CHAPTER 2
THEORETICAL FOUNDATION

2.1 Risk Assessment Frameworks Overview

This chapter discusses on some of the available frameworks and their comparison. In order to conduct risk assessment on iOS and Android mobile devices properly, a framework will be needed. The framework will assist this research by providing information on the necessary materials and the methodologies to use these materials for determining the risk level of both systems. Without using framework, it will be very difficult to determine the risk level. Listed below are the available frameworks and their general comparison [17]. Table 2.1 shows the general comparison of the frameworks.

Table 2.1 Frameworks Comparison

Framework	Comparison
ISO/IEC 13335 Set	Technical Security Controls Procedures
ISO/IEC 27000 Series	ISMS Related Processes
ISO/IEC 31000	Principles of Risk Management Implementation
NIST SP 800-16	Controls
NIST SP 800-30	Risk Assessment and Risk Mitigation Processes
NIST SP 800-39	Risk Management Framework
AS/NZS 4360	Broad Risk Management Processes (needs continuous communication with stakeholder)
OCTAVE	Intended for Organization and Requires to be Led by a Team
NIST SP 800-30 Rev1	In-Depth Risk Assessment Processes

2.1.1 ISO/IEC 13335 Set

ISO/IEC 13335 is intended to provide guidance for the IT security department management [17]. The contents of this guide are concentrated on the control procedures. It consists of four parts:

2.1.1.1 ISO/IEC 13335-1:2004

This standard is the first part of the set which explains concepts, policy and strategy principles; describes the required organizational structure in terms of protection implementation; and explains the risk management methods. [17]

2.1.1.2 ISO/IEC 13335-2

This standard is the second part of the set. It provides operational guidance on Information and Communication Technology security. [17]

2.1.1.3 ISO TR 13335-3:1998

This standard delivers direction on methods to conduct the process of risk assessment, identifies four risk analysis approaches, provides risk calculation models, and identifies the risk assessment process flow. [17]

2.1.1.4 ISO TR 13335-4:2000

This standard is the last part of the set. It provides various technical security controls to be carefully chosen. [17]

2.1.2 ISO/IEC 27000 Series

The series provides guidance that focuses on Information Security Management Systems which aims to protect the CIA of organizational assets. The guide delivers best practices to the activities related to the ISMS. [17]

2.1.2.1 ISO/IEC 27000

This standard identifies and aims to describe the essential parts for the series. It is a known fact that only few people are able to define key terms in information security accurately, therefore the value of vocabulary is important. [17]

2.1.2.2 ISO/IEC 27001:2005

In this standard, the parts that are required for an Information Security Management System are described. The ISMS is described using the Deming's Plan-Do-Check-Act cycle as presented in Figure **2.1**. [17]

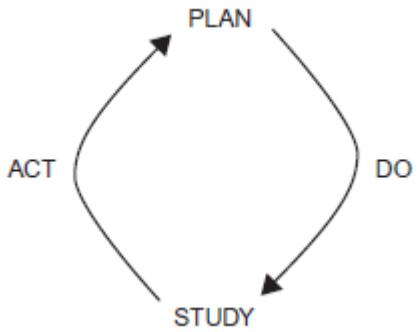

Figure 2.1 PDCA Cycle **[17]**

- Plan: involves describing the required parts, the methods that can be used to assess risks, and determining applicable controls.
- Do: comprises the methods that can be used to applying and operating the ISMS.
- Check: comprises the methods that can be used to observing and studying the ISMS.
- Act: comprises the methods that can be used to preserving and enhancing the ISMS.

Sections of ISO/IEC 27001:

- **Introduction:** describes the process approach based on the cycle.
- **Scope:** describes the requirements of ISMS that will be appropriate to be used by a variety of organizations.
- **Normative References:** ISO/IEC 27002:2005 in particular.

- **Terms and Definitions:** self-explanatory.
- **Information Security Management System:** describes the core of the ISO/IEC 27001 based on the cycle.
- **Management Responsibility:** describes the necessity of management to prove their commitment to the ISMS.
- **Internal ISMS Audits:** focuses on the necessity of internal audits to make sure that the ISMS use satisfactory controls.
- **Management Reviews of the ISMS:** focuses on the review of effectiveness of the ISMS that is needed to be done frequently.
- **ISMS Improvements:** focuses on the improvement of ISMS by conducting assessment and implementing changes to the ISMS.

2.1.2.3 ISO/IEC 27002:2005

This standard focuses on the security of information assets. In order to identify information security risk exposures, this standard describes a set of 133 controls under 39 security objectives. [17]

Contents of ISO/IEC 27002:

- **Introduction.** Contains description on the usage of the standard.
- **Scope.** Contains the description of the scope that covers information security management recommendations.
- **Terms and Definitions**

- **Structure and Standard.** Contains the information about the core of the standard that includes control objectives, recommended controls, and guide for implementation.
- **Risk Assessment and Treatment.** Contains the risk management.
- **Security Policy.** Covers the necessity of security policy in organizations.
- **Organization of Information Security.** Covers the necessity to design and apply information security.
- **Asset Management.** Covers the necessity for organization to recognize every asset that the company has.
- **Human Resources Security.** Covers the necessity for organization to have the control of their employees' privileges.
- **Physical and Environment Security.** Covers the necessity to defend the organizational assets physically.
- **Communications and Operations Management.** Covers the needed controls for network related operations.
- **Access Control.** Covers the necessity of managing access in IT systems.
- **Information Systems Acquisition, Development, and Maintenance.** Covers the necessity to protect every activity that is related to IT systems.

- **Information Security Incident Management.** Covers the necessity for quick response and reports of every event.
- **Business Continuity Management.** Covers the necessity to analyze and plan activities related to business continuity.
- **Compliance.** Covers the necessity to understanding every compliance concerns.

2.1.2.4 ISO/IEC 27003

This standard is intended to deliver guide to implement ISO/IEC 27001 standard. The key sections of this standard include acquire agreement to implement the ISMS, define ISMS scope and procedure, analyze business, assess the risks, design the ISMS, and implement the ISMS. [17]

2.1.2.5 ISO/IEC 27004

This standard is intended to cover the measurements of information security management. It provides input regarding the way to determine and notify the value of ISMS. It comprises the processes of security management from ISO/IEC 27001 and the controls from ISO/IEC 27002. Organizations may use this standard to create a base in perform activities associated to ISMS data processing. [17]

2.1.2.6 ISO/IEC 27005:2008

This standard acts as guidance for risk management. It is designed to give assistance on the implementation of information security. It also provides recommendations to choose and use risk assessment methods without the necessity of identifying any particular risk analysis method. [17]

2.1.3 ISO/IEC 31000

This standard is intended to provide guidance on the principles related to the risk management implementation [17]. In this standard, it is mentioned that to be more competent, a risk management should stick to these principles:

- It should create value.
- It should be a fundamental measure of organizational procedures.
- It should be a part of decision-making.
- It should clearly state ambiguity.
- It should be systematic and organized.
- It should be based on the best accessible data.
- It should be tailored.
- It should take human influences into consideration.
- It should be comprehensive and transparent.
- It should be dynamic, iterative, and reactive to modification.
- It should be capable of repetitive enhancement and improvement.

2.1.4 NIST SP 800-16

This standard focuses specifically on controls in which it covers:

- Management Controls
    - Policies and processes of the system
    - Standard operating processes
    - Personnel security
    - System rules of behavior
    - Individual accountability
    - IT security awareness and drill
    - User accountabilities for unfitting activities of others

- Acquisition/Development/Installation/Implementation Controls
    - Stages and functions of the system life-cycle
    - IT security necessities in system life-cycle stages
    - Official system security strategy
    - Correlation of configuration and modification management programs to IT security objectives
    - Testing system security controls and certification
    - Senior manager agreement for operation

- Operational Controls
    - Physical and environmental security

  - Marking, handling, shipping, storing, cleaning, and clearing
  - Contingency planning

- Technical Controls
  - How technical controls aid management controls
  - How system controls may tolerate positive association of activities to individuals
  - Identifying attacks
  - User activities to prevent loss
  - Role of cryptography in securing data

This standard provides responsibilities that risk management personnel have. They are divided for three different tiers: junior staff, intermediate staff, and advanced staff where each of the tiers have different responsibilities. [17]

2.1.5 NIST SP 800-30

This standard covers a summary of risk management, the relation with SDLC, and roles of the workforces that aid and use this procedure. It explains the methods of risk assessment and nine steps to conduct the assessment for a system. This standard also includes the risk mitigation processes. This standard is intended to be used by various IT personnel in an organization or individuals that are related to IT systems. [17]

Nine primary steps of the risk assessment:

- Step 1: System Characterization
- Step 2: Threat Identification
- Step 3: Vulnerability Identification
- Step 4: Control Analysis
- Step 5: Likelihood Determination
- Step 6: Impact Analysis
- Step 7: Risk Determination
- Step 8: Control Recommendations
- Step 9: Results Documentation

2.1.6 NIST SP 800-30 rev1

This standard is a revision of NIST SP 800-30 in which it no longer includes the risk mitigation process and now focuses only on the risk assessment part [18]. It has been significantly stretched out to provide more in-depth material with various risk factors that are required to determine information security risks. This standard has three steps of risk assessment processes. Figure 2.2 shows the overview of the processes.

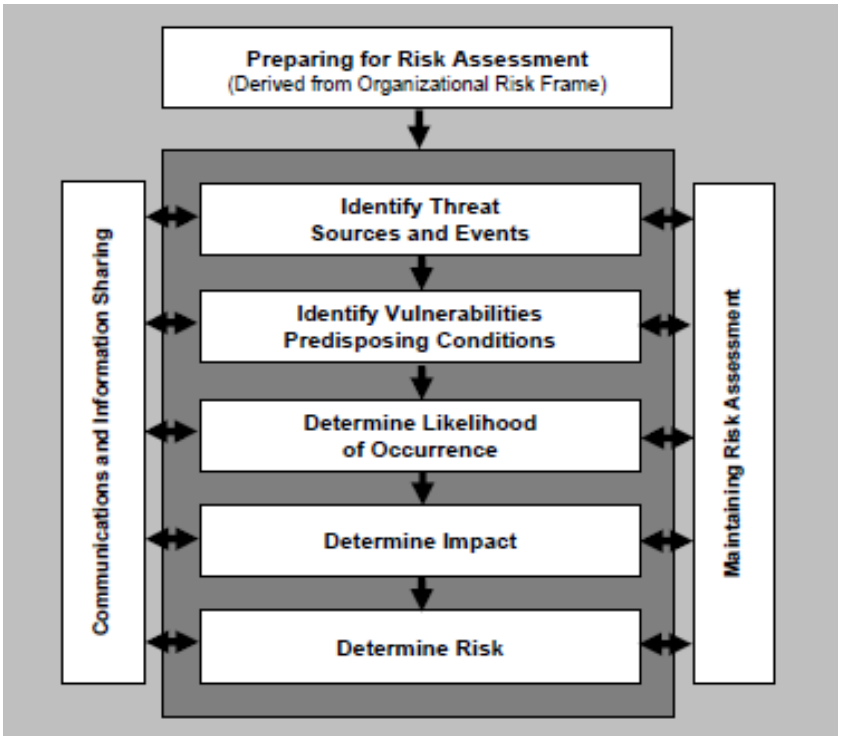

Figure 2.2 Risk Assessment Steps [18]

- **Preparing for the risk assessment**. It includes identification of purpose, scope, assumptions and constraints, and information sources, as well as defining the risk model.
- **Conducting the risk assessment**. It includes identification of threat sources, threat events, vulnerabilities and predisposing conditions, as well as determination of likelihood, impact, and risk.
- **Maintaining the risk assessment**. It includes monitoring risk factors and updating the risk assessment.

2.1.7 NIST SP 800-39

This standard describes a risk management framework which includes information systems classification with concern to business influences, security controls selection and documentation, controls implementation and assessment, the authorization for supporting framework and corporate risk acceptance, and information systems and operational environments security state monitoring. Figure 2.3 shows the six steps of the risk management framework. [17]

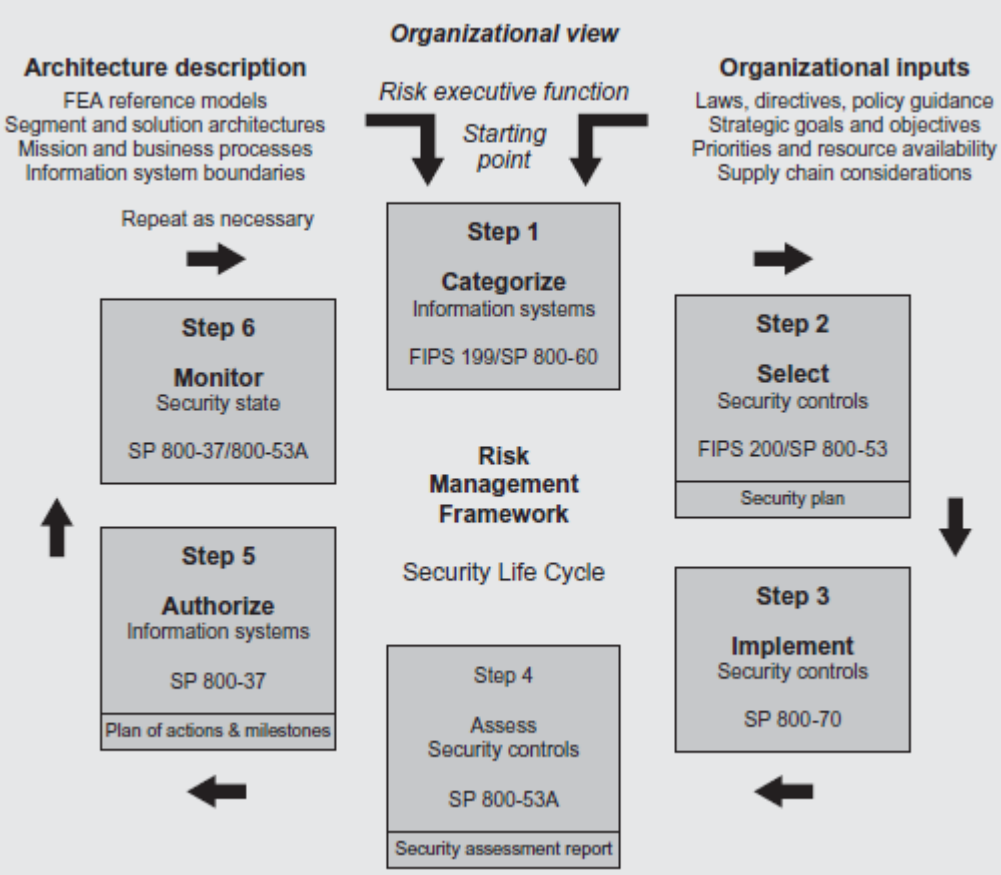

Figure 2.3 Risk Management Framework [17]

2.1.8 AS/NZS 4360

This standard delivers guidelines to establish and implement risk management processes. The processes include identification, analysis, assessment, treatment, and continuous risk monitoring. This standard also needs continuous consultation with stakeholders. Figure 2.4 shows the processes of the risk management used in this standard. [17]

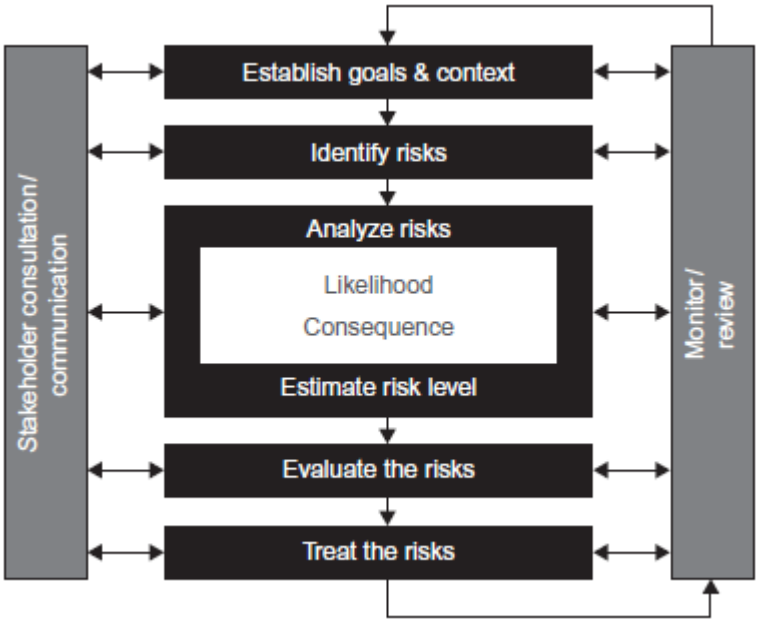

Figure 2.4 Risk Management Processes [17]

2.1.9 OCTAVE

It is a set of methodologies that can be used to plan and evaluate data protection. It has three approaches: [17]

- Original OCTAVE process which is the center of it.
- OCTAVE-S is good for smaller organizations.
- OCTAVE-Allegro is a methodology to evaluate data protection.

OCTAVE is self-directed, flexible, and evolved. It focuses on the identification of crucial assets their specific threats. It obliges that an assessment must be directed and executed by a team of a company. It is based on a set of principles that requires catalog of practices, generic threat profile, and catalog of vulnerabilities.

OCTAVE is divided into eighteen volumes of guidance: Introduction, Preliminary Activities, the OCTAVE Process (volume 3-12), After the Evaluation, Bibliography and Glossary, Appendices (volume 15-18).

In OCTAVE, it is stated that to have a successful evaluation, there are some keys: senior management sponsorship acquisition, analysis team selection, OCTAVE scope, and participant selection.

OCTAVE uses three phases approach: asset-based threat profiles construction, infrastructure vulnerabilities identification, security strategy and plans development. [17]

2.2 Choosing the most Suitable Framework

There are some criteria that are used to compare the frameworks. For this research, the author needs to choose a framework that:

- Can be used for both organizations and individual users
- Focuses solely on the risk assessment processes to determine the level of risk
- Provides comprehensive and clear methodologies

The 13335 set concentrates on technical security controls procedures which is not suitable since this research requires a framework that focuses on risk assessment. The 27000 series focuses too much on the management and business side related to ISMS instead of risk assessment methodologies which will not be good to be used in this research. ISO 31000 provides guidance on risk management broadly which is not suitable because this research requires a framework concentrating on the risk assessment itself.

NIST SP 800-16 focuses heavily on the controls side without enough information on risk assessment which is not a framework that is needed in this research. NIST SP 800-39 is similar with ISO 27001 which focuses more on the management side which. AS 4360 also provides risk identification, analysis, estimation, evaluation, and treatment. However, this standard needs continuous communications with stakeholders which will be better used for business instead of individuals.

OCTAVE is intended to be used by organizations and requires to be led by a team which is not suitable for this research because the goal is intended for both organizations and individuals. NIST SP 800-30 is a very good framework and suitable for this research. However, the newer version, NIST SP 800-30 Rev1, provides much more in depth processes to conduct the risk assessment.

The most appropriate framework to be used in this research is NIST SP 800-30 Rev1. It provides a comprehensive guide to conduct risk assessment thoroughly. It provides clear step by step methodologies to be studied and used. It also provides comprehensive figures and tables to ensure that the assessment is conducted more accurately. It is also the most relevant framework to this

research because it only focuses on risk assessment, which is the main process that is crucial for determining the risks iOS and Android pose. Furthermore, this framework can be used for both organization and individual users.