Development Team Project

A Status Report Document for an Information Risk Management (IRM) Report

MSc Cyber Security

Information Risk Management, Unit 3 Submission

Words 646

## 

[**Introduction**](#_heading=h.60iug66i4rxk) **2**

[**Assessment Scope & Assumptions**](#_heading=h.5vq7aae89cb1) **2**

[Functional requirements](#_heading=h.qekaechi7350) 2

[Non-Functional requirements](#_heading=h.40k6fytsj0o0) 2

[**Assessment Approach**](#_heading=h.fxvhhjd8rvou) **2**

[Stage 1: Establish a Risk Management Framework](#_heading=h.ife93cew2lwe) 3

[Stage 2: Identify Risks](#_heading=h.ti0narr8yzz4) 3

[Stage 3: Analyse Risks](#_heading=h.ic9hsd4g490c) 3

[Stage 4: Evaluate Risks](#_heading=h.yff7z3mqz3of) 3

[Stage 5: Risk Treatment](#_heading=h.xinwte2v5w4q) 3

[**Conclusion**](#_heading=h.rsn29k480cnp) **3**

[**References**](#_heading=h.kcs2n1b4psoa) **4**

## 

## Introduction

This document provides an overview of the planned risk assessment for ACME manufacturing; considering the three potential solutions for a new Enterprise Resource Planning (ERP) system. This document outlines the requirements and approach for the risk assessment and any potential business challenges and assumptions.

## Assessment Scope & Assumptions

The scope of the risk assessment will be the ERP, taking into consideration the function and non-functional requirements listed by ACME:

### Functional requirements

* ERP platform for 150 staff.
* Flexibility to manage changes in supply chain and production demand.

### Non-Functional requirements

* RPO of 15 mins.
* RTO of 4 hours.

It is assumed that the ERP system is integral to a wide range of operational activities, and therefore, migration will be high risk (Oracle, N.D.; Fruhlinger et al., 2020). However, it is clear that the existing system of managing these processes via spreadsheets presents a risk of failure regarding scalability. Based on the diversity of an ERP system, the risk to data assets will be considered, including intellectual property and personal data.

Based on the industry and size of the business, it is assumed that there is a limited budget available for security and a limited number of staff to support such initiatives (DCMS, 2019). Although no risk appetite has been clearly outlined, the assessment will be completed in line with industry best practice, prioritising risks that contravene legal, regulatory, and mandatory requirements within the industry, including the GDPR.

## Assessment Approach

Sections of the ISO27000 series of standards will be followed for this assessment as it covers both information security practices and business continuity. These are well-documented standards that fall in line with European standards, such as GDPR, and ISO27001 accreditation could be pursued to provide a commercial advantage to ACME.

Risk scores will be calculated by multiplying the likelihood and impact scores (Sutton, 2014). A semi-quantitative approach will be taken to determine the scores for impact and likelihood through clearly defining quantitative thresholds for each score from 1 to 5. Whilst likelihood will have frequency-based thresholds, the impact will consider thresholds across different types of impact, such as technical, financial, and reputational. Whilst a quantitative approach to risk is often favoured, this approach to scoring will promote consistency in the absence of historical quantitative data which is often scarce and expensive (Hubbard, 2009).

The assessment is split into five stages (Irwin, L., 2021).

### Stage 1: Establish a Risk Management Framework

The chosen framework is a scenario-based risk assessment. This is ideal as it can be quicker than an asset-based assessment which is necessary under time restrictions (Leal, 2019).

### Stage 2: Identify Risks

Each review will ask the same questions to identify risks to ensure this has been conducted fairly. Risks will be identified in relation to the CIA triangle of Confidentiality, Integrity and Availability (Fruhlinger, 2020).

### Stage 3: Analyse Risks

This includes documenting a risk statement for each identified risk. This will provide insight into how a threat could impact risk or vulnerability.

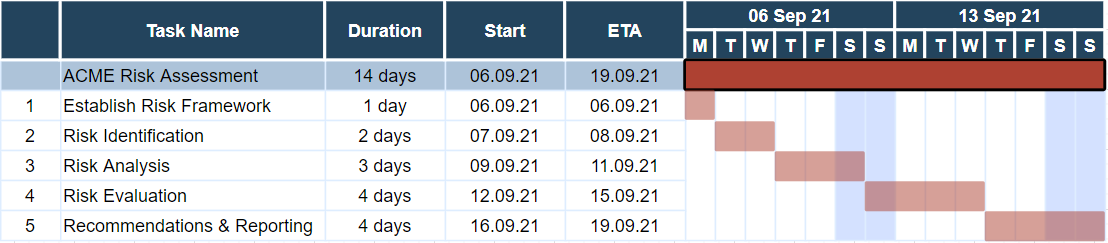
### Stage 4: Evaluate Risks

The evaluation of risks will be conducted using a 5x5 risk matrix (Stoneburner et al., 2002). This evaluation is based on the likelihood of that risk being exploited and its impact if it occurred.

### Stage 5: Risk Treatment

As part of this stage, risk treatment will also be documented based on cost and effort. This will impact again which solution is chosen as the most ideal.

Each stage will be completed within a particular time frame, as documented in the Gantt Chart below:

**

## Conclusion

This document provides an overview of the risk assessment for a new ERP solution for the ACME organisation, including any potential challenges faced, scope and requirements. Also included is a breakdown of the proposed approach taken and timelines for each stage. As a result of this assessment, a recommendation will be made out of the three options ACME has chosen, as well as a disaster recovery solution.

## References

Department for Digital, Culture, Media, and Sport (DCMS) (2019) Cyber Security Breaches Survey. Available from:<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950063/Cyber_Security_Breaches_Survey_2019_-_Main_Report_-_revised_V2.pdf> [Accessed 27 August 2021].

Fruhlinger, J. (2020) The CIA triad: Definition, components and examples. Available from: <https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html> [Accessed 21 August 2021].

Fruhlinger, J., Wailgum, T. & Sayer, P. (2020) 16 famous ERP disasters, dustups and disappointments. Available from:<https://www.cio.com/article/2429865/enterprise-resource-planning-10-famous-erp-disasters-dustups-and-disappointments.html> [Accessed 27 August 2021].

Hubbard, D. (2009) *The Failure of Risk Management: Why It's Broken and How to Fix It.* 2nd Ed. Wiley.

Irwin, L. (2021) 5 steps to an effective ISO27001 risk assessment. Available from: <https://www.itgovernance.eu/blog/en/what-is-an-iso-27001-risk-assessment-and-how-should-you-report-on-it> [Accessed 19 August 2021].

Leal, R. (2019) Scenario Based Risk Assessment. Available from: <https://community.advisera.com/topic/scenario-based-risk-assessment/> [Accessed 21 August 2021].

Oracle (N.D.) What is ERP? Available from:<https://www.oracle.com/uk/erp/what-is-erp/> [Accessed 27 August 2021].

Stoneburner, G., Goguen, A. & Feringa, A. (2002) *SP 800-30: Risk Management Guide for Information Technology Systems.* Gaithersburg, MD, USA: National Institute of Standards & Technology.

Sutton, D. (2014) *Information Risk Management.* 1st ed. Swindon, UK: BCS Learning & Development Limited.