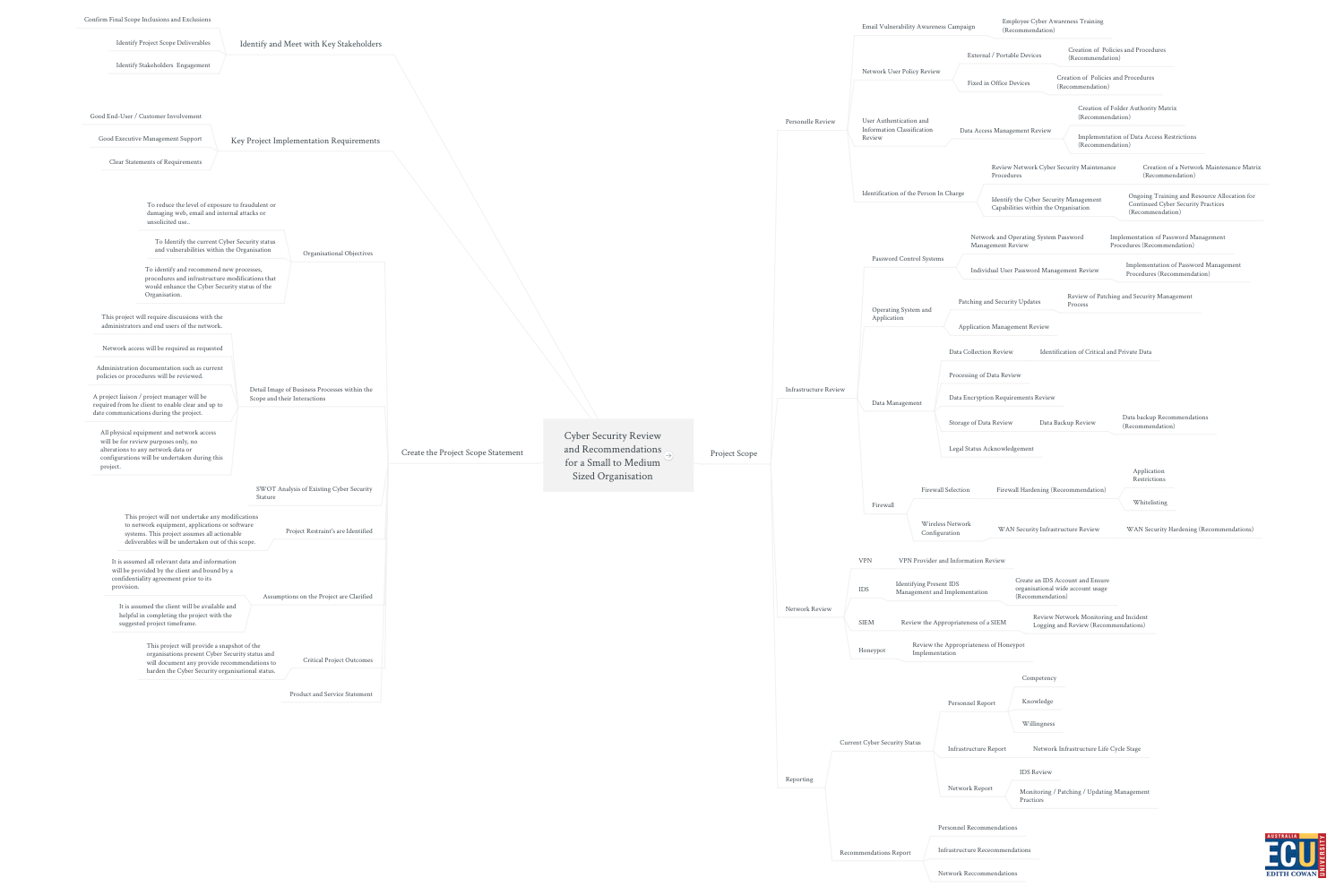


Cyber Security Review and Recommendations for a Small to Medium Sized Organisation



<https://www.mindmeister.com/1813750801>

Contents

# Project Scope

## Personelle Review

### Email Vulnerability Awareness Campaign

#### Employee Cyber Awareness Training (Recommendation)

### Network User Policy Review

#### External / Portable Devices

##### Creation of Policies and Procedures (Recommendation)

#### Fixed in Office Devices

##### Creation of Policies and Procedures (Recommendation)

### User Authentication and Information Classification Review

#### Data Access Management Review

##### Creation of Folder Authority Matrix (Recommendation)

##### Implementation of Data Access Restrictions (Recommendation)

### Identification of the Person In Charge

#### Review Network Cyber Security Maintenance Procedures

##### Creation of a Network Maintenance Matrix (Recommendation)

#### Identify the Cyber Security Management Capabilities within the Organisation

##### Ongoing Training and Resource Allocation for Continued Cyber Security Practices (Recommendation)

## Infrastructure Review

### Password Control Systems

#### Network and Operating System Password Management Review

##### Implementation of Password Management Procedures (Recommendation)

#### Individual User Password Management Review

##### Implementation of Password Management Procedures (Recommendation)

### Operating System and Application

#### Patching and Security Updates

##### Review of Patching and Security Management Process

#### Application Management Review

### Data Management

#### Data Collection Review

##### Identification of Critical and Private Data

#### Processing of Data Review

#### Data Encryption Requirements Review

#### Storage of Data Review

##### Data Backup Review

###### Data backup Recommendations (Recommendation)

#### Legal Status Acknowledgement

### Firewall

#### Firewall Selection

##### Firewall Hardening (Receommendation)

###### Application Restrictions

###### Whitelisting

#### Wireless Network Configuration

##### WAN Security Infrastructure Review

###### WAN Security Hardening (Recommendations)

## Network Review

### VPN

#### VPN Provider and Information Review

### IDS

#### Identifying Present IDS Management and Implementation

##### Create an IDS Account and Ensure organisational wide account usage (Recommendation)

### SIEM

#### Review the Appropriateness of a SIEM

##### Review Network Monitoring and Incident Logging and Review (Recommendations)

### Honeypot

#### Review the Appropriateness of Honeypot Implementation

## Reporting

### Current Cyber Security Status

#### Personnel Report

##### Competency

##### Knowledge

##### Willingness

#### Infrastructure Report

##### Network Infrastructure Life Cycle Stage

#### Network Report

##### IDS Review

##### Monitoring / Patching / Updating Management Practices

### Recommendations Report

#### Personnel Recommendations

#### Infrastructure Receommendations

#### Network Reccommendations

# Create the Project Scope Statement

## Organisational Objectives

### To reduce the level of exposure to fraudulent or damaging web, email and internal attacks or unsolicited use..

### To Identify the current Cyber Security status and vulnerabilities within the Organisation

### To identify and recommend new processes, procedures and infrastructure modifications that would enhance the Cyber Security status of the Organisation.

## Detail Image of Business Processes within the Scope and their Interactions

### This project will require discussions with the administrators and end users of the network.

### Network access will be required as requested

### Administration documentation such as current policies or procedures will be reviewed.

### A project liaison / project manager will be required from he client to enable clear and up to date communications during the project.

### All physical equipment and network access will be for review purposes only, no alterations to any network data or configurations will be undertaken during this project.

## SWOT Analysis of Existing Cyber Security Stature

## Project Restraint's are Identified

### This project will not undertake any modifications to network equipment, applications or software systems. This project assumes all actionable deliverables will be undertaken out of this scope.

## Assumptions on the Project are Clarified

### It is assumed all relevant data and information will be provided by the client and bound by a confidentiality agreement prior to its provision.

### It is assumed the client will be available and helpful in completing the project with the suggested project timeframe.

## Critical Project Outcomes

### This project will provide a snapshot of the organisations present Cyber Security status and will document any provide recommendations to harden the Cyber Security organisational status.

## Product and Service Statement

# Key Project Implementation Requirements

## Good End-User / Customer Involvement

## Good Executive Management Support

## Clear Statements of Requirements

# Identify and Meet with Key Stakeholders

## Confirm Final Scope Inclusions and Exclusions

## Identify Project Scope Deliverables

## Identify Stakeholders Engagement