Risk Management Report
For
HMP Prison, Doncaster, UK

ACME AG

Table of Contents

List of Tables

Table of Figures

1.INTRODUCTION

The purpose of this document is to build an Information Risk Management Report for the HMP Beechnut Prison, Doncaster, UK. The prison is already built, commissioned and contracted to ACME AG Prison Service to operate for 25 years with further scope to innovate using the latest technology innovations. Therefore, the key considerations in this report include: the policies, the controls and the standards of using technology that need to be adopted to reduce the associated threats, vulnerabilities and consequences.

Introduction of technology no doubt will enhance efficiency and effectiveness but also opens up a wide range of possible threats that can occur to the information assets in the prison system. Recently there have been increase in Cyber-attacks, DoS attacks, Ransomware, Data breaches and malicious incidents (Ncsc.gov.uk, 2019). With the internet in prison cells, the prisoners can transmit sensitive information from prison, therefore the database needs to be secure and encrypted to protect confidential information from prison and the drones can be used for wrong reasons to deliver drugs and sims for contacting others for prison escape and so on. Lack of awareness and preparedness is the basic factor in IT risk management. The six best practices of IT risk management are Security, Availability, Recoverability, Performance, Scalability and Compliance (HUGHES, G., 2006).

In this report hybrid ISO 31000 process is used as the risk management framework as it is internationally recognised and is concise and easy to use. The ISO 27001 is used for implementing controls and NIST SP 800-61 is used for Incident Response standards. The tool used for threat modelling is STRIDE and Elevation of Privilege game (Shostack, 2014) along with additional threats related to the given scenario.

This report is divided into four sections- The Context, Risk Assessment, Risk Mitigation and Incident response.

2.CONTEXT

This section discusses the context and purpose of the project.

2.1 Objectives

The main objective of the ACME AG is to continue to innovate the prison sector by using technology. It plans to show how well a prison can be managed with the help of technology and it aims at showcasing it by operating the new prison in the 25 years contract and taking it to new heights in terms of performance, efficiency and operation with the help of technological innovations. As prison is already built and commissioned the current aim is to make a risk management report to address the potential security issues and concerns of key innovations and technology as shown in Table 1 below:

Table 1:Objectives and Innovation of Prison

Innovation	Objective
Internet Connection	To provide Internet connectivity for individual prisoners.
Virtual Visits	To Introduce Virtual visits to allow prisoners to meet their families in video conferencing.
Local Database	To build a Prison local database of prisoner information and make it accessible by both internal and external stakeholders.
Resist Drones	To resist the illegal use of drone technology and to avoid drones delivering drugs and sims.

2.2 Context Modelling of the prison System

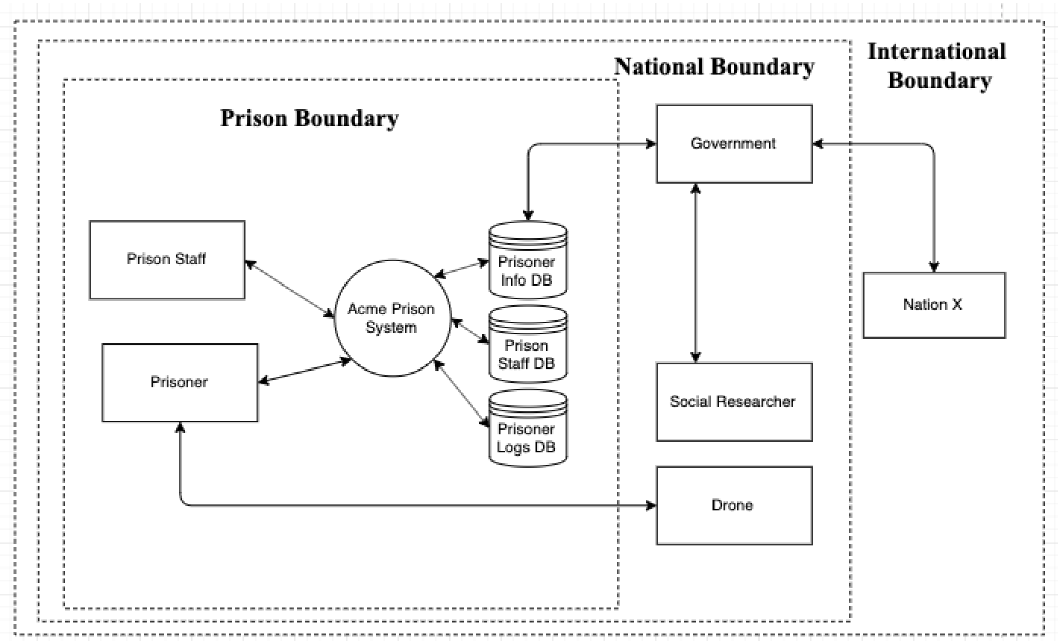
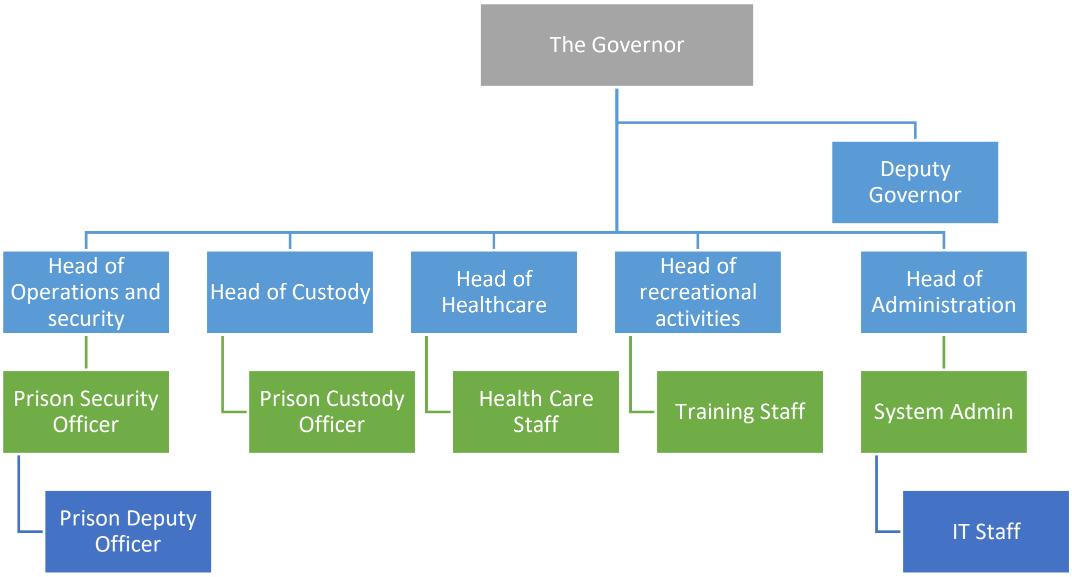


Figure 1 Context diagram of the Acme Prison and its Environment, Boundaries and the System

Figure 1 shows the context / Level 0 DFD for the given scenario. Appendix A has the DFD notation used for the given scenario. There are three boundaries in the system which are Prison Boundary, National Boundary and the International Boundary. In Prison, there are 1200 prison cells one for each prisoner. The entities in the prison are Prisoner and the Prison staff and there is one process which is Acme Prison System for accessing the internet and video conferencing. There are 3 Databases which are: 1) Prisoner Database will contain all the prisoner information, 2) Prison staff Database will store the staff details and 3) Prisoner Logs Database will hold all the logs taking place in the Acme prison system. Based on the given scenario in the National Boundary there are 3 entities which are Government, Social Researcher and Drone. In the International Boundary, there is Nation X is the only entity and it has a tie-up with the government to access the prisoner information.

2.3 The Prison Management (Hse.gov.uk, 2019)



Roles and Responsibilities of the Management are discussed in Appendix B.

2.4 Assumptions

The Assumptions made are as follows:

1 There are policies existing for physical and environmental security in the prison.

2 There are policies existing for segregation of duties in the prison.

3 There are policies existing for usage of mobile devices and teleworking in the prison.

4 There are policies existing for Human resource security in the prison.

5 There are policies existing for supplier relationships in the prison.

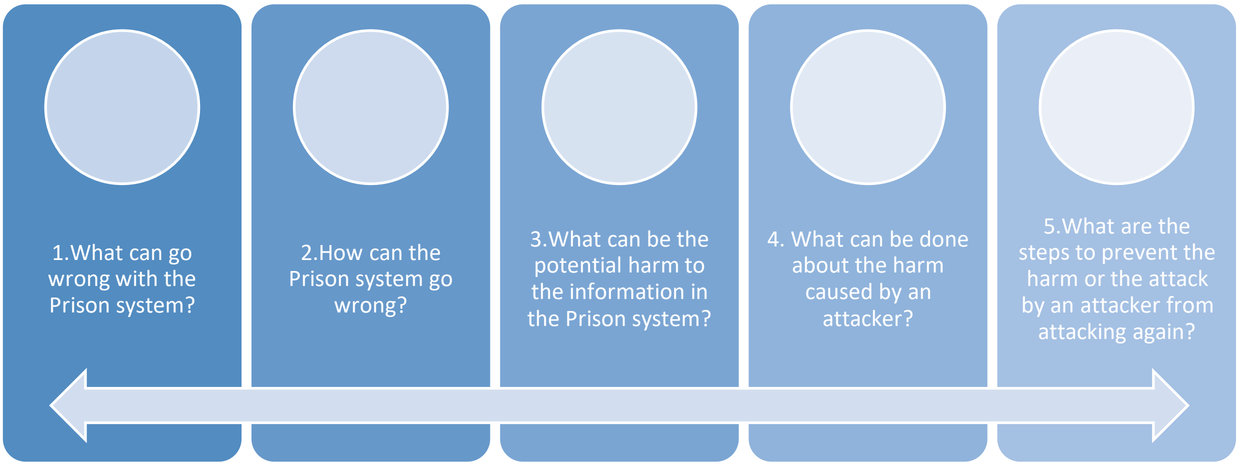
6 The Prisoner information can be accessed only by government and government will be responsible for sharing the data with the social researcher and Nation X

7 Database of the prison will be implemented locally as there are risks involved in making it cloud based.

3.RISK ASSESSMENT

This section discusses about the Risk Identification tools, Risk analysis of the prison, Risk evaluation using likelihood and impact, Risk responsibility and Risk response for the given prison scenario.

Risk assessment typically deals with 5 questions (Wpc.0064.edgecastcdn.net, 2019) which are as follows:



1.What can go wrong with the Prison system?

2.How can the Prison system go wrong?

3.What can be the potential harm to the information in the Prison system?

4. What can be done about the harm caused by an attacker?

5.What are the steps to prevent the harm or the attack by an attacker from attacking again?

Considering some of the available Threat Modelling Tools (Resources.sei.cmu.edu, 2019):

i. STRIDE threat model can be easily to adapted to any system as it has properties which are exactly opposite to the CIA triad which has confidentiality, integrity and availability, identify the mitigation techniques and is one of the most mature models but it can be time-consuming when the system starts increasing in size and complexity.

ii. PASTA is a risk-centric threat model it is good for implementing business and technical objectives together with rich documentation, but it involves many tasks and so is laborious.

iii. CVSS has automated components and can give consistent results but score calculations are not transparent.

iv. Attack trees are very easy to build upon for threat modelling, but they are useful only when the person modelling the system has a thorough understanding of the complete system.

v. Security cards involve stakeholders and help in identifying some extraordinary threats but can lead to false positives.

3.1 Risk Identification

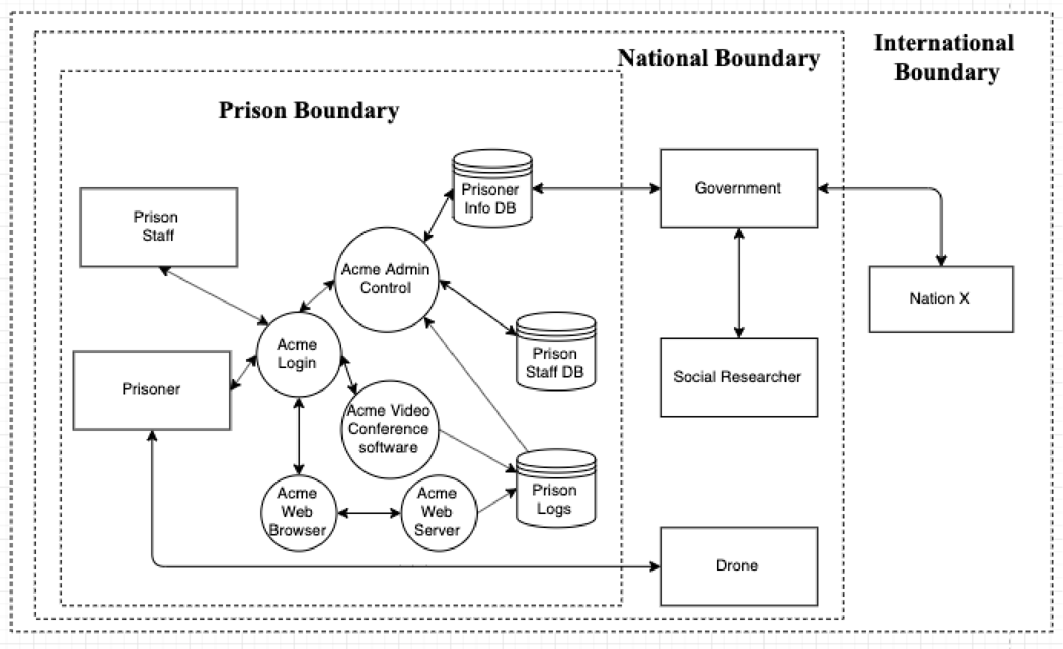


Figure 2 Level 1 DFD For Acme Prison System

It can be seen in Figure 2 that the processes in the Acme prison system are further divided into more processes such as Acme Login for authenticating the user whether they are a prison/System administrator. The prisoner can login for accessing the web browser and Acme Video conference software. The prison staff can login for performing Admin controls. Table 2 shows the identified prison assets in Level 1 DFD.

Table 2 Prison Assets

Asset	Asset Type	Prison Example
Asset 1:	Processes	Acme login, Acme web server
Asset 2:	Data	Prisoner information DB, Prisoner log, Prisoner/staff Login details, Prison staff DB
Asset 3:	Software	Acme Prison software
Asset 4:	Hardware	Prison computers, Prison server
Asset 5:	Network	Servers and Security Systems

3.2 Risk Analysis

This includes threats and vulnerabilities as detailed below:

Table 3 List of Threats and their Vulnerabilities (Shostack, 2014):

Threat Type	Threats	Vulnerability
Spoofing: Violation of Authentication	T01: Prisoner can perform squatting attack on the ports/sockets of the server.	There is no Access control list implemented.
	T02: Prisoner can use brute force attack for gaining access to the network as staff.	There is no strong Encryption of network security
	T03: Prisoner can perform a spoofing attack to spoof a server.	The prisoner was able to gain the networks IP address.
	T04: Prisoner can steal staff credentials using a spoofed authentication website.	The server is not strongly encrypted. There is no encryption for the credentials stored in rest/motion.
	T05: Prisoner can use cookies stored on the web browser.	There is no proper policy for storing the cookies implemented on the web browser.
	T06: Prisoner can access the prison system through default staff password.	The staff did not change the system's default password.
Tampering: Violation of Integrity	T07: Prisoner can use the previous conversation data and replay it.	There are no Time stamps/ sequence numbers in the code for data.
	T08: Prisoner can write information into the Database	There is no Access control List implemented.
	T09: Prisoner can tamper data in the network.	There is no integrity protection for data on the prison network.

	T10: Prisoner can control the state of information.	System relies on URL parameter or something an attacker can manipulate.
	T11: Prisoner can load code inside a process of the prison system through an extension point.	There is no integrity protection for data on the prison network.
Repudiation: Violation of Non-Repudiation	T12: Prisoner can read security information in the Logs.	Logs are not encrypted.
	T13: Prisoner can alter the Digital Signature.	The used Digital Signature was weak
	T14: Prisoner can alter the log messages on a network.	There are no integrity controls implemented on the network
	T15: Prisoner can create log entry without timestamp.	There is no Access control List implemented.
	T16: Prisoner can edit the Logs without proof.	There is no Heartbeat option implemented.
	T17: Prisoner deletes the log file	There was no proper ACL implemented
Information Disclosure: Violation of Confidentiality	T18: Prisoner can view the system error messages with security sensitive content.	The security sensitive content in logs is not encrypted.
	T19: Prisoner can read messages even when the channel is encrypted.	There is no encryption for the message in the channel.
	T20: Prisoner can perform MITM attack.	Endpoints are not authenticated in the network.
	T21: Prisoner can access information through search indexer or a logger	There Should be limited access what the search indexer can search based on the user privilege.

	T22: Prisoner can read confidential information in a file.	There is no proper ACL implemented in the system
Denial of Service: Violation of Availability	T23: Prisoner can disrupt the availability of the authentication system	There is account lockout mechanism implemented to avoid Brute force attacks.
	T24: Prisoner can disrupt the availability of the Prison system software (client) for temporary/ persistent amount of time.	There is no network hardware configuration for stopping against DoS attacks.
	T25: Prisoner can disrupt the availability of the Prison Server for temporary/persistent amount of time.	There is no network hardware configuration for stopping against Dos attacks.
	T26: Prisoner can disrupt the bandwidth of the network	There is no extra bandwidth for handling the network.
	T27: Prisoner can disrupt the availability of the Video conferencing software	There is no network hardware configuration for stopping against Dos attacks.
Elevation of Privilege: Violation of Authorization	T28: Prisoner can use the unnecessary permissions taken by frameworks.	Taking user permissions which are not needed.
	T29: Prisoner can use cross site scripting	There is no proper input and output validation implemented.
Other threats	T30: Drone can deliver Sim / drugs	There is no proper Anti-drone technology implemented.

	T31: Prisoner can perform malware attack on the prison systems.	There are outdated software and no proper antivirus and anti-malware solutions.
	T32: Disgruntled employee can disrupt the prison system	There are no proper insider threats counter measures.

3.3 Risk Evaluation: (Owasp.org, 2019)

Table 4 below has been used for scaling the likelihood and Impact the risk into Low, Medium and High

Table 4 Scale for Likelihood and Impact

Likelihood and Impact Levels	
0-3.5	LOW
3-6	MEDIUM
6-9	HIGH

The scores have been assigned based on Appendix C. The overall likelihood in the Table 5 has been calculated as average scores of Threat agent factors and Vulnerability factors.

Table 5 Factors for Estimating Likelihood

Factors for Estimating Likelihood									
	Threat Agent Factors				Vulnerability Factors				
Threat ID	Skill Level	Motive	Opportunity	Size	Ease of Discovery	Ease of Exploit	Awareness	Intrusion Detection	Overall Likelihood
T01	6	4	4	4	7	5	4	1	4.37
T02	6	9	9	6	7	9	6	1	6.62
T03	6	4	7	6	3	9	6	1	5.25
T04	6	9	4	4	3	5	6	8	5.62

T05	6	9	7	6	7	5	6	3	6.12
T06	6	4	7	4	1	1	1	1	3.3
T07	6	4	4	4	7	5	4	1	4.37
T08	6	4	7	4	1	1	1	3	3.3
T09	6	4	7	6	3	3	4	1	4.25
T10	6	4	7	6	3	9	4	9	6
T11	6	4	7	6	3	9	6	8	6.12
T12	6	4	7	6	1	9	4	8	5.62
T13	6	4	7	6	3	9	1	8	5.5
T14	6	4	7	6	3	9	6	1	5.25
T15	6	4	7	4	1	1	1	3	3.375
T16	6	4	7	4	1	1	1	3	3.37
T17	6	4	7	4	1	1	1	3	3.37
T18	6	4	7	6	3	9	6	1	5.25
T19	6	9	9	6	7	5	6	3	6.3
T20	6	9	9	6	7	9	6	1	6.6
T21	6	4	7	6	3	9	6	1	5.25
T22	6	4	7	6	3	9	6	1	5.25
T23	6	9	9	6	7	5	6	3	6.625
T24	6	4	7	6	3	9	6	1	5.2
T25	6	9	9	6	7	9	6	1	6.625
T26	6	9	9	6	7	9	6	1	6.625
T27	6	4	7	4	1	1	1	3	3.3
T28	6	9	9	6	7	9	6	1	6.625
T29	6	4	7	6	3	9	6	1	5.25
T30	6	9	9	6	7	9	6	1	6.62
T31	6	9	9	6	7	5	6	3	6.3
T32	6	9	9	6	7	9	6	1	6.6

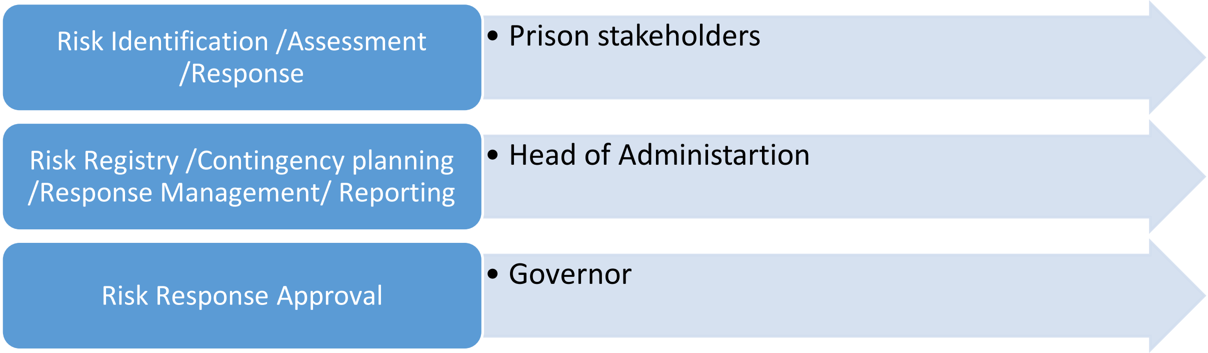
The scores have been assigned based on score categories in Appendix C. The Overall impact in the Table 6 has been calculated as average scores of Technical Impact Factors.

Table 6 Factors for Estimating Impact

Factors for Estimating Impact					
	Technical Impact Factors				
Threat ID	**Loss of Confidentiality**	**Loss of Integrity**	**Loss of Availability**	**Loss of Accountability**	**Overall Impact**
T01	7	1	1	7	4
T02	9	9	9	7	8.5
T03	7	7	1	7	5.5
T04	9	7	9	9	8.5
T05	9	7	9	9	8.5
T06	2	1	1	9	3.25
T07	7	7	1	7	5.5
T08	2	9	1	1	3.25
T09	9	9	1	7	6.5
T10	7	9	7	7	7.5
T11	9	9	7	7	8
T12	9	1	1	7	4.5
T13	9	9	1	7	6.5
T14	9	9	1	7	6.5
T15	7	9	1	7	6.0
T16	9	9	1	7	6.5
T17	9	9	1	7	6.5
T18	9	1	1	7	4.5
T19	9	1	1	7	4.5
T20	9	9	1	7	6.5

T21	9	1	1	7	4.5
T22	9	1	1	7	4.5
T23	1	1	9	7	4.5
T24	1	1	9	7	4.5
T25	1	1	9	7	4.5
T26	1	1	9	7	4.5
T27	1	1	9	7	4.5
T28	9	9	9	7	8.5
T29	9	9	1	7	6.5
T30	7	7	1	7	5.5
T31	9	9	9	7	8.5
T32	9	9	9	7	8.5

3.4 Risk Responsibilities



Risk Identification /Assessment /Response

- Prison stakeholders

Risk Registry /Contingency planning /Response Management/ Reporting

- Head of Administartion

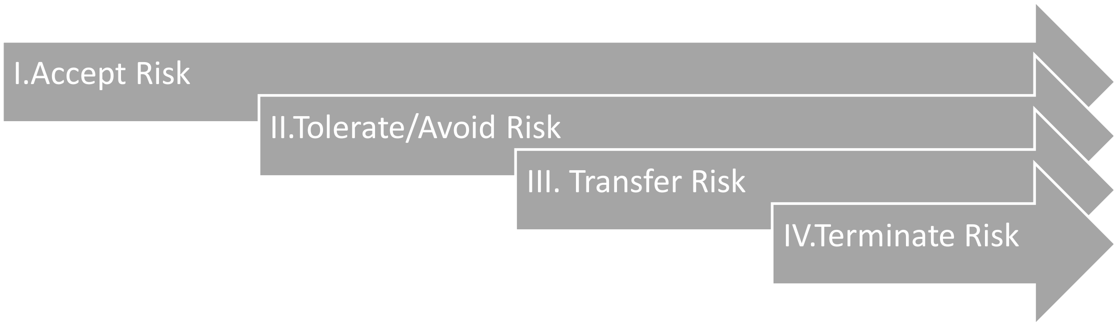
Risk Response Approval

- Governor

Appendix D has the Risk owners for each of the identified risks along with risk treatment due.

4. RISK MITIGATION

This subsection discusses about the mitigation strategies the organizational policies, Recommended controls and the Recommended standards for the given prison scenario. According to the ISO/IEC 27001 there are four ways for treatment of Risk which are as follows:



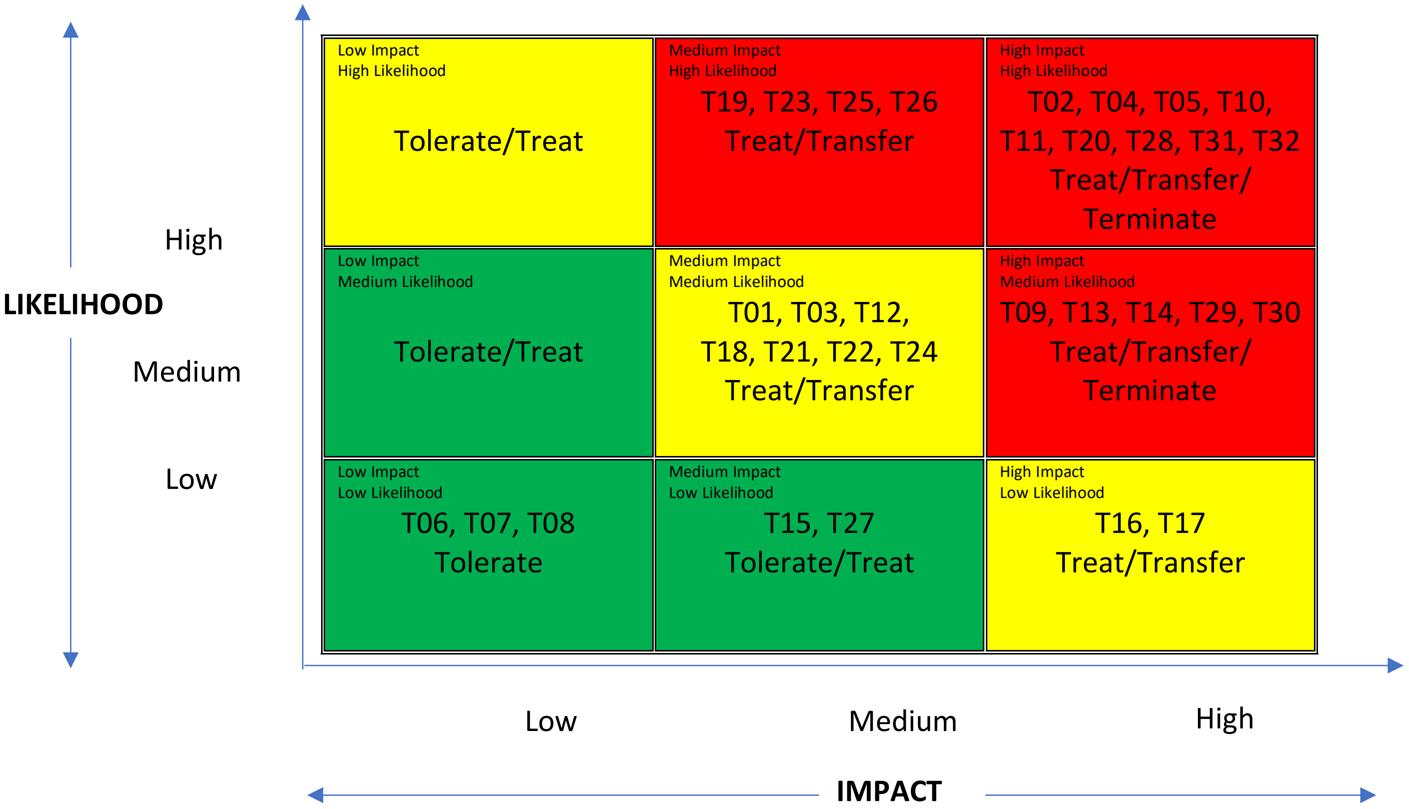
I.Accept Risk

II.Tolerate/Avoid Risk

III. Transfer Risk

IV.Terminate Risk

Risk Assessment Matrix:



LIKELIHOOD
IMPACT

	Low	Medium	High
High	Low Impact High Likelihood Tolerate/Treat	Medium Impact High Likelihood T19, T23, T25, T26 Treat/Transfer	High Impact High Likelihood T02, T04, T05, T10, T11, T20, T28, T31, T32 Treat/Transfer/ Terminate
Medium	Low Impact Medium Likelihood Tolerate/Treat	Medium Impact Medium Likelihood T01, T03, T12, T18, T21, T22, T24 Treat/Transfer	High Impact Medium Likelihood T09, T13, T14, T29, T30 Treat/Transfer/ Terminate
Low	Low Impact Low Likelihood T06, T07, T08 Tolerate	Medium Impact Low Likelihood T15, T27 Tolerate/Treat	High Impact Low Likelihood T16, T17 Treat/Transfer

Figure 3 Risk Assessment Matrix with overall Risk Severity (Source: Gcu.ac.uk, 2019)

The Risk Assessment Matrix in Figure 3 is used for classifying the risks into mitigation standards. Even though there is low budget to mitigate threats the prison is planning to mitigate the threats through implementation of the controls.

4.1 Organizational Policies

In this case following Information Security Policies are relevant:

Table 7 Organization Policies

Policy	Objective
Patch Management	A set of policies should be defined for fixing the vulnerabilities and bugs in the Technology used in the Prison
Access Controls	A set of policies should be defined for access controls for different users in the prison.
Acceptable use	A set of policies should be defined for the time duration a prisoner can access the System, Web and Video Conference.
Workplace monitoring	A set of policies must be defined for monitoring the prisoner, prison staff and vendors/janitors working in the prison.
Password Creation	A set of policies must be defined for creating a strong password for accessing the system and the network.
Removable Devices	A set of policies must be defined for usage of Removable device inside the prison.
Malware protection	A set of policies must be defined for protection against any malware attacks.
Electronic Communication	A set of policies should be set for electronic communication Email, Video Conferencing.
Staff Training	A set of policies must be defined for conducting workshops and training the staff regularly.
Security teams	A set of policies must be defined for shift change of duties of the staff.
Security monitoring	A set of policies must be defined as how the system, prisoner, prison cells should be monitored

Protection of information security and physical assets	A set of policies must be defined for assuring the security of the data, assets, network and database in the prison.
Disaster Recovery	There should be a set of policies defined for disaster recovery

4.2 Recommend Control(s)

Table 8 Security Controls and Control Areas for the Threats

<table>
<tr><th>Threat</th><th>Security Controls
to be Implemented</th><th>Control Areas for Treatment From ISO-27001 ((Esdebe.com, 2019); (Purba and Soetomo, 2018))</th><th>Treated Residual Risk</th></tr>
<tr><td>Spoofing</td><td>Authentication is the way to mitigate.
<table>
<tr><th>Authenticating</th><th>Technology</th></tr>
<tr><td>Computer</td><td>IPSec, SSH host Keys.</td></tr>
<tr><td>Connections</td><td>Cookies</td></tr>
<tr><td>Files/Messages</td><td>Digital Signature, Hashes</td></tr>
<tr><td>People</td><td>Biometric</td></tr>
</table></td><td>
<table>
<tr><th>TID</th><th>Controls</th></tr>
<tr><td>T01</td><td>A.9</td></tr>
<tr><td>T02</td><td>A.10</td></tr>
<tr><td>T03</td><td>A.12.6.2, A.10, A.13</td></tr>
<tr><td>T04</td><td>A.10, A.13</td></tr>
<tr><td>T05</td><td>A.9.3</td></tr>
<tr><td>T06</td><td>A.12.4.4</td></tr>
</table></td><td>Low</td></tr>
<tr><td>Tampering</td><td>Integrity is the way to mitigate.
<table>
<tr><th>Integrity</th><th>Technology</th></tr>
<tr><td>Network Traffic</td><td>IPSec, SSH, SSL.</td></tr>
<tr><td>Files, Database Messages</td><td>Digital Signature, Hashes and ACLs</td></tr>
</table></td><td>
<table>
<tr><th>TID</th><th>Controls</th></tr>
<tr><td>T07</td><td>A.12.4.4, A.13.1.1, A.10.1.1</td></tr>
<tr><td>T08</td><td>A.9.2.5, A.9.2.3, A.9.2.2, A.9.4</td></tr>
<tr><td>T09</td><td>A.13.1, A.9.4.1</td></tr>
<tr><td>T10</td><td>A.13.1, A.13.2.1,</td></tr>
</table></td><td>Low</td></tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td>
<table>
<tr><td></td><td>A.9.4.1,
A.9.4.5,
A.9.4.4</td></tr>
<tr><td>T11</td><td>A.13.1,
A.9.4.4,
A.10.1</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td><b>R</b>epudiation</td>
<td>Non-Repudiation is the way to mitigate.
<table>
<tr><th>Technology</th></tr>
<tr><td>Logging, Hash tree, Digital Signatures, Secure time stamp</td></tr>
</table>
</td>
<td>
<table>
<tr><th>TID</th><th>Controls</th></tr>
<tr><td>T12</td><td>A.12.4.2,
A.10.1,
A.9.4.1,
A.9.3,
A.9.1.2</td></tr>
<tr><td>T13</td><td>A.10.1.1</td></tr>
<tr><td>T14</td><td>A.9.4.1,
A.13.1,
A.12.4.4</td></tr>
<tr><td>T15</td><td>A.9.4.1,
A.12.4.2,
A.12.4.4</td></tr>
<tr><td>T16</td><td>A.12.4.2,
A.9.2</td></tr>
<tr><td>T17</td><td>A.12.4.2,
A.9.2,
A.12.3.1</td></tr>
</table>
</td>
<td>Low</td>
</tr>
<tr>
<td><b>I</b>nformation Disclosure</td>
<td>Confidentiality is the way to mitigate.
<table>
<tr><th>Confidentiality</th><th>Technology</th></tr>
<tr><td>Files</td><td>ACLs, Encryption</td></tr>
<tr><td>Network Data</td><td>Encryption, Key Management</td></tr>
<tr><td>Communication Headers</td><td>Onion Routing, Steganography</td></tr>
</table>
</td>
<td>
<table>
<tr><th>TID</th><th>Controls</th></tr>
<tr><td>T18</td><td>A.9.1.2,
A.10.1.1,
A.12.4.2</td></tr>
<tr><td>T19</td><td>A.10.1</td></tr>
<tr><td>T20</td><td>A.13.1.1,
A.13.1.2</td></tr>
<tr><td>T21</td><td>A.12.4.2</td></tr>
<tr><td>T22</td><td>A.9.4.1</td></tr>
</table>
</td>
<td>Low</td>
</tr>
</table>

<table>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>Denial of Service</td><td>Availability is the way to mitigate.<table><tr><th>Technology</th></tr><tr><td>ACLs, Filters, Quotas for rate limiting, thresholding, throttling, Extra Bandwidth</td></tr></table></td><td><table><tr><th>TID</th><th>Controls</th></tr><tr><td>T23
T24
T25
T26
T27</td><td>A.13.1,
A.11.2.4,
A.12.1.3,
A.9.4.2</td></tr></table></td><td>Low</td></tr>
<tr><td>Elevation of Privilege</td><td>Authorization is the way to mitigate.<table><tr><th>Technology</th></tr><tr><td>ACLs, Role based access control, Unix sudo and Windows privilege.</td></tr></table></td><td><table><tr><th>TID</th><th>Controls</th></tr><tr><td>T28</td><td>A.9.1,
A.9.2.3,
A.9.4.2</td></tr><tr><td>T29</td><td>A.13,
A.12.6.1</td></tr></table></td><td>Low</td></tr>
<tr><td>Other Threats</td><td>Implementation of Anti-drone technology, Anti-malware software and Intrusion detection</td><td><table><tr><th>TID</th><th>Controls</th></tr><tr><td>T30</td><td>A.11.1</td></tr><tr><td>T31</td><td>A.12.2,
A.12.6</td></tr><tr><td>T32</td><td>A.9.2,
A.9.3,
A.9.4</td></tr></table></td><td>Low</td></tr>
</table>

4.3 Recommended Standards

ISO /IEC 27000 series focusses on IT security techniques and information security management systems in organizations and ISO/IEC 31000 series focusses on principles and guidelines for risk management in organizations(Sunthonwutinun and Chooprayoon, 2013). So, in this report ISO 27000 series standard ISO 27001 is used for applying the security controls for the threats as it is more technical and helps in addressing the mitigation of the threats in the organization and the ISO 31000 standard is used for planning the overall risk management of the prison as it advises approach risk management strategically and comprehensively as shown in Figure 4. Additionally, relevant policies need to be created by the organization as there is no particular standard for policies.

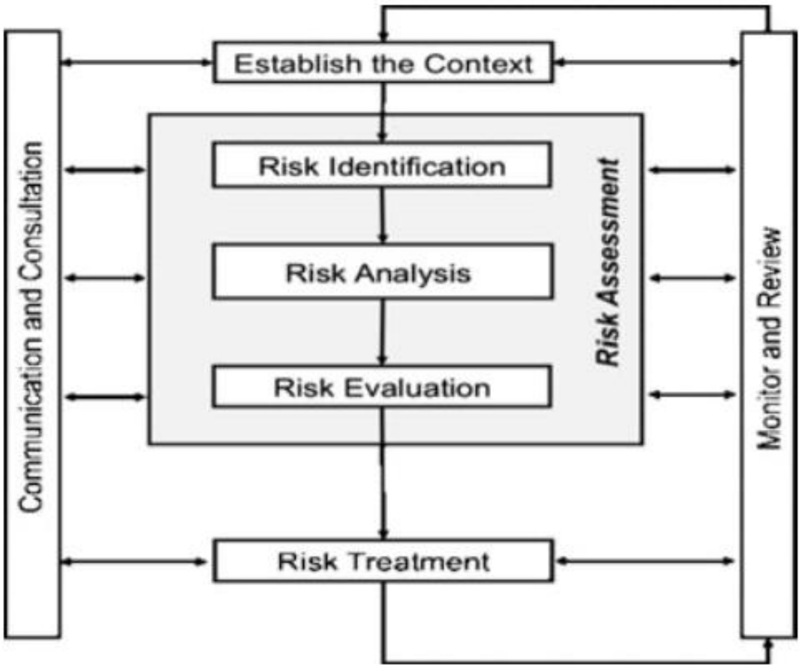


Figure 4 Risk Management Process from ISO 31000:2009(Source: Purdy, 2010)

Risk management standards need to be implemented in the organisations as they help in achieving the objectives and requirement of the organisation to prevent risks through High quality risk management reports.

ISO 31000 series	1. ISO 31000:2009 for Principles and Guidelines on Risk Management Implementation 2. ISO/IEC 31010:2009 for Risk Management and Risk Assessment Techniques
ISO 27000 series	1. ISO 27001-Implemention requirements for an ISMS 2. ISO 27002- Supplement to ISO 27001 for Information Security Controls. 3. ISO 27017- For Information stored in Cloud
Incident response Standard	1.NIST SP 800-61-Computer Security Incident handling guide.

5.INCIDENT RESPONSE

This subsection discusses about the role and the responsibility of the Incident Response team (Iltanet.org, 2019) in the prison and how they are to be notified, the types of incidents that can take place, what are their responsibilities and how the risks should be identified and the incident response lifecycle to be followed for each risk.

5.1 Incident Response Team

Incident response team has been made to deal with incidents in an effective and a feasible manner to avoid loss of Information and will be responsible for dealing with any incidents taking place in the prison which can cause damage to any prison services or prison information such as sensitive prison information containing prisoner information etc. They are authorized to take any steps for protecting the Confidentiality, Integrity and Availability of the prison and prison services. The Team consists of The Governor, Deputy Governor, Head of Operations and Security, Head of Administration, IT staff.

5.1.1 Incident Response Notification

There will be an IT help desk operating in the prison by a prison staff who will be available 24X7 hrs and their responsibility is to register any incidents when reported and then immediately contacting the Incident Response Team.

5.1.2 Types of Incidents

There can be many incidents taking place within a prison some of them are listed below: Software Attacks, Port scans, Information disclosure, Denial of Service, Malware Attack, Prison escape, Drone reporting, Data tampering etc.

5.1.3 Employee Responsibility

The Employee should report any incidents immediately upon discovery to the IT help desk and should assist in acquiring the required information about incident and if any evidence found during discovery, they should preserve it for Investigation.

5.1.4 Classification/Identification of Potential Incident

All the reported incidents must be classified in terms of the risk and damage level they can cause to the prison and its services.

5.1.5 Incident Response Life Cycle for Prison (Cichonski et al., 2012)

When a potential incident has been identified the Incident Response Team must follow the four phases of the incident response life cycle NIST SP 800-61, which are as follows:

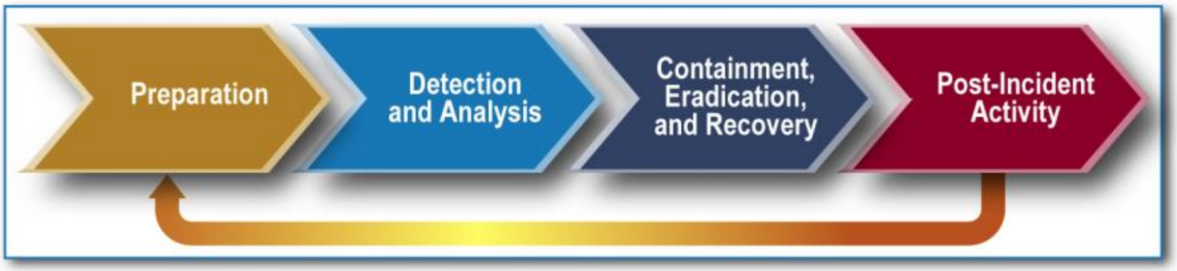


Figure 5 Incident Response Lifecycle (Source: Cichonski et al., 2012)

Based on Figure 5 in 1) Incident response team must prepare for incident handling. 2) They must analyse the symptoms of the incident to decide whether the reported incident has taken place. 3)They must try to contain the incident, eradicate or recover from the incident by check whether all the vulnerabilities of the system are eliminated, and system operations are restored.4) They must stop the incident from repeating, improve the procedure for handling the incident and also must review the Incident response plan quarterly.

REFERENCES

CICHONSKI, P., MILLAR, T., GRANCE, T. & SCARFONE, K. 2012. Computer security incident handling guide. NIST Special Publication, 800(61), pp.1-147.

Esdebe.com. (2019). [online] Available at: http://www.esdebe.com/perch/resources/iso-27001-annex-s-control-mapping.pdf [Accessed 29 Oct. 2019].

Gcu.ac.uk. (2019). [online] Available at: https://www.gcu.ac.uk/media/gcalwebv2/theuniversity/supportservices/financeoffice/Risk_Management_Strategy.pdf [Accessed 29 Oct. 2019].

Hse.gov.uk. (2019). OC 334/2: Prison service organisation, management and inspection. [online] Available at: http://www.hse.gov.uk/foi/internalops/ocs/300-399/334_2/#para5-12 [Accessed 29 Oct. 2019].

HUGHES, G., 2006. Five Steps to IT Risk management Best Practices. Risk Management, 53(7), pp. 34-36,38,40.

Iltanet.org. (2019). [online] Available at: https://www.iltanet.org/HigherLogic/System/ DownloadDocumentFile.ashx?DocumentFileKey=966e76a0-5664-43b6-9f3e-fa0540055508&ssopc=1 [Accessed 29 Oct. 2019].

Ncsc.gov.uk. (2019). [online] Available at: https://www.ncsc.gov.uk /section/advice-guidance/all topics?topics=cyber%20attack&sort=date%2Bdesc &start=0&rows=20 [Accessed 31 Oct. 2019].

Owasp.org. (2019). OWASP Risk Rating Methodology - OWASP. [online] Available at: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology [Accessed 29 Oct. 2019].

PURBA, A. & SOETOMO, M. 2018. Assessing Privileged Access Management (PAM) using ISO 27001: 2013 Control. ACMIT Proceedings, 5, 65-76.

PURDY, G. 2010. ISO 31000: 2009—setting a new standard for risk management. Risk Analysis: An International Journal, 30, 881-886.

Resources.sei.cmu.edu. (2019). [online] Available at: https://resources.sei.cmu.edu /asset_files/WhitePaper/2018_019_001_524597.pdf [Accessed 31 Oct. 2019].

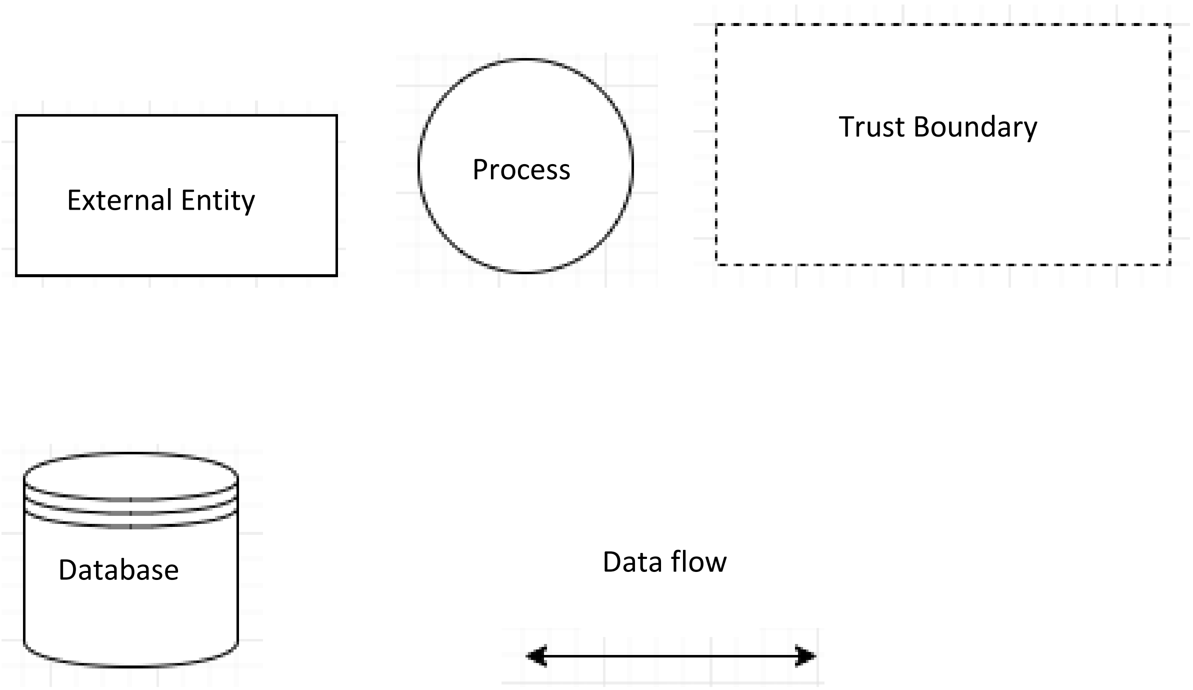
SHOSTACK, A. 2014. Threat Modeling: Designing for Security, Wiley Publishing.

SUNTHONWUTINUN, W. & CHOOPRAYOON, V. A benchmarking study of standard frameworks for information technology governance. Second Asian Conference on Information Systems, Phuket. http://saki. siit. tu. ac. th/acis2013/app/webroot /downloads/acis2013_proceeding. pdf, 2013.

Wpc.0064.edgecastcdn.net. (2019). [online] Available at: http://wpc.0064.edgecastcdn.net /000064/accelus-pdf/whitepapers/Mastering_Risk_Assessment.pdf [Accessed 29 Oct. 2019].

Appendix A

DFD Notations:



1.External Entity: It is used for sending /receiving data from the system

2.Process: It is an activity used for transforming and manipulating input data to output data.

3.Trust Boundary: It is used for boundary where program data / execution changes its level of trust.

4.Database/Datastore: It is used for storing the data permanently/temporarily.

5.Data Flow: It is used for conveying the flow of data between Entity, Process and database

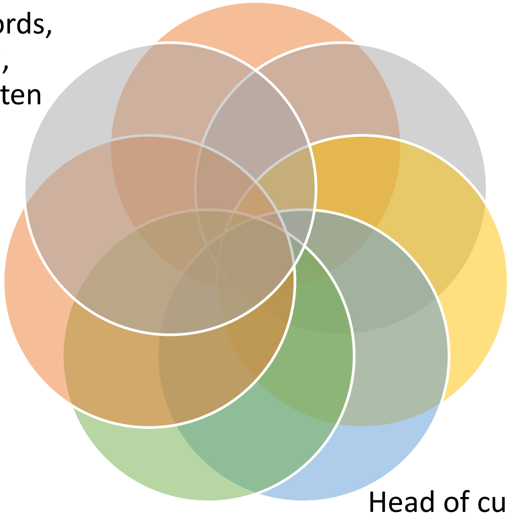
Appendix B

Roles and Responsibilities of the Management are as follows (Hse.gov.uk, 2019):

Governor is the managerial head of the prison and he will be held responsible and accountable for all staff.

Head of administration is responsible for employing and managing staff in keeping records, filing papers, photocopying, printing and dealing with written and phone enquires.

Deputy Governor is second in charge of the prison.



Head of operations and Security is responsible for safeguarding the prison with prison officers and prison support staff.

Head of recreational activities is responsible for conducting rehabilitation programmes, entertainment activities, vocational training.

Head of healthcare is responsible for health care staff and primary care of the prisoners.

Head of custody is responsible for implementing safer custody with strict rules and will also take care of prisoner induction to their prison cells.

Risk Responsibilities:

Overall:

All the prison staff are responsible for identifying, handling and securing prison information.

Governance:

The Governor has the responsibility for managing the risk and establishing the required standards, policies and controls for proper functioning of the overall prison.

Head of Administration will have the overall responsibility of handling the information risks from risk identification till the risk mitigation.

System Admin will have the admin control to the prison software system and will have IT staff working under him for updating and maintaining the prison software.

Head of Operations and security will have the overall responsibility of physical security of the prison and works closely with Head Administration for information related security.

Head of custody will have overall responsibility of security inside the prison cells.

Head of Healthcare will have the overall responsibility of health care related to the prison.

Head of recreational activities will be responsible for conducting the staff training so that information risk is understood and efficiently handled in everyday activities of the prison.

Appendix C

Factors Considered for Scoring the Threat Agent (Owasp.org, 2019)**:**

Factors	Characteristics	Score
Skill Level	No Technical Skills	1
	Some Technical Skills	3
	Advanced Computer User	5
	Network and Programming Skills	6
	Security Penetration Testing	9
Motive	Low/No Reward	1
	Possible Reward	4
	High Reward	9
Opportunity	Full Access /Expensive resources required	0
	Special Access/resources required	4
	Some Access/resources required	7
	No Access/resources required	9
Size	Developers	2
	System Administrators	2
	Intranet Users	4
	partners	5
	Authenticated users	6
	Anonymous internet users	9

Factors Considered for Scoring the Vulnerability (Owasp.org, 2019)**:**

Factors	Characteristics	Score
Ease of Discovery	Practically impossible	1
	Difficult	3
	Easy	7
	Automated Tools	9
Ease of Exploit	Theoretical	1
	Difficult	3
	Easy	5
	Automated Tools	9
Awareness	Unknown	1
	Hidden	4
	Obvious	6
	Public Knowledge	9
Intrusion Detection	Active Detection in Application	1
	Logged and Reviewed	3
	Logged without Review	8
	Not Logged	9

Factors considered for scoring the Technical Impact (Owasp.org, 2019)**:**

Factors	Characteristics	Score
Loss of Confidentiality	Minimal non-sensitive data disclosed	2
	Minimal critical data disclosed	6
	Extensive non-sensitive data disclosed	6
	Extensive critical data disclosed	7
	All data disclosed	9
Loss of Integrity	Minimal slightly corrupt data	1
	Minimal seriously corrupt data	3
	extensive slightly corrupt data	5
	extensive seriously corrupt data	7
	all data totally corrupt	9
Loss of Availability	Minimal secondary services interpreted	1
	Minimal primary services interpreted	5
	extensive secondary services interpreted	5
	extensive primary service interrupted	7
	all services completely lost	9
Loss of Accountability	Fully Traceable	1
	Possibly Traceable	7
	Completely anonymous	9

Appendix D

Risk and Risk owners are as follows:

Risk	Risk Owner	Risk Treatment Due
T01	System Admin	Authentication Related Risks are to be solved within 1 Hr.
T02	System Admin, IT Staff	
T03	System Admin	
T04	System Admin, IT Staff	
T05	IT Staff	
T06	IT Staff	
T07	System Admin	Integrity Related Risks are to be solved within 2 Hrs
T08	System Admin	
T09	System Admin	
T10	IT staff	
T11	System Admin	
T12	System Admin	Repudiation Risks are to be solved within 3 Hrs.
T13	IT staff	
T14	System Admin	
T15	System Admin	
T16	System Admin	
T17	System Admin	
T18	System Admin	Confidentiality Risks are to be solved within 1 Hr.
T19	System Admin	
T20	IT staff	
T21	IT staff	
T22	System Admin	
T23	IT staff	Availability Risks are to be solved within 3 Hrs.
T24	IT staff	
T25	IT staff	
T26	System Admin	
T27	IT staff	
T28	IT staff	Authorization Risks are to be solved within 45 Minutes
T29	IT staff	
T30	Prison Security officer	Drone Risk is to be solved within 30 Minutes
T31	IT staff	Malware risk is to be mitigated within 1 Hr.
T32	System Admin	Intrusion detection should be mitigated within 1.30 Hr.