



Information Security Management

DNV IT Global Services - Core Capability

Modern businesses face many challenges and opportunities. Competitive advantage and sustained profitability are essential for survival and development in the marketplace. Standards and performance in the public sector are also under constant and ever closer scrutiny. A critical area that is too often overlooked is that of information security management. This is a process that must be embedded within an organisation from the top down, underpinned by a culture of support and cooperation. When it is done correctly, tangible business benefits can be realised, including increased efficiency, greater clarity and visibility of business processes, awareness of critical assets, risk reduction, and ultimately a direct improvement on the bottom line. Customers can also be assured that information security is taken seriously, including such key aspects as data protection and freedom of information.

The challenge for business leaders is to understand the extent to which information security management already exists within their organisation and to mobilise market leading information security management services to provide the specialist support that will guarantee compliance with industry best practice and national and international standards.

Information Security Management

ITRM offers a portfolio of professional information security management services that can be tailored to meet your specific needs. Whether it is a one-off gap analysis or a full cycle of implementation and certification, we guarantee to identify your critical and other business assets and to deliver appropriate management reports and recommendations. Our consultants have extensive experience across public and private sectors and are uniquely equipped to provide the market leading information security management service.

Our Services

- **Gap Analysis;** a review of current practices, procedures and policies against the standard. Key deliverable – a detailed management report highlighting gaps and including recommendations for corrective action.
- **Security Risk Assessment;** can be performed in isolation or as part of the implementation service. Key deliverable – a detailed management report with a focus on areas of risk and a prioritised set of recommendations for corrective action.
- **Implementation;** a range of professional consulting support to implement the controls specified in the standard.

Key deliverable – expert support tailored and delivered in a way that addresses all controls specified by the standard.

- Certification; a service delivered at the end of the implementation phase that provides formal certification against the standard.

Your Benefits

- A short process that will benchmark performance and compliance against the standard. Provides a quick and effective view of strengths and weaknesses.
- Identification of critical assets, threats and vulnerabilities. Effective information security risk management via implementation of our recommendations.
- Thorough and rigorous process to develop and embed core information security management processes, policies and procedures.
- Protection of key assets and no waste of resources on noncritical areas.
- Business process improvement.
- Improved efficiency
- Compliance with the standard.
- Formal acknowledgement from a recognised certification body of compliance with the standard.

Network Penetration Testing

Computer networks are a critical resource for modern business operations. They provide an ever increasing and diverse range of data, services and functions, both internal and external, denial of access which will inevitably have a negative and direct impact on profitability, reputation, and ultimately survival in the marketplace. Even where the most rigorous design and configuration control standards are implemented, networks and the software needed to run them are inherently vulnerable to malicious attack and accidental or unpredictable events.

Network penetration testing is a crucial element in the armoury of defence against the threat of denial of service. Data confidentiality and integrity are now paramount concerns for most boards of directors. Threats are manifested in many forms, from the casual amateur with no real motivation or resources, through to the state-sponsored full time team of professional hackers, seeking specific targets over an extended time period. The challenges for Chief Information Officers and IT Directors are to understand where they may be vulnerable and to mobilise market leading network penetration testing services as part of a sustained programme of protective measures.

ITRM offers a portfolio of professional network penetration testing services that can be tailored to meet your specific needs. Whether it is a one-off health check or a fully managed service that includes an ongoing schedule of tests, we guarantee to identify and prioritise network vulnerabilities quickly and to provide detailed remedial countermeasures. With direct access to current national threat assessments, tools and techniques, our penetration testing teams operate with complete discretion across heterogeneous environments.

Our Services

- Network discovery; via a range of techniques we can map the network environment down to individual device and service level. Key deliverable – full technical report and executive management summary.
- External test; using only information that is available within the public domain, our penetration testers will attempt network penetration via the Internet. The objective is to gain access to your internal network resources and to escalate the level of privilege to the maximum extent possible. Key deliverable – full technical report including detailed and prioritised remedial countermeasures, plus management summary.
- Internal test; acting as an authorised user, but with no special administrative or other privileges, our penetration testers will attempt to exploit network vulnerabilities in order to escalate privileges and gain access to resources that would not be part of a standard user profile. Key deliverable – full technical report including detailed and prioritised remedial countermeasures, plus management summary.
- Fully managed penetration testing service; a tailored service to meet the specific needs of your environment, providing as a minimum annual internal and external tests, close liaison with your technical specialists, and full support in the implementation of remedial action, as required.

Key deliverables – full technical reports including detailed and prioritised remedial countermeasures, plus management summary.

Your Benefits

- You will know what you have so that you can protect it!
- Clear view of network vulnerabilities that can be exploited via an external attack.
- Rapid protection of critical assets.
- Improved resilience, better availability/ service levels where external attacks are prevented, and enhanced business continuity.
- Reduced Total Cost of Ownership (TCO)
- Clear view of network vulnerabilities that can be exploited via an internal attack.
- Confidence & reassurance of a fully managed service
- Quality output and professional project management
- Guarantee of no service interruptions
- Increased awareness for internal staff on threats, countermeasures and basic tools and techniques for network protection
- Training & knowledge transfer.

Contact

Germany	Tel.: +49 (0) 40 671022 70
UK	Tel.: +44 (0) 207 3576080
	Tel.: +44 (0) 1252 627799
France	Tel.: +33 (0) 1 49 08 58 00
Netherlands	Tel.: +31 (0) 30 230 89 00
Italy	Tel.: +39 0 6 5196 2251
Sweden	Tel.: +46 (0) 46 286 3000
USA	Tel.: +1 (0) 281 721 6600
China	Tel.: +86 (0) 21 3208 4518

e-mail: itgs@dnv.com

web: www.dnv.com/itgs

For further information please contact your local DNV IT Global Services office