



Ensuring Safe Data Delivery

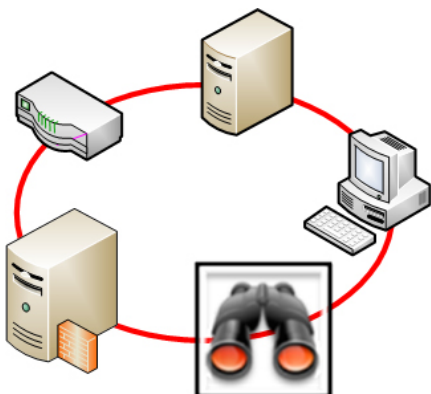
Overview

Information Security consultancy is a core service competency for CNS. Our IT Security expertise has been developed whilst acquiring accreditation (CESG CHECK Scheme & CLAS & PCI DSS QSA), by building strategic partnerships with industry leading institutes (OWASP, BSI, OSTTM, ISO, CPNI, SANS) and with 10 years experience and research in the IS arena.

CNS have developed their own portfolio of services and solutions to assist our clients with achieving Best Practice & accreditation within IT Security. Whether attempting to achieve ISO27001, FSA, CoBIT, PCI DSS, SOX, or any other level of governance or compliance, CNS's services provide pragmatic solutions to what can appear to be complex problems. CNS can manage the full security lifecycle or provide advise, consultancy, testing or rubber stamping.

PLAN: The CNS **Technical & Procedural GAP Analysis against Best Practice** provides any organisation with a clear and invaluable starting point to any IS compliance project. CNS set out to find actual answers to actual questions using a strong technical testing methodology to find every area of weakness (and we do find everything). We then give those weaknesses real risk ratings that can be used at a Business Operational Risk or IT Operational Risk level.

Gaps will be identified at the system or asset level, where appropriate, and reported as control met, partially met, or not met, with supporting detail. There will be a detailed remediation suggestion with each gap identified along with appropriate resources and indication of whether the gap is to be accepted or mitigated, and to what extent mitigation is to occur.



The GAP Analysis will look at, though is not limited to:

1. Policies, processes and standards
2. Security architecture
3. Security controls and tools
4. System development lifecycle
5. Operational IT Security
6. Monitoring, Management and Incident Response
7. General Security Awareness & Training

SERVICES

SECURITY ASSESSMENT

- Penetration Testing
- Application Testing
- Code Review
- PCI DSS Audit
- ISO27001 Audit
- Risk Assessment
- Security Audit
- Compliance Audit
- Configuration Review
- GAP Analysis
- RMADS

MANAGED SERVICES

- 24 x 365
 - Threat Alerting
 - Threat Management
 - Device Management
 - Change Management
 - Fault Resolution
 - Secondments
 - Compliance Monitoring
- #### SECURITY SOLUTIONS
- IPS/NAC
 - Secure Networking
 - Design & Installation
 - Firewall & VPN
 - Identity & Authorisation

ACCREDITATION

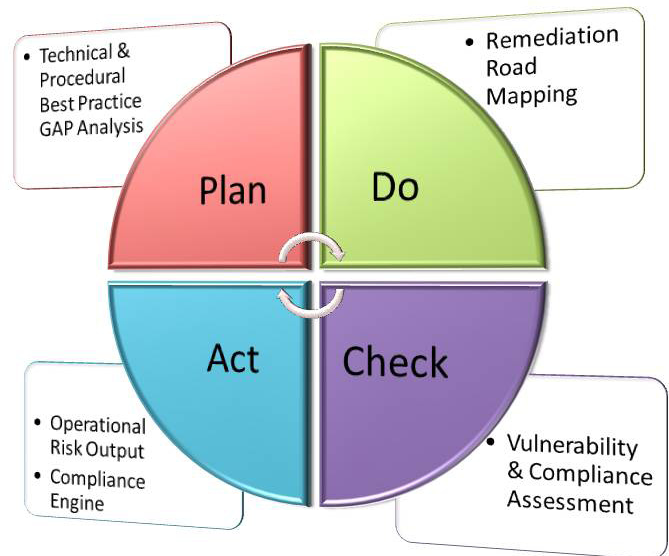


DO: CNS Remediation Roadmapping will pull the information found during the GAP process into an overview roadmap to closing the gaps identified in the analysis and present a clear remediation path that will cover the following:

- Approach and Benchmark
- Description of existing controls and ISMS maturity level
- Identified Gaps and risk categorisation
- Map of Gaps to regulatory compliance needs of chosen standard.
- Recommendations for improvement.
- A roadmap of initiatives for improvement detailing a programme of development, with priorities based on risk and impact analysis.

Using CNS's **Compliance SCAN Engine** the following metrics can be monitored:

- Configuration change alerting on network devices
- Vulnerability scans on network devices
- Automated (with manual checking) network device (e.g. firewall) configuration checks
- Patch checking (multiple platforms)
- Configuration checking (multiple platforms)
- Vulnerability scans on hosts
- Port scanning (and port scanning diffs)
- AV status
- Application (e.g. Oracle, SQL, Apache) configs and changes
- Configuration change on AD policies
- File/db column change alerting
- Password strength checks



ACT: The output from operational monitoring is constantly compared to previous results, and analysed against trends overtime, in order to ensure an improving security posture; the results of which can be fed into the CNS **Compliance Report Engine**. The compliance engine not only ensures that compliance is maintained but will also match the relevant controls from one standard of regulation against the corresponding element of another in order to reduce duplication of effort and maximise the effect of CNS services with in a customer. For example ISO27001, PCI, CoBIT & FSA regulation can be measured concurrently.

CHECK: CNS's **Managed Vulnerability & Compliance Assessment** combines a number of vulnerability assessment activities to deliver a constant review of a customers applications & infrastructure. Rather than producing a snap shot of the system vulnerability footprint the service seeks to regularly assess the network in order to manage threats as the vulnerability landscape evolves.

About CNS

Convergent Network Solutions Ltd was established in 1999 in response to market demand for a highly skilled security and networking consultancy in the heart of the city. CNS has grown rapidly since this time, both in company size, the depth and breadth of services offered and reputation for providing exemplary service. The company is majority owned by the principle directors.