | Items |
|---|---|
| Statutory / Regulatory | • Laws • Statutes • Regulations |
| Standards | • ISO • NIST |
| Policies | • Organizational • Information Tech. • Information Security |
| Contracts / Commits | • PCI • Customer Contracts • B2B Agreements |
| Processes / Procedures | • NIST CSF • ISO • Organizational |
| Controls | • Administrative • Physical • Technical |

**Risk**

| Category | Items |
|---|---|
| Risk Assessment | • Tier 1 - Organization • Tier 2 – Business Lines • Tier 3 – Assets (e.g. Systems, People) |

**Compliance**

| Category | Items |
|---|---|
| Monitor | • Threat Landscape • Implemented Controls • Insider Behavioral Analysis |
| Self Assess | • Systems • Processes • Audit Preparation |
| External Audits | • Regulatory Audits • Standard |
| Reporting | • PCI • Customer Contracts • B2B Agreements |

**SYSTEMS AUTHORIZATION** (NIST, RMF, ISO, COBIT)

Cycle: Categorize System → Select Controls → Implement Controls → Assess Controls → Authorize System → Continuously Monitor System → (Categorize System)

Outer labels:
- CONTINUOUS IMPROVEMENT
- CONTINUOUS COMPLIANCE
- SECURE SYSTEMS
- RESPONSIBLE WORKFORCE
- INFORMED DECISIONS
- RESILIENT ORGANIZATION

## Why Enfo

Our values are at the core of our actions; collaboration, trust, continuous development and expertise. We walk beside our customers in their data-driven business transformation, taking ownership of their transformation as if it were our own.

**Mastering complexity**

**Confidence in cloud**

**Genuine care**

## Contact us
Email: cybersecurity@enfogroup.com
Web : www.enfogroup.com
Phone:+46 774 404 400

enfo