telkomtelstra

Security Consulting

Network Compliance Strategy

How we can help

Our Network Compliance Strategy Service helps you:

- Analyse your high level network security compliance gaps against relevant security compliance requirements, regulations, standards and industry best practices. These include the telkomtelstra Network Security Reference which leverages better practices from our own network experience as well as a range of referenceable standards and guidelines, including but not limited to SANS Critical Security Controls, DSD ISM, PCI-DSS, ISO27001-2, etc.
- Define a strategy to better manage your network security compliance gaps and issues on an ongoing basis.

About the service

The key objectives of this service are to:

- Identify or confirm your security compliance requirements, based on the industry standards and best practices, laws and regulations which you advise us as being applicable to your business
- Conduct a high level compliance gap assessment of your network security position and network security controls, including architecture/ technologies, processes and people, against the standards you've selected and best practices
- Provide strategic recommendations to manage your network security compliance gaps on an ongoing basis, inclusive of an actionable strategic plan.

The assessment activities rely on a combination of:

- Interviews with key stakeholders
- High level desktop review of available technology risk and security management artefacts relevant to your network environment
- The results and recommendations are prioritised according to their relevance to your business, security compliance obligations and risk appetite.

What's Included

1. **Planning and Preparation**
   Gain an understanding of the following:
   - The relevant security stakeholders and responsible parties within your organisation
   - Any specific, existing security-related concerns
   - The details of any recent security incidents
   - Your network environment, including topology, technology and management processes
   - Confirmation of the assessment plan.

2. **Conduct Assessment**
   The assessment is typically made up of the following activities:
   - A high level understanding of your organisation's business and IT assets, ie: services, information, architecture and technologies
   - Identification of internal and external compliance requirements based on industry standards, best practices, regulations and as they apply to your business
   - Undertake a compliance gap analysis against the above for; governance, processes, architecture and technologies
   - Draft recommendations for improvement and present as a strategic and prioritised action plan
   - Provide input into the business case.

3. **Test the Recommendation**
   Discuss the findings and analysis with you and test our proposed recommendations to validate they are meaningful, realistic and achievable.

4. **Report**
   Produce a report including the following sections:
   - Executive Summary: a business view of our results and what they means to you
   - Methodology: what we did and how
   - Findings, analysis and recommendations.

5. **Follow up**
   A follow up meeting to discuss the report and progress remediation activity.

What we do

In addition to the above, the following are our responsibilities as part of the Network Compliance Strategy Service:

- Assessment plan
- Report delivery
- Provision of an experienced senior security consultant.

What you do

The following are ways in which you can help us deliver your Network Compliance Strategy Service:

- Program/project management and co-ordination
- Business and technical information, as required
- Ensure all information provided by you is up to date and valid for your current environment, including designs, topologies and requirements
- Identify your key representatives and define how they'll participate in the delivery of this service; include executive and senior management across the business, business analysts/architects, systems and network engineers
- Ensure that your people are available during the course of the engagement to provide information and to participate in scheduled information gathering sessions, interviews, meetings and conference calls.

Related Services

- Network Architecture Assessment
- Penetration Testing
- Vulnerability Assessment