

## Suggested review of IT related Governance, Risk and Compliance (GRC) elements

Non-compliance with IT elements of EuroSox<sup>®</sup> can create severe consequences for your company.

- Compliance to the EU directives (EuroSox) must be a top priority on the agenda of CIOs and internal legal departments to avoid sanctions in the event of non-compliance.
- Focus on Financial Reporting processes, IT documentation, internal controls or risk assessment procedures.
- Board members and directors may face personal liability under national laws if the internal control systems or risk management systems are deemed to be inadequate.
- Review the scope of actual IT changes when implementing GRC requirements. Many companies are already subject to similar obligations.

### Recommendations

1. Review the existing documentation of manual processes and IT systems.
2. Review the existing strategy regarding certification under IT security standards
3. Review existing agreements with your suppliers and business partners
4. Review existing contracts that impose IT security and compliance requirements
5. Review or audit compliance with existing IT security and data protection requirements in relation to national data protection laws.

### IT risk Analysis

Regularly search for vulnerabilities in the IT systems. Secure a safety breach before the 'intruder'.

A regular test of IT security is necessary to identify that your defences are working. Verify that your current risk level corresponds to security policy requirements (ISO, CoBIT, ITIL).

Ensure that your IT network is not a potential target by intrusion and vulnerability assessments.

Ensure ongoing fine tuning of the digital defences of the entire IT system.

Implement accurate change management procedures to the periodical changes required in the daily system operation.

Implement accurate change management procedures when implementing changes to the system configuration.

Protect your infrastructure with a variety (firewall, vpn tunnel, anti-virus, etc) of different defence and protection mechanism to defend against intruders.

IT risks appear because:

- Design issues related to system setup or code.
- Missing security patches.
- Systems have been incorrectly configured.
- Software errors in applications.

Ensure continuous monitoring of servers for vulnerabilities.

Assure a complete overview of the current risk level of the corporate network to protect against 'intruders'.