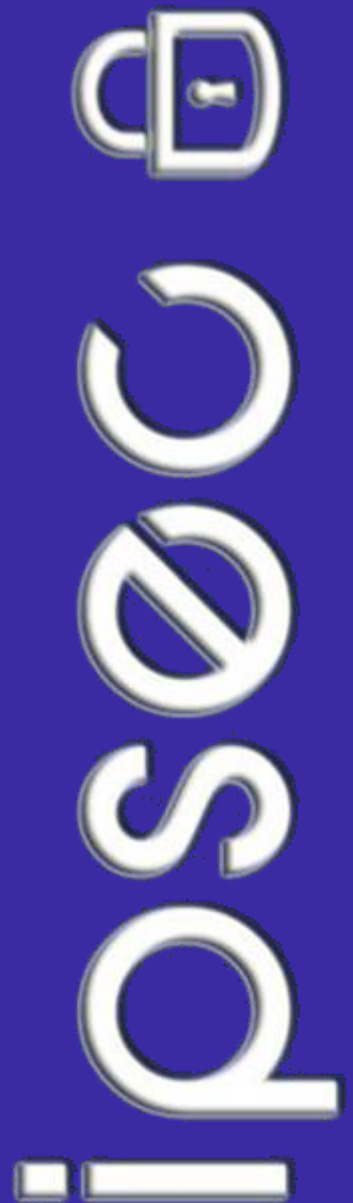


IPSec Risk and Compliance Reporting

Sample Output – ISO 27001

ipsecc  consult



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

REPORT DESCRIPTION

XXXXXX - ISO 27001


This Report measures Assessment against 27001.

Assessment Period: 27 September 2016 to 28 September 2016


Assessed Objects: 1
Control Statements: 433
Risk tolerance 1

Creator: Jeff Sussman (29 September 2016)

Management Comments



RESPONDENTS:



ASSESSED TOPICS:

Audit

Cryptography

Outsourcing

Procurement

Social Media

more

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, the organisation's operations being significantly impacted by legal proceedings and financial loss to the organisation for IPSec was identified.

CRITICAL RISKS

No critical risks were identified.

25 VERY HIGH RISKS

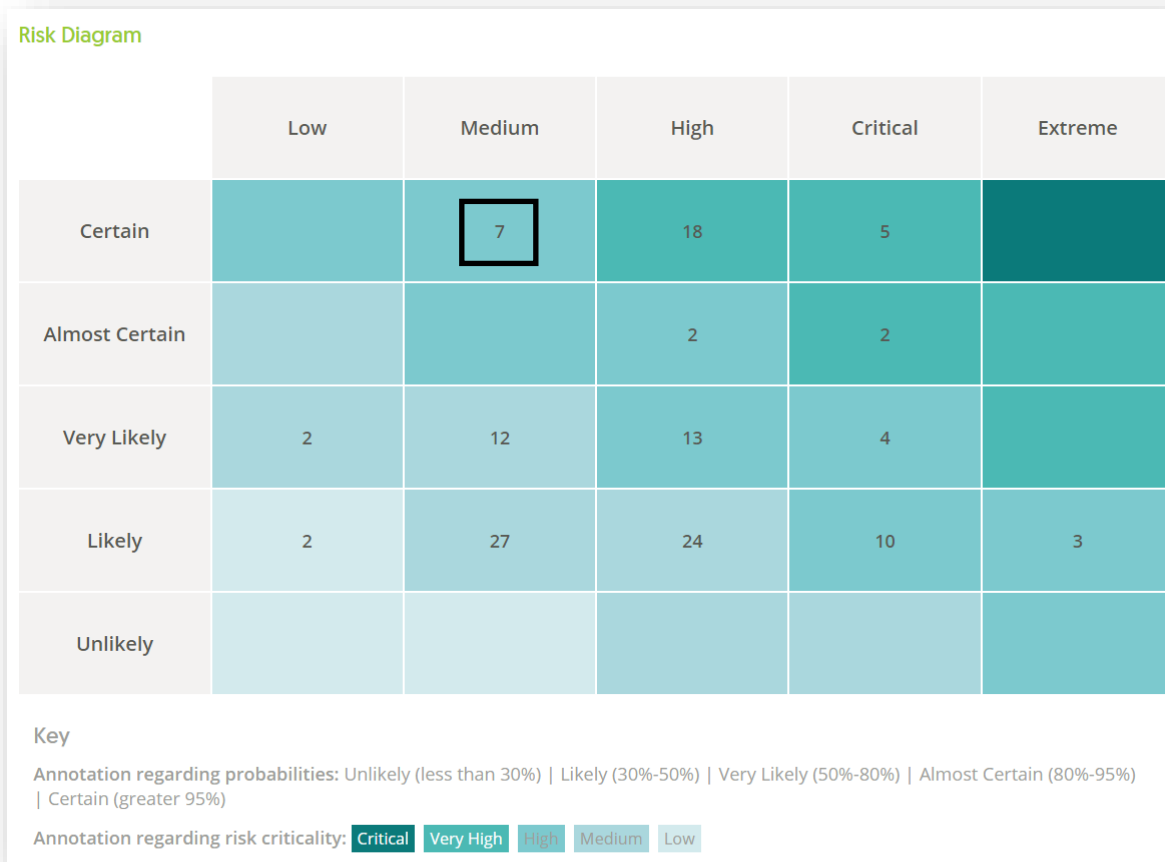
[Show risk details](#)

A very high risk of

- passwords being disclosed to unauthorised parties,
- people having inappropriate access to the organisation's assets,
- theft of the organisation's assets,
- inappropriate use of the organisation's assets,
- unethical business practices,
- resources being used inefficiently,
- physical damage to an asset of the organisation,
- quality issues with production IT systems,
- insufficient capability of analysing security events,
- insufficient response to a security event,
- data loss or data breaches going undetected,
- repeated breaches of non-public information,
- the organisation's trustworthiness being damaged through bad press,
- systems or applications and underlying data being accessed by unauthorised parties,
- opportunity costs to the business,
- classified information being disclosed to unauthorised parties,
- 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,
- parts of the organisation being no longer operational,
- reduced revenue,
- legal and regulatory requirements not being met,
- the organisation being fined and
- funds being used inappropriately

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.

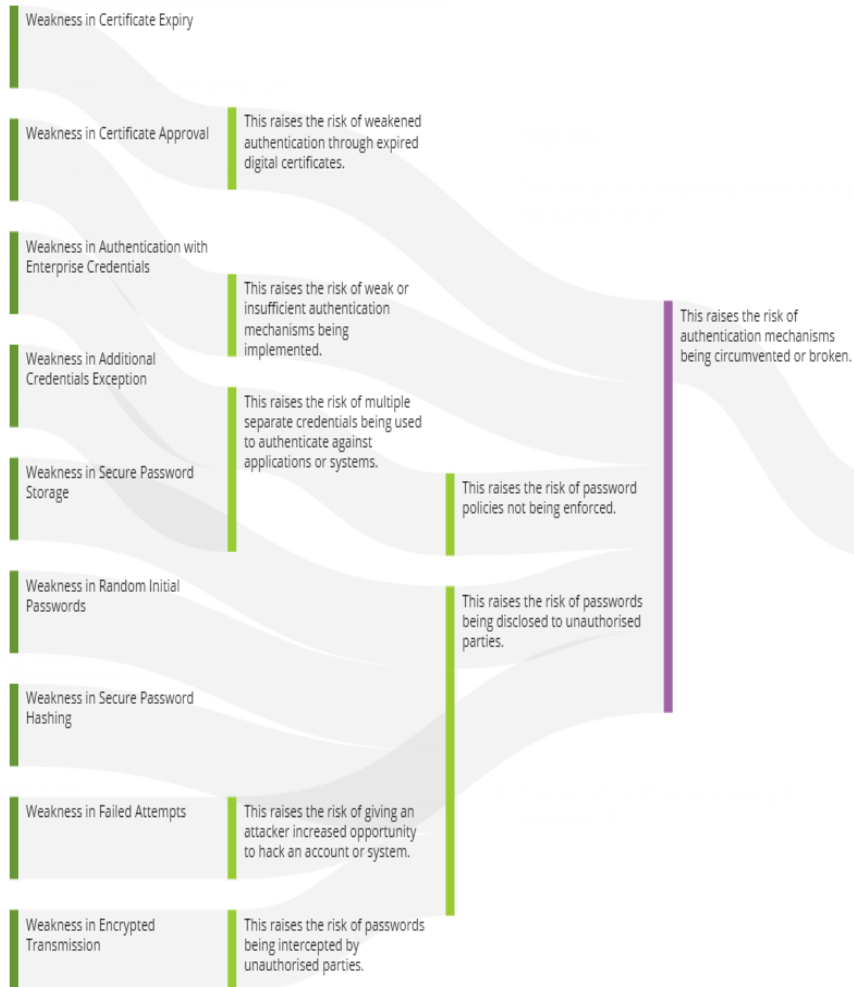
Drill down of **7 High Risk** items (Likelihood = Certain / Consequence = Medium)

- There is a high risk of authentication mechanisms being circumvented or broken.
- There is a high risk of incorrect processing of information.
- There is a high risk of IT providing insufficient support to the organisation's business.
- There is a high risk of insufficient reactions to data breaches.
- There is a high risk of the organisation's failure to notify data subjects of a breach.
- There is a high risk of the organisation's customers lose faith in the organisation's ability to secure personally identifiable information.
- There is a high risk of legal or regulatory business continuity requirements not being met.

3. Risk Diagram

Highlighting Control Weaknesses that lead to Business Risks

Root Cause Graph: There is a high risk of authentication mechanisms being circumvented or broken.



Source Control	Deviation
Certificate Approval <	2
Certificate Expiry <	2
Authentication with Enterprise Credentials <	2
Additional Credentials Exception <	2
Secure Password Storage <	2
Random Initial Passwords <	2
Secure Password Hashing <	2
Encrypted Transmission <	2
Failed Attempts <	2

4. Gap Analysis

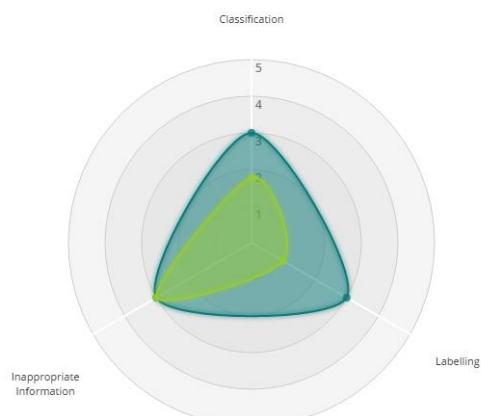
Deviation Radar

Expected vs Assessment Maturity by Topic



Each topic allows further drill down to understand underlying control scoring

Topic: Information Classification



Subtopic (Expected / Assessed)

1	Labelling	3 / 1
2	Classification	3 / 1.78
3	Inappropriate Information	3 / 3

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.

Compliance Summary

Compare the compliance to 2 standards

Medium Deviations: 72 Control Statements					Sample of Standards	
					ISO/IEC 27001:2013	COBIT 4.1
Control Statement Title	Target	Assessed	Primary Standards	Secondary Standards	ISO/IEC 27001:2013	COBIT 4.1
Application Governance Tasks	3	1	A.12.1.1	DS1.4, DS1.5, DS1.6	Select standard 1	
Application Product Plan	3	1	8.1, A.12.1.2, A.14.2.2	AI2.10	ISO/IEC 27001:2005	
Vulnerability Assessment	3	1	A.17.1.1		ISO/IEC 27001:2013	
Approved Cryptographic Measures	3	1	A.10.1.1, A.18.1.5	DS5.8	COBIT 4.1	
Usage of Cryptography	3	1	A.10.1.1	DS5.8	COBIT 5	
Cryptography Strength	3	1	A.10.1.1, A.8.2.2	DS5.8	BSI Grundschrift	
Encryption Requirements	3	1	A.10.1.1, A.8.2.2, A.14.1.2, A.14.1.3	DS5.11	MAS TRMG	
Cryptography Review	3	1	A.10.1.1	DS5.8	FIN-FSA OpRisk	
Key Generation	3	1	A.10.1.1, A.10.1.2	DS5.8	MaRisk BA (10/2012)	
Key Storage	3	1	A.10.1.1, A.10.1.2	DS5.8	UK Cyber Essentials	
Redundant Storage	3	1	A.10.1.1, A.10.1.2	DS5.8	NIST Cyber security 2014	
Cryptography at Application Layer	3	1	A.10.1.1	DS5.8	GOBS	
					HGB	
					Fed Guideline IS	
					ISO 22301:2012	
					VPDSS	
					BDSG	
					EU Directive 95/46/EC	
					PCI DSS v3.1	
					TMG	

Example of Vulnerability Assessment cross referenced to ISO 27001:2013 Annex A.17.1.1

A.17 Information security aspects of business continuity management		
A.17.1 Information security continuity		
Objective: Information security continuity shall be embedded in the organization's business continuity management systems.		
A.17.1.1	Planning information security continuity	<i>Control</i> The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.
A.17.1.2	Implementing information security continuity	<i>Control</i> The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

6. Risk Register Dashboard & Task Manager

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.

