IPSec Risk and Compliance Reporting

Sample Output – VPDSS
Sample assessment output

After completion of the assessments, the results are immediately available from the reporting engine.

This document is intended to demonstrate some of the features within the reporting functionality delivered via the browser based tool.

The header of Risk Report is the identifier and the other core components are as follows:

1. Management Summary
2. Risk Heat Map
3. Risk Diagram
4. Gap Analysis
5. Compliance Summary
6. Risk Management
1. Management Summary

Below is a sample of the management summary output. As can be seen, the findings are collated by risk rating.

Management Summary

Overall a key risk of harm to health and safety of people, financial loss to the organisation and the organisation's operations being significantly impacted by legal proceedings for IPSec was identified.

No critical risks were identified.

A very high risk of
- inactivity in case of a disruptive or emergency event,
- people being insufficiently protected in emergency events,
- people's health and safety being affected through the effects of the disruptive or emergency event,
- one person obtaining conflicting permissions to circumvent established controls (Segregation of Duties),
- inappropriate use of the organisation's assets,
- unethical business practices,
- the organisation's trustworthiness being damaged through bad press,
- classified information being disclosed to unauthorised parties,
- fraudulent, illegal or reckless business practices remaining undetected,
- fraudulent business or accounting practices remaining undetected,
- the organisation violating data privacy legal requirements,
- excessive risk remaining intransparent or unmanaged to risk owners,
- the organisation's intellectual property being disclosed to competitors,
- customers reducing business with the organisation,
- reduced operational effectiveness,
- resources being used inefficiently,
- opportunity costs to the business,
- funds being used inappropriately,
- the organisation being unprepared for certain types or severities of threats,
- insufficient action taken to ensure continuity of operations in case of a disruptive or emergency event,
- parts of the organisation being no longer operational,
- reduced revenue,
- legal and regulatory requirements not being met and
- the organisation being fined

was identified.
2. Risk Heat Map

The above diagram determines the risk criticality based on identified deviations of the controls between expected and assessed maturity, the degree of separation in the risk tree and linkage to further control statements. The weighted overview identifies all possible risks which need to be assessed in the context of each individual organisation.

Drill down of 7 Very High Risk items (Likelihood = Certain / Consequence = Critical)

- There is a very high risk of classified information being disclosed to unauthorised parties.
- There is a very high risk of the organisation's intellectual property being disclosed to competitors.
- There is a very high risk of the organisation being unprepared for certain types or severities of threats.
- There is a very high risk of insufficient action taken to ensure continuity of operations in case of a disruptive or emergency event.
- There is a very high risk of parts of the organisation being no longer operational.
- There is a very high risk of reduced revenue.
- There is a very high risk of the organisation being fined.
3. Risk Diagram

Highlighting root cause Control Weaknesses that lead to Business Risks

Root Cause Graph: There is a very high risk of classified information being disclosed to unauthorised parties.

- Weakness in SEM Definition
- Weakness in Incident Response
- Weakness in Alerting and Escalation
- Weakness in Physical Security Controls
- Weakness in Email Service
- Weakness in Mobile Device Management Leadership
- Weakness in Remote Wiping Capability
- Weakness in Mobile Device Management Tools
- Weakness in Two Factor Authentication
- Weakness in Authentication for External Network Access
- Weakness in Non-Permanent Employees
- Weakness in Secure Destruction Requirement
- Weakness in Dedicated Credentials
- Weakness in Data Ownership

- This raises the risk of insufficient security event information not being actionable.
- This raises the risk of insufficient capability of analysing security events.
- This raises the risk of insufficient response to a security event.
- This raises the risk of insufficient reactions to data breaches.
- This raises the risk of data loss or data breaches going unreported.

This raises the risk of people having inappropriate access to the organisation's assets.

This raises the risk of system or applications and underlying data being accessed by unauthorised parties.

This raises the risk of wakalhe pledgencies on untrusted mobile platforms remaining unmanaged.

This raises the risk of insufficent protection against malicious applications or applications being placed to the organisation's data.

This raises the risk of insufficient control mechanisms being incorporated or broken.

This raises the risk of classified information during external processing.

This raises the risk of insufficient data ownership.
4. Gap Analysis – core component of SRPA

Each topic allows links back to the assessment to understand underlying control scoring
5. Compliance Summary

This report shows all major compliance deviations and allows cross referencing to any two information security standards to highlight the applicable control statements.
Link to Business Continuity Protocols

Standard
An organisation must establish, implement and maintain a business continuity management program that addresses the security of public sector data.

Statement of Objective
To enhance an organisation’s capability to prevent, prepare, respond, manage and recover from any event that affects the confidentiality, integrity and availability of public sector data.

Protocol 8.1
There is executive sponsorship of security requirements, and they are incorporated in the organisation’s business continuity management program.

Protocol 8.2
Security requirements are implemented in the organisation’s business continuity management program.

Protocol 8.3
Security requirements are appropriately monitored and reviewed in the organisation’s business continuity management program.
6. Risk Register Dashboard & Task Manager – core component of PDSP

The on-line dashboard allows the risks to be grouped (on an inclusive or exclusive basis) showing the Risk appetite vs Residual risk based on a chosen standard. As risks are mitigated through control improvements, the dashboard shows dynamically in real time the reduction in the risk profile.

The inbuilt task manager makes assigning and managing individual tasks straightforward.