ISO 27001: A Guide to Implementation

June 2020

Craig Thornton

- Part-Owner Mango Limited
  - craig@mangolive.com
  - +64 29 377 5444
  - LinkedIn
    - https://www.linkedin.com/in/craigthorntonmango/
- Resources
  - https://www.mangolive.com/resources
- Survey
  - ISO Integrated Systems Questionnaire - 2020
  - https://app.surveyhero.com/s/1343fc6

https://www.mangolive.com/resources

https://www.mangolive.com/blog-mango/how-to-implement-an-information-security-framework-to-meet-iso-27001

Cyber attack underway against Australian Government - Prime Minister Scott Morrison

UPDATED | 19/06/2020 | Reuters | Mark Quinlivan | Mitch McCann

ACT govt urged to improve data security after shocker audit

Agencies lacking understanding, awareness.

Jun 22 2020 1:54PM

WHO reports fivefold increase in cyber attacks, urges vigilance

23 April 2020 | News release | Geneva

New Zealand vulnerable to cyber attacks, Key says

Susan Edmunds · 10:58, Jun 27 2020

Introduction to ISO 27001

The Equation

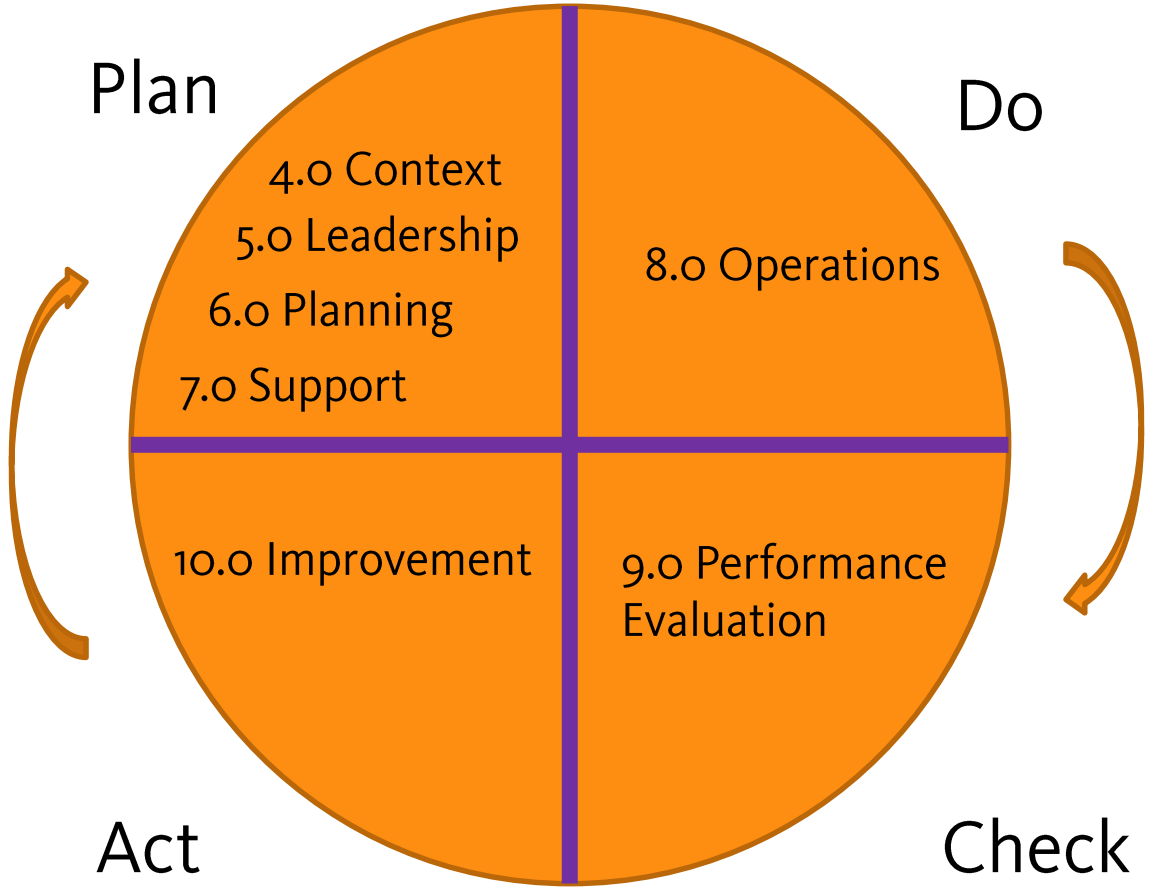
ISO 27001 = ISO 27001 + Annex A (ISO 27002)

Management System

Objectives and Controls "8.0 Operations"

ISO 27001

- ISO 27001
  - 4.0 Context
  - 5.0 Leadership
  - 6.0 Planning
  - 7.0 Support
  - 8.0 Operations
  - 9.0 Performance Evaluation
  - 10.0 Improvement
  - Annex A – ISO 27002



Annex A - ISO 27002

- Objectives and Controls
  1. A5 Information Security Policies (2 controls)
  2. A6 Organisation of Information Security (7 controls)
  3. A7 Human Resource Security (6 controls)
  4. A8 Asset Management (10 controls)
  5. A9 Access Control (14 controls)
  6. A10 Cryptography (2 controls)
  7. A11 Physical and Environmental Security (15 controls)
  8. A12 Operations Security (14 controls)
  9. A13 Communications Security (7 controls)
  10. A14 System acquisition, development and maintenance (7 controls)
  11. A15 Supplier Relationships (5 controls)
  12. A16 Information Security Incident Management (7 controls)
  13. A17 Business Continuity (4 controls)
  14. A18 Compliance (8 controls)

Implementation of ISO 27001

Step 1: Define Your Strategy for Information Security

Step 2: Create a “Statement of Applicability”

Step 3: Conduct Risk Management Methods

Step 4: Implement Controls

Step 5: Implement Management System

Step 1: Define Your Strategy for Information Security

1. To preserve the confidentiality, integrity and availability of customers' data
2. To assure customers that Mango is a well managed and professional organisation
3. To give confidence to the customer's IT Department
4. To use best practice for its information security
5. To be compliant with other standards, GDPR, POPI, Privacy Acts

Step 2: Create a “Statement of Applicability”

6.1.3 Information security risk treatment
d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;

Step 3: Conduct Risk Management Methods

1. Define the scope, context and the risk criteria
2. Ensure that staff are involved and participate.
3. Conduct the risk assessment:
    1. Risk identification
    2. Risk Analysis
    3. Risk Evaluation.
4. Determine the risk treatments.
5. Monitor and continuously review progress.
6. Make sure that it's easy to record and report risks and opportunities

Types of Information Assets

1. Digital - data stored electronically
2. Material form – paper-based, whiteboards, desks
3. Knowledge – know-how employees or contractors

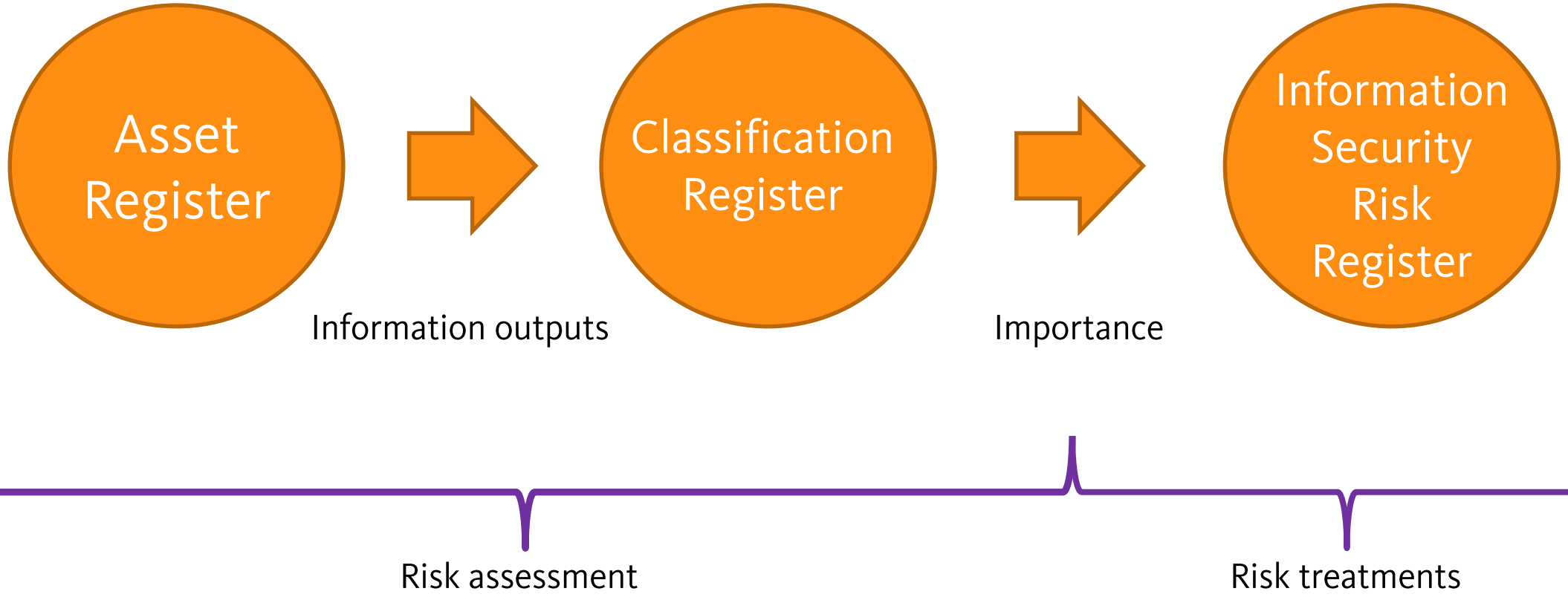
Elements of Information Security

Vulnerability	Entry to your building	Malware
Threat	Enter through windows	Email
Threat agent	Thief	Gang
Risk	Loss of computers	Shutdown
Exposure	Leave window open	Click on link
Treatment or controls	Lock windows	Filter

Common Cyber Threats

Business email compromise
Phishing
Spear phishing and whaling
Credential dumps
Insider threat
Denial-of-service
Ransomware
Data breach

https://www.cert.govt.nz/business/common-threats


Asset Register
Information outputs
Classification Register
Importance
Information Security Risk Register
Risk assessment
Risk treatments

Classification Register

Secret	Extremely sensitive and of the highest value to the organisation. Unauthorized access or disclosure would be critically damaging to the organisation. Access should be limited to a very small number of names and authorised individuals
Confidential	Sensitive and confidential within the organisation. Unauthorized access or disclosure would be critically damaging to the organisation. Access should be limited to those with a legitimate business need
Internal	Non- sensitive and used for day to day operations within the organisation. Unauthorized access or disclosure would be inconvenience but not critical. Access should be limited to workers within the company
Public	Non- sensitive and can be made publicly available. Unauthorised access or disclosure would not be an issue. Access does not need to be limited to anyone

Information Security Risk Register

- Risk Register
  - Item
  - Vulnerability
  - Harm
  - Risk Level (High, Medium, Low)
  - Controls and Actions
  - Residual Risk Level
  - Mitigations
  - Contingency Steps

Name	Vulnerability	Harm	Risk Level	Controls and Actions	Additional Controls	Re Ris

Step 4: Implement Controls

1. A5 Information Security Policies (2 controls)
2. A6 Organisation of Information Security (7 controls)
3. A7 Human Resource Security (6 controls)
4. A8 Asset Management (10 controls)
5. A9 Access Control (14 controls)
6. A10 Cryptography (2 controls)
7. A11 Physical and Environmental Security (15 controls)
8. A12 Operations Security (14 controls)
9. A13 Communications Security (7 controls)
10. A14 System acquisition, development and maintenance (7 controls)
11. A15 Supplier Relationships (5 controls)
12. A16 Information Security Incident Management (7 controls)
13. A17 Business Continuity (4 controls)
14. A18 Compliance (8 controls)

108

Step 5: Implement Management System

1. Write Your ISMS Manual
    1. Clause 4 Context of the Organisation
    2. Clause 5 Leadership
    3. Clause 6 Planning
    4. Clause 7 Support
    5. Clause 8 Operation
    6. Clause 9 Performance Evaluation
    7. Clauses 10 Improvement
2. Implement the manual
3. Conduct internal audit
4. Conduct management review

Q&A