

Security for IT Governance, Risk Management & Compliance (IT GRC) Align IT Security Policy Management, Enforcement & Audit Logging With Business Risk Management

IT Governance, Risk Management, and Compliance

Today's typical mishmash of siloed technologies and processes leads to inefficiency, increased costs and higher risks to the organization. Security managers, risk managers, and CISOs are asked to deal with ever-increasing and multifaceted threats, but are at the same time challenged to provide increased capabilities and support increased agility to the businesses. These business imperatives, together with increased regulatory pressure and customer demands are forcing many CIOs and CISOs to adopt a unified, structured, enterprise-wide approach to align various governance, risk management, and compliance initiatives. Governance, Risk Management, and Compliance (GRC) is an integrated approach to several overlapping and related activities within an organization, e.g. internal audit, compliance programs like Sarbanes Oxley (SOX), enterprise risk management (ERM), operational risk, incident management, etc. GRC for their IT landscape is called IT-GRC and involves:

- **IT Governance** determines and assigns decision-making, accountability, and decision measuring / monitoring. This is often still ad hoc, siloed and informal.
- **IT Risk Management & Info Security Management** sets the risk tolerance, identifies potential risks, prioritizes the tolerance for risk based on the organization's business objectives, and selects controls to manage and mitigate IT risk. IT risk management includes information security management, which identifies and justifies – based on threats, vulnerabilities, control effectiveness, and residual risk – the controls that need to be implemented to protect information and IT assets against the risks of loss, misuse, disclosure or damage. Numerous standards are available, e.g. ISO 17799, ITIL v3 / ISO 2700x, and COBIT.
- **Compliance** establishes and monitors IT controls to ensure that an organization is adhering to laws and regulations, corporate responsibilities and industry standards. This involves regulatory research, mapping control requirements to regulations, designing IT controls, advising IT and third parties on control requirements and assessing and reporting compliance with regulatory and other requirements. Controls for IT risk and compliance should ideally be unified and based on industry standard common control frameworks (e.g.

COBIT) that can meet multiple regulatory, legal and audit requirements simultaneously.

IT-GRC Needs to Be “Made Real”

While products with built-in mappings for multiple regulations, frameworks and management are now available, most of them do not traceably extend controls from policy to actual operational IT security enforcement, audit logging, and monitoring. Traditional enterprise security policy management for today's complex, interconnected IT environments normally does not achieve this efficiently and consistently due to duplication across technology silos technology-driven / manual administration, and lack of support for agility.

ObjectSecurity's OpenPMF aligns operational IT security enforcement & monitoring with IT-GRC, i.e. automatically ensures that IT security traceably matches with IT-GRC controls (thanks to its unique “model-driven security” approach). It unifies policy management across silos, and enables security managers to maintain security requirements close to their thinking:



ObjectSecurity OpenPMF lets you intuitively select business-centric security & compliance policies, which are then automatically enforced across your IT landscape (using a “model-driven security” approach). You can conveniently manage your policies at run-time, and even change your software applications and workflows without extra administration. OpenPMF reduces costs, improves security, and enables agility. Available as a packaged product and as an integrated turn-key solution.

Products & Services

- OpenPMF (packaged product & turn-key solution)
- SimulateWorld 4D synthetic environment toolkit
- SecureMiddleware: secure open source middleware
- Services: security policy management, Web 2.0 / SOA / Cloud / SaaS Security, middleware security, training workshop, tech. support, R&D
- Studies: in-depth documents about hot topics in security, e.g. model-driven security & SOA

www.objectsecurity.com