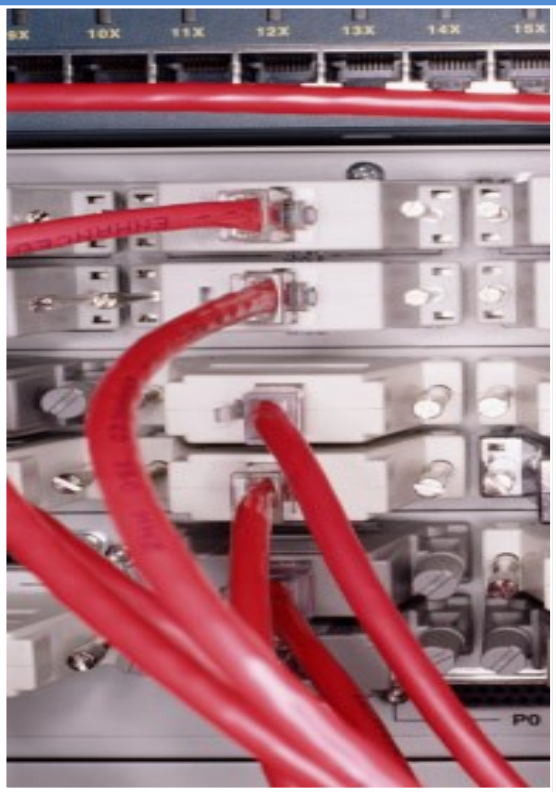
YourIT!
Your Logo Goes Here

GDPR Assessment

Data Protection Impact Assessment



Scan Date: 1/18/2018

Prepared for:
My Client Company
Prepared by:
YourIT Company

1/18/2018

Table of Contents

Overview

Risk management, a component of the assessment process, includes the implementation of security measures to reduce risk to reasonable and appropriate levels to, among other things, ensure the confidentiality, availability and integrity of data and protect against any reasonably anticipated threats, hazards, or disclosures not permitted or required. This document provides a risk analysis with an emphasis on the protection of personal data.

After performing the risk analysis, the next step in the risk management process is to develop and implement a Risk Treatment Plan. The purpose of a Risk Treatment Plan is to provide structure for the evaluation, prioritisation, and implementation of risk-reducing measures and controls.

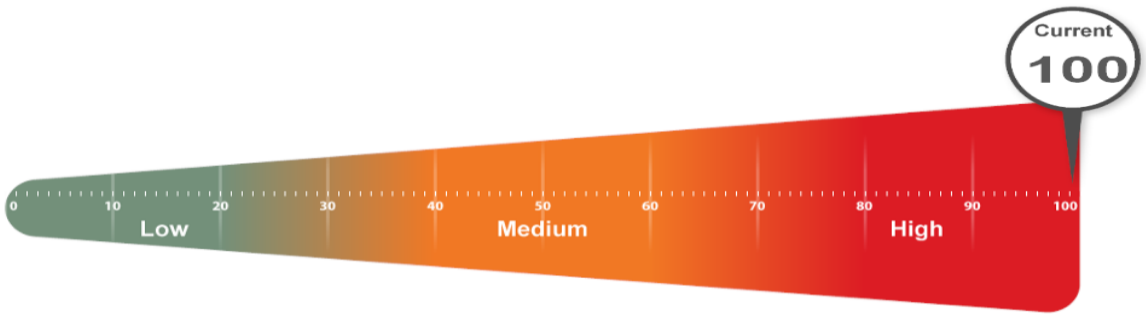
Risk prioritisation and mitigation decisions will be determined by answering which controls and measures should be implemented and the priority in which they should be addressed based upon their "risk score". The implementation components of the plan include:

- Risk score (threat and vulnerability combinations) assigned to a particular issue being addressed.
- Recommendation(s) of measures and controls selected to reduce the risk of an issue.
- Ongoing evaluation and monitoring of the risk mitigation measures.

Risk analysis and risk management are not one-time activities. Risk analysis and risk management are dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management process to reduce newly identified or updated risk levels to reasonable and appropriate levels.

Risk Score

The Risk Score is a value from 0 to 100, where 100 represents significant risk potential. The score is based on the issues with the highest risk identified during the assessment.

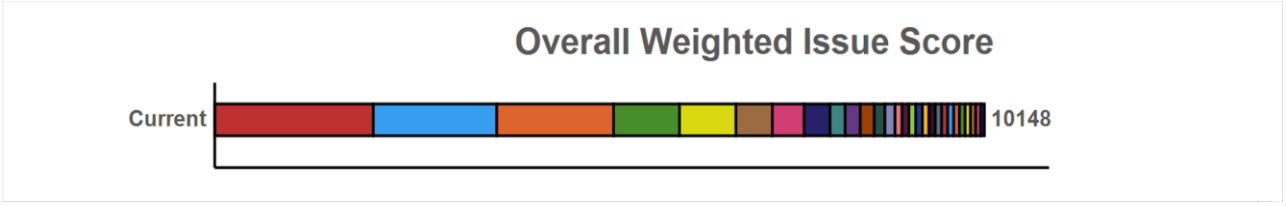


Several critical issues were identified. Identified issues should be investigated and addressed according to the Risk Treatment Plan.

If additional information is needed on how the Risk Score was determined, please consult the Evidence of Compliance.

Issue Summary

This section contains a summary of issues detected during the assessment process, and is based on industry-wide best practices for network health, performance, and security. The Overall Issue Score grades the level of issues in the environment. An Overall Issue score of zero (0) means no issues were detected in the environment. It may not always be possible to achieve a zero score in all environments due to specific circumstances.



Weighted Score: Risk Score x Number of Incidents = Total points: Total percent (%)

	Issues found during walk-through of physical environment (95 pts each)
2090	***Current Score:*** 95 pts x 22 = 2090: 20.6%
	Requirement: ISO 27001-2013 (8.3.1) - Management of removable media ISO 27001-2013 (8.3.2) - Disposal of media ISO 27001-2013 (11) - Physical and environmental security
	Issue: ISO 27001 defines several controls to protect the physical environment, media, and computing facilities from unauthorised physical access. Issues were found during the walk-through of the physical environment and documented in the Site Walkthrough Checklist.
	Recommendation: Address the issues found during the walk-through of the physical environment.

	Inadequate password lockout duration (74 pts each)
1628	***Current Score:*** 74 pts x 22 = 1628: 16.04%
	Requirement: ISO 27001-2013 (9.4.3) - Password management system
	Issue: Account lockout duration not set to a minimum of 30 minutes or until an administrator enables the user ID.
	Recommendation: Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

	Password attempt lockout not enforced (77 pts each)
1540	***Current Score:*** 77 pts x 20 = 1540: 15.18%
	Requirement: ISO 27001-2013 (9.4.3) - Password management system
	Issue: Limit repeated access attempts by locking out the user ID after not more than six attempts.
	Recommendation: Ensure password lockout is enforced after more than six attempts.

	Unrestricted web access from DPE (87 pts each)
870	***Current Score:*** 87 pts x 10 = 870: 8.57%
	Requirement: ISO 27001-2013 (13.1.1) - Network controls
	Issue: Web access should be restricted to what is necessary. Access to various sites were found to be unrestricted in the Data Processing Environment (DPE).

	Recommendation: Block web traffic to all sites not required by the DPE.

	Potential Former Employee and Former Third Parties with Enabled Accounts (62 pts each)
744	***Current Score:*** 62 pts x 12 = 744: 7.33%
	Requirement: ISO 27001-2013 (9.4.1) - Information access restrictions
	Issue: One or more user accounts had no activity in the past 30 days. This could be an indication that these accounts should be disabled.
	Recommendation: Investigate and determine if the users are former employees or third parties. Disable the accounts if they are no longer necessary.

	Privacy policy missing required elements (80 pts each)
480	***Current Score:*** 80 pts x 6 = 480: 4.73%
	Requirement: GDPR Regulation (EU) 2016/679 Article 13 - Information to be provided where personal data are collected from the data subject Article 14 - Information to be provided where personal data have not been obtained from the data subject
	Issue: GDPR lists a set of requirements that should be presented to the data subject where personal data is collected. A response of 'no' was provided in the GDPR Compliance Questionnaire to one or more of these required elements in the Privacy Policy.
	Recommendation: Ensure that the Privacy Policies has the required elements.

	Potential Generic Accounts found (70 pts each)
420	***Current Score:*** 70 pts x 6 = 420: 4.14%
	Requirement: ISO 27001-2013 (9.4.1) - Information access restrictions
	Issue: Generic account logins were used on one or more computers and should be investigated. The use of generic logins may prevent proper tracking and identification and is discouraged. There are legitimate uses for generic logins, such as limited administrative access and use, as well as access to workstations where secondary logins are required to access the Data Processing Environment. If access is deemed inappropriate, further action should be taken to ensure the situation is remediated.
	Recommendation: Investigate and either disable or note compensating controls to ensure these potential generic accounts are not used inappropriately. Service accounts are excluded.

	Best practises not adhered to regarding access to program source code (85 pts each)
340	***Current Score:*** 85 pts x 4 = 340: 3.35%
	Requirement: ISO 27001-2013 (9.4.5) - Access control to program source code
	Issue: ISO 27001 requires controls regarding access to program source code. The ISO 27001 Compliance Questionnaire indicates that some controls are not adhered to.
	Recommendation: Adhere to the best practises regarding access control to program source code.

	Unauthorised user (100 pts each)

200	***Current Score:*** 100 pts x 2 = 200: 1.97%
	Requirement: ISO 27001-2013 (9.2.5) - Inventory of assets
	Issue: As part of reviewing the user access, some users were identified as unauthorized.
	Recommendation: Investigate and remove all users that are not authorised.

	Non-compliance with principles relating to processing of personal data (100 pts each)
200	***Current Score:*** 100 pts x 2 = 200: 1.97%
	Requirement: GDPR Regulation (EU) 2016/679 Article 5 - Principles relating to processing of personal data
	Issue: GDPR lists a set of guiding principles relating to the processing of personal data. A response of 'no' was provided in the GDPR Compliance Questionnaire to one or more of these principles.
	Recommendation: Ensure that personal data is processed in a manner that complies with these principles related to data processing.

	Anti-spyware not turned on (92 pts each)
184	***Current Score:*** 92 pts x 2 = 184: 1.81%
	Requirement: ISO 27001-2013 (12.2.1) - Controls against malware
	Issue: Malware protection is required but not identified as being enabled on computers in the network.
	Recommendation: Enable anti-spyware programs on the computers indicated in the Endpoint Security section of the Evidence of GDPR Compliance report.

	Automatic screen lock not turned on (70 pts each)
140	***Current Score:*** 70 pts x 2 = 140: 1.38%
	Requirement: ISO 27001 – 11.2.8 Unattended user equipment
	Issue: Automatic screen lock prevents unauthorized access when users leave their computers. Having no screen lock enabled allows unauthorized access to network resources.
	Recommendation: Enable automatic screen lock on the specified computers.

	Third-party access should be disabled when not in use (67 pts each)
134	***Current Score:*** 67 pts x 2 = 134: 1.32%
	Requirement: ISO 27001-2013 (9.4.1) - Information access restrictions
	Issue: Third-party user accounts with access rights to the Data Processing Environment and/or system components must be disabled when not in use.
	Recommendation: Disable third-party accounts when not in use.

	Anti-virus not turned on (92 pts each)
92	***Current Score:*** 92 pts x 1 = 92: 0.91%
	Requirement: ISO 27001-2013 (12.2.1) - Controls against malware
	Issue: Malware protection is required but not identified as being enabled on computers in the network.

Recommendation: Ensure anti-virus programs on the computers indicated in the Endpoint Security section of the Evidence of GDPR Compliance report are up-to-date.

	Many security patches missing on computers (90 pts each)
90	***Current Score:*** 90 pts x 1 = 90: 0.89%
	Requirement: ISO 27001-2013 (12.2.1) - Controls against malware
	Issue: Address patching on computers with missing security patches.
	Recommendation: Security patches are missing on computers. Maintaining proper security patch levels helps prevent unauthorised access and the spread of malicious software. Many is defined as missing three or more patches.

	Consent not provided for the use of personal data (90 pts each)
90	***Current Score:*** 90 pts x 1 = 90: 0.89%
	Requirement: GDPR Regulation (EU) 2016/679 Article 7 - Conditions for consent
	Issue: GDPR requires that all processing of personal data have explicit consent. Some processing of personal data was indicated to not have consent in the GDPR Compliance Questionnaire.
	Recommendation: Ensure that the processing of personal data has explicit consent.

	Administrative account auditing adequately enabled (89 pts each)
89	***Current Score:*** 89 pts x 1 = 89: 0.88%
	Requirement: ISO 27001-2013 (12.4.3) - Administrator and operator log
	Issue: Accounts with increased privileges, such as the \"administrator\" or \"root\" account, have the potential to greatly impact the security or operational functionality of a system. Without a log of the activities performed, an organisation is unable to trace any issues resulting from an administrative mistake or misuse of privilege back to the specific action and individual.
	Recommendation: Enable auditing of all actions taken by any individual with root or administrative privileges.

	Lack of information security awareness training (85 pts each)
85	***Current Score:*** 85 pts x 1 = 85: 0.84%
	Requirement: ISO 27001-2013 (7.2.2) - Information security awareness training
	Issue: ISO 27001 requires that all employees and contractors, if relevant, receive awareness education and training and regular updates of security policies and procedures. The ISO 27001 Compliance Questionnaire indicates that documentation that all employees have received information security awareness training is not available.
	Recommendation: Provide security awareness and training for employees and contractors, if relevant, and provide appropriate records and documentation.

	Documentation of contact with authorities not provided (85 pts each)
85	***Current Score:*** 85 pts x 1 = 85: 0.84%
	Requirement: ISO 27001-2013 (5.1.2) - Review of the policies for information security
	Issue: ISO 27001 requires contacts with relevant authorities be maintained. The ISO 27001 Compliance Questionnaire indicates you either do not maintain documentation of

	contact with authorities or did not provide attached documentation.
	Recommendation: Maintain documentation of when and which authorities to contact and how identified information security incidents should be reported in a timely manner.

	Lack of documented information security incident management (83 pts each)
83	***Current Score:*** 83 pts x 1 = 83: 0.82%
	Requirement: ISO 27001-2013 (16) - Information security incident management
	Issue: ISO 27001 requires documented procedures for information security incident management, including procedures for incident response, escalation and reporting. The ISO 27001 Compliance Questionnaire indicates that documented procedures for information security incident management are not available.
	Recommendation: Document information security incident management procedures. See ISO 27001-2013 (16) for additional guidance.

	Documentation of cryptographic controls procedures not provided (80 pts each)
80	***Current Score:*** 80 pts x 1 = 80: 0.79%
	Requirement: ISO 27001-2013 (10.1) - Cryptographic controls
	Issue: ISO 27001 requires a documented cryptographic control procedure which includes key management. The ISO 27001 Compliance Questionnaire indicates lack of a documented cryptographic control procedure.
	Recommendation: Document cryptographic control procedures, including key management.

	Information security not integrated into the project management process (80 pts each)
80	***Current Score:*** 80 pts x 1 = 80: 0.79%
	Requirement: ISO 27001-2013 (6.1.5) - Information security in project management
	Issue: ISO 27001 requires that information security be integrated with project management methods to ensure risks are identified and addressed. The ISO 27001 Compliance Questionnaire indicates information security is not integrated into the project management process, regardless of type of project.
	Recommendation: Integrate information security into the project management methodology to ensure risks are identified and addressed.

	Lack of documented information security continuity plan (75 pts each)
75	***Current Score:*** 75 pts x 1 = 75: 0.74%
	Requirement: ISO 27001-2013 (17.1) - Information security continuity
	Issue: ISO 27001 requires documented procedures for information security incident management, including procedures for incident response, escalation and reporting. The ISO 27001 Compliance Questionnaire indicates that documented procedures for information security incident management are not available.
	Recommendation: Document information security incident management procedures. See ISO 27001-2013 (16) for additional guidance.

	Best practises not adhered to during physical media transfer (75 pts each)
75	***Current Score:*** 75 pts x 1 = 75: 0.74%

	Requirement: ISO 27001-2013 (8.3.3) - Physical media transfer
	Issue: ISO 27001 requires media containing sensitive information be protected during transport. The ISO 27001 Compliance Questionnaire indicates that some best practices are not adhered to.
	Recommendation: Adhere to the following best practices for physical media transfer.

	Method of consent not provided for the use of personal data (70 pts each)
70	***Current Score:*** 70 pts x 1 = 70: 0.69%
	Requirement: GDPR Regulation (EU) 2016/679 Article 7 - Conditions for consent
	Issue: GDPR requires that all processing of personal data have explicit consent. A documented reason for processing of personal data was not provided in the GDPR Compliance Questionnaire.
	Recommendation: Enter a documented reason for the processing of personal data in the GDPR Compliance Questionnaire.

	Auditing for account changes required (69 pts each)
69	***Current Score:*** 69 pts x 1 = 69: 0.68%
	Requirement: ISO 27001-2013 (12.4.3) - Administrator and operator log
	Issue: Auditing use of and changes to identification and authentication mechanisms - including but not limited to creation of new accounts and elevation of privileges - and all changes, additions, or deletions to accounts with root or administrative privileges is required.
	Recommendation: Enable auditing of changes to account identification and authentication mechanisms.

	Lack of documented information labelling process (65 pts each)
65	***Current Score:*** 65 pts x 1 = 65: 0.64%
	Requirement: ISO 27001-2013 (8.2.2) - Labelling of information
	Issue: ISO 27001 requires a documented information labelling process. The ISO 27001 Compliance Questionnaire indicates that a documented information labelling process is not available.
	Recommendation: Implement a documented information labelling process.

	Contact with special interest groups not provided (50 pts each)
50	***Current Score:*** 50 pts x 1 = 50: 0.49%
	Requirement: ISO 27001-2013 (6.1.4) - Contact with special interest groups
	Issue: ISO 27001 suggestions maintenance of contacts with special interest groups and information security-related professional organisations to stay up to date with relevant security information.
	Recommendation: Maintain contact with special interest groups and document which individuals participate in the organisations.