Table of Contents

Table of Figures ..... *i*
Table of Tables ..... *ii*
1 Introduction *3*
2 Risk Management *3*
2.1 Establish the context **3**
2.1.1 Strategic Objectives Scope 3
2.1.2 Current Requirements/Plans 3
2.1.3 Internal & External boundaries 3
2.1.4 Organization Structure 4
2.1.5 Governance Model 6
2.2 Risk Identification **7**
2.2.1 Asset Identification 7
2.2.2 Assets Classification 8
2.2.3 Assets Prioritization 8
2.2.4 Threat Assessment 8
2.2.4.1 Threat analysis 8
2.2.4.2 Threat model 9
2.3 Risk Assessment **10**
2.4 Risk Controls **12**
2.4.1 Risks Defended 12
2.4.2 Risks Terminated 13
2.4.3 Risks Mitigated 14
2.4.3.1 Disaster Recovery plan 15
2.4.4 Risk Transferred 15
2.4.5 Risks Accepted 16
2.5 Threat Model after Controlling risks **16**
3 Performance Monitoring & Communication *17*
4 Conclusion *18*
5 References *19*
6 APPENDICES *20*
6.1 Appendix A: System Configuration Policy **20**
6.2 Appendix B: Network Configuration Policy **21**
6.3 Appendix C: Server Configuration Policy **22**
6.4 Appendix D: Password Protection Policy **23**
6.5 Appendix E: Disaster Recovery Plan **24**
6.6 Appendix F: Statement of Applicability **31**

Table of Figures

Figure 1: Prison Environment 4
Figure 2: HMP Beechnut Prison Hierarchy 5
Figure 3: Enhanced Prison Hierarchy 5
Figure 4: Governance Model 7
Figure 5: Threat Model 9

Figure 6: Defense Risk-handling process 12
Figure 7: Termination Risk-handling process....14
Figure 8: Mitigation Risk-handling Process 14
Figure 9: Transferred Risk-handling process....15
Figure 10: Accepted Risk-Handling Process 16
Figure 11: Threat Model with Controls 17
Figure 12:ISO 27001 Controls Status 18

Table of Tables

Table 1:Enhanced Prison Jobs 5
Table 2: Prison Assets....7
Table 3: Assets Classification....8
Table 4:Threats Identified....8
Table 5: Qualitative Risk Assessment 10
Table 6: Classification Purpose 10
Table 7: Ranked Vulnerability risk worksheet 11
Table 8: Risks Defended....12
Table 9: Risk Terminated....14
Table 10: Risk Mitigated 15
Table 11: DRP Assigned Roles....15
Table 12: Risk Transferred 15
Table 13:Risk Accepted....16
Table 14: Risk 1 and 2 Registration....18
Table 15: DRP Version....24
Table 16:Internal Contact Information 24
Table 17: External Contact Information 25
Table 18: Emergency Services Information 25
Table 19: Back-up Strategy 26
Table 20: DR Threat Assessment 26
Table 21: DR Risk Assessment Classification....27
Table 22: DR Risks Identified 27
Table 23: Recovery Procedure....28
Table 24: Escape Procedure....29
Table 25: DR Checklist....30
Table 26: Statement of Applicability....31

1 Introduction

This report is a risk management report that will aid in identifying the risks, asses them, and then provide suitable controls for their environment. Subsequently, the process will focus on the innovation of a Swiss organization called “ACME AG “in increasing the use of technology in prison called “HMP Beechnut “which is classified as a category B prison and holds 1200 prisoners.

2 Risk Management

This section covers identifying, assessing and controlling risks. There are multiple standards for risk management processes, such as ISO 31000 and ISO 27005. Although both of them are applicable and provide a general site of the risk management approach, this document will follow ISO/IEC 27005 (2018) to obey with information security management system (ISMS) requirements. In addition, it precisely focuses in information security risk. On the other hand, ISO 31000 provides wide guidelines that could be appealed to any aspect of risk management.

The following report will begin with identifying the organization context, identifying the risks, assess them, and then controlling them.

2.1 Establish the context

This section provides a general view of the strategic objective of the report, requirements, the internal and external boundaries, organization structure, and the governance model.

2.1.1 Strategic Objectives Scope

ACME AG is a Swiss organization that had won the chance to innovate in HMP Beechnut prison with a 25-year contract. The primary purpose of the innovation is to modernize the prison. ACME AG will achieve that by engaging technology in the daily life of both employees and prisoners. Thus, this report stands out as a management level report that will assess all the possible risks that come along with the innovation process.

2.1.2 Current Requirements/Plans

The plan and requirements of modernizing the prison are focused on accomplishing the following:

- Allowing the individual prisoners to access and connect to the internet by commencing a network access point in their cells.
- Establishing a video conference rooms to allow the prisoners to have virtual visits.
- Moving the current “on-site” database of prisoners to a cloud environment in order to be accessed by the UK government, social research centers, and nation X.
- Preventing the abuse of drones in delivering drugs and sims to the prisoners.

2.1.3 Internal & External boundaries

The prison environment is divided into three boundaries, which are a prison, national, and international boundary, as shown in Figure 1.

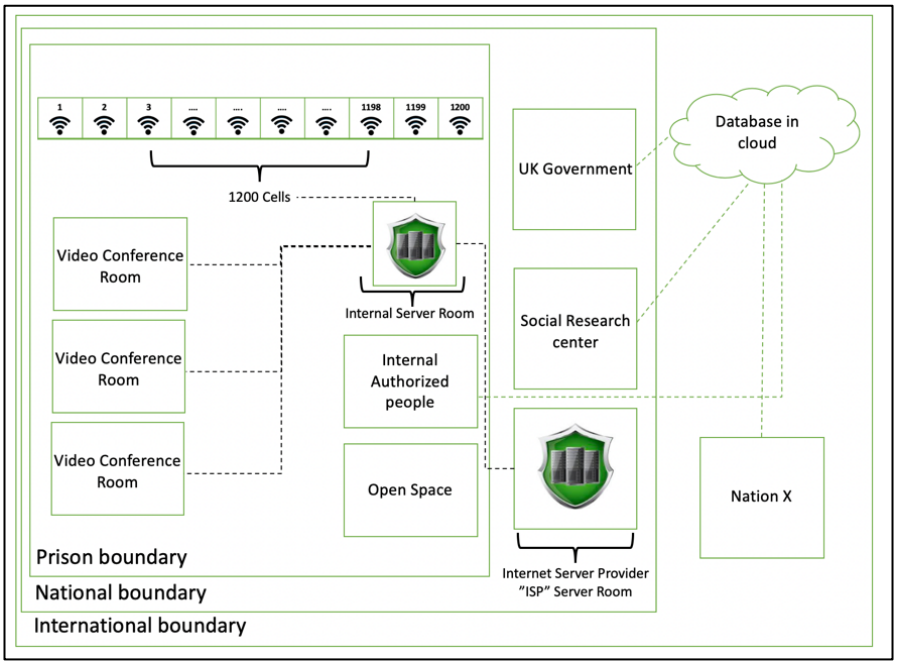

Figure 1: Prison Environment

2.1.4 Organization Structure

According to the UK government (2019), the following are the job roles in the prison:

- Manager
  - Responsible for making new decisions and should involve in creating a policy. He is the director of the prison.
- Prison operation support (POS)
  - Responsible for helping people to bring them back on the right track by providing supervision, training, and motivating the prisoners.
- Prison operation officer (POO)
  - Responsible for monitoring daily operations in prison. For example, monitoring and checking CCTV records.
- Admin Officer (AO)
  - Responsible for maintaining, dealing, and analyzing with the files.
- Admin Assistant (AA)
  - Responsible for inputting data.

All of these roles outcomes are reviewed and monitored by HM Chief Inspector of Prisons (HCIOP). Figure 2 shows the prison hierarchy.

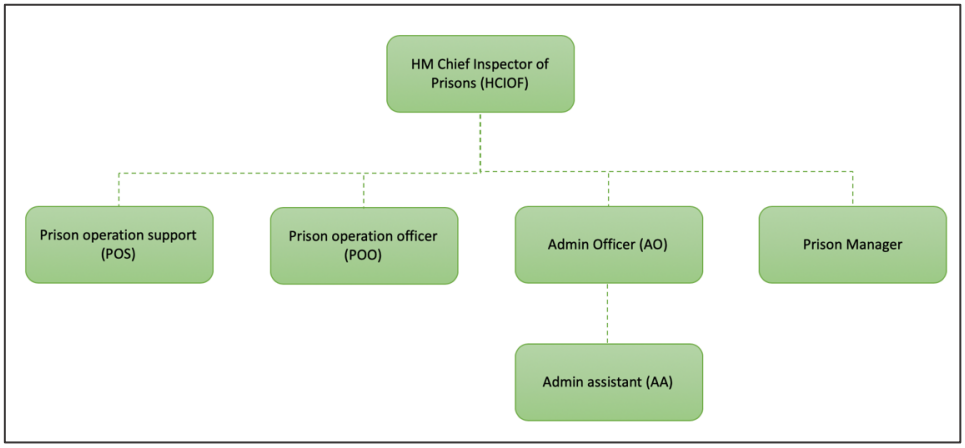

Figure 2: HMP Beechnut Prison Hierarchy

However, the prison should have decent top management who have sufficient IT knowledge, which is demanded to establish decisions that support the performance of IT governance and risk management process. Consequently, based on Whitman and Mattford the prison hierarchy was enhanced as shown in Figure 3 (2013).

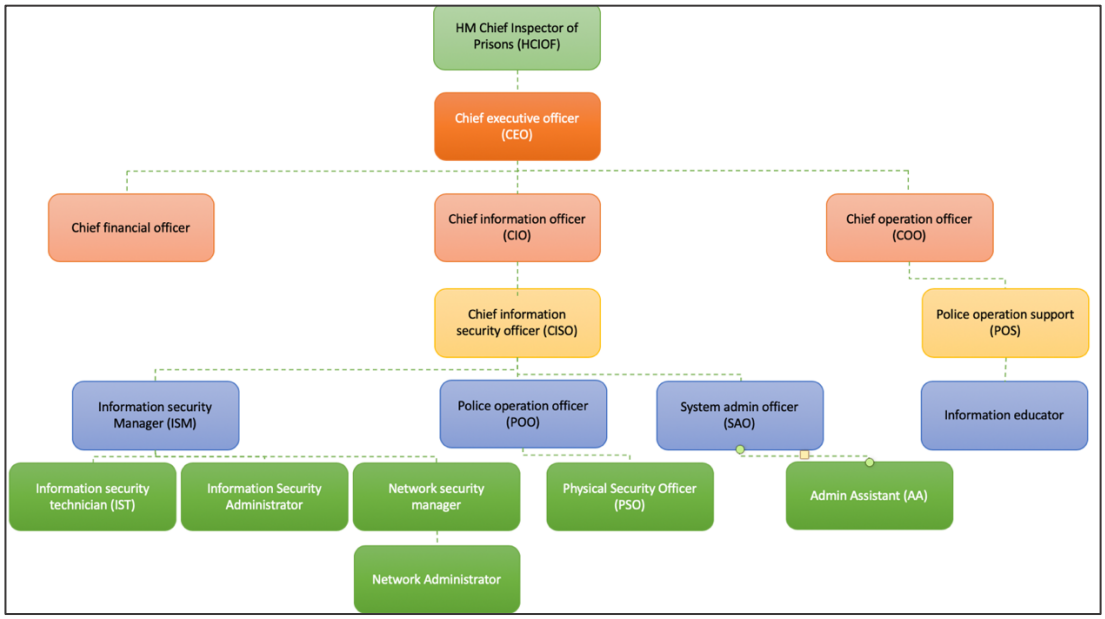

Figure 3: Enhanced Prison Hierarchy

Table 1 list all the prison positions and their description.

Table 1:Enhanced Prison Jobs

Position	Description
Executive team members	
Chief Executive Officer (CEO)	Responsible for effective and efficient management and leadership.
Chief Information Officer (CIO)	Responsible for directing the CISO on producing and establishing coherent and supportive plans
Chief Financial Officer (CFO)	Responsible for reporting the financial status of the prison.

Chief Operation Officer (COO)	Responsible for directing PSO to monitor the prison's physical operations.
Chief Information Security Officer (CISO)	Initiating and developing the plans charged by the CIO.
Other roles	
Information Educator (IE)	Communicating policies and initiating training programs.
System Admin Officer (SMO)	Responsible for maintaining, dealing, and analyzing with the files in the systems.
Information security administrator (ISA)	Responsible for handling, monitoring, and assessing all the IT-related security compliance.
Network Technician (NT)	Capable of configuring and troubleshooting all the network infrastructure. Report any incidents to NSM.
Physical Security Officer (PSO)	Monitor the prison's physical operations and report any incidents to COO.
Information Security Manager (ISM)	Monitor day-to-day operations of the information security program.
Information Security Technician (IST)	Enhance the security state of all the system based on specific security requirements.
Network Security Manager (NSM)	Monitor the network technician and ensure that the network infrastructure can assure compliance with the security policies.

2.1.5 Governance Model

Figure 4 shows the Information security governance model for the prison that was established based on ISO/IEC 27014 (2013), which indicate that the governing body will be responsible for the following:

- Evaluate the most recent security objectives that need to be reflected in the current process.
- They provide direction to the executive management in which security activities that need to implement.
- Assess and Monitor the outcomes of the security objectives.
- Communicate and exchange the security objectives and processes with stakeholders.

The HCIOP will monitor and validate the security objectives that were associated with carrying out governance activities to accomplish the desired level of information security.

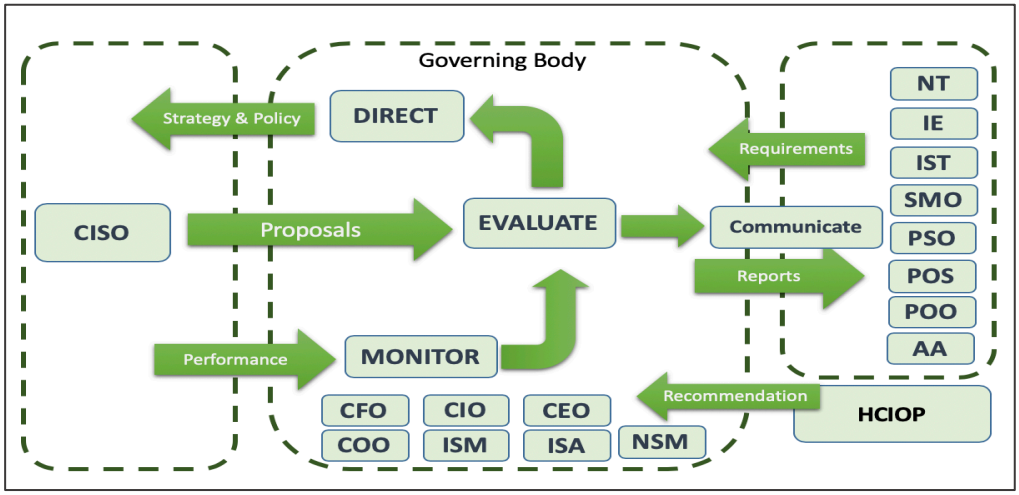

Figure 4: Governance Model

2.2 Risk Identification

The purpose of risk identification is to identify what are the possible potential losses, how, and where it could happen.

2.2.1 Asset Identification

This process identifies and create an inventory of the assets as shown in table 2 that must be labeled and monitored regularly.

Table 2: Prison Assets

System Components		Risk Management Assets	Asset Owner
People	Internal authorized personnel (IAP)	IAP	IE
	External authorized personnel (EAP)	UK government Social Research Center Nation X	
Data		All information that are in transmission, processing, or storage state in the **DB**.	SMO, AA.
Software		DB	SMO
Hardware	System devices and peripherals	Internal Server.	NSM
		Video/audio system.	IST
	Networking components	Router in each cell to provide internet connectivity.	NT
Physical		Prison open space.	PSO
		Individual prisoners' cells.	POO.

2.2.2 Assets Classification

The classification scheme of the assets considered as the following: confidential, internal, and public that will label the level of protection for the asset. Table 3 shows the classification of the assets and their impact.

Table 3: Assets Classification

Risk Management Assets	Classification	Impact on		
		Public image	Technical	Business
IAP	Internal.	Low.	Moderate.	High.
EAP	Public.	Low.	Moderate.	High.
DB	Confidential.	High.	High.	High.
Internal server.	Confidential.	High.	High.	High.
Video/audio system	Internal.	High.	High.	High.
Router.	Internal.	High.	High.	High.
Prison open space.	Confidential.	Moderate.	High.	High.
Individual prisoners' cells.	Confidential.	High.	High.	High.

2.2.3 Assets Prioritization

Based on table 3, the following is the list of assets in order of significance:

1. DB
2. Internal server.
3. Individual prisoners' cells.
4. Prison open space.
5. Router.
6. Video/audio system.
7. IAP
8. EAP

2.2.4 Threat Assessment

This process includes analyzing the threats and establishing a threat model.

2.2.4.1 Threat analysis

Based on the assets identified, table 4 shows the possible identified threats and vulnerabilities.

Table 4:Threats Identified

Threat	Possible vulnerability
Information discloser • **Sniffing the network.** • **SQL injection.** • **Eavesdropping in video calls.**	• Unencrypted network. • The usage of UDP in virtual-visits system.
Software attacks • **SQL Injection.** • **Installing a malware.** • **Compromising cloud API.** • **Session hijacking.**	• Absence of input validation. • Unprotected DB. • Vulnerable operating system (OS). • Vulnerable cloud schedular.

• **DoS attacks on networks.**	• Weak session management. • Low-bandwidth network.
Human error • **Social Engineering**	• Uneducated personnel.
Theft • **Identity theft**	• The usage of default password.
Forces of nature	-
Physical attack • **Physical breach.** • **Sending drugs/cells using drones.**	• Guards losing key • Prisoner cell's window. • Weak physical security. • Open spaces.

2.2.4.2 Threat model

A threat model has been initiated to determine and assess all the possible circumstances of each listed asset. Figure 5 shows all the threats listed in numbers using the threat model. As this report assess the innovation, there are still no controls deployed for each threat.

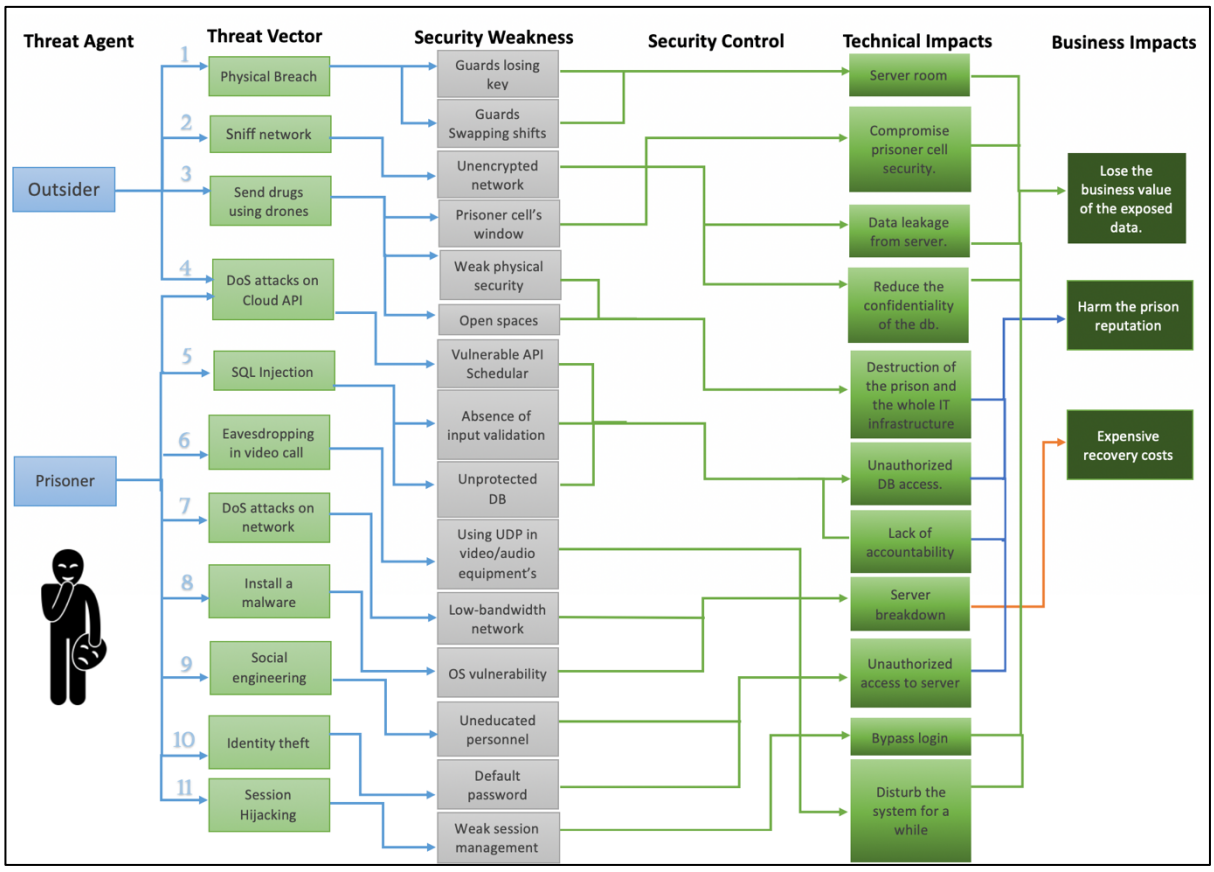

Figure 5: Threat Model

2.3 Risk Assessment

There are two ways for risk assessment which are Qualitative and Quantitative Risk assessment. However, due to the difficulties in determining an actual value to assess the risk, a qualitative risk assessment approach will be used. This approach uses two factors, which are the likelihood of the threat to happen and consequences that indicate the effects of the threat. Table 5 shows the likelihood of each listed threat in the threat model. Moreover, table 6 shows the purposes behind classifying each threat.

Table 5: Qualitative Risk Assessment

Risk level	**Consequence**				
Likelihood	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
A (almost certain)				2,5,9	
B (likely)			1	11	8
C (possible)				10	3,7
D (unlikely)	6				
E (rare)				4	
Classification					
Extreme Risk (E)	High Risk (H)	Medium Risk (M)	Low Risk (L)		

Table 6: Classification Purpose

Threat	Classification Purpose
1	The threat is likely to happen since the vulnerabilities are part of the prison routine. Moreover, there is a high financial loss because the attacker only has access to the server physically but not the credentials.
2	The first thing usually the attacker check is whether the network is protected or not; that's why it is almost certain to occur. Besides, it has a major consequence because it will affect one of the security objectives, which is the confidentiality of both the network and DB.
3	The usage of drones is widespread nowadays, thus, it is possible to be used for sending drugs or cells to the prison. However, the impact of this threat is catastrophic because it will cause a long-term distraction on the prison system.
4	It rarely happens because usually, the prison will select a trusted third party to provide a cloud platform for them to store their DB. On the other hand, even though the prison will shift the legal liability to the third party, the prison will face a major impact due to unauthorized access to DB.
5	An SQL injection is one of the well-known tricks that will be examined by various people. Hence, it is almost certain to happen. Also, there is a major consequence behind this threat because once it is successful, the attacker will have unauthorized access to DB.
6	It is unlikely to occur due to the need for further tools and equipment to implement it. Also, the impact is low because there is a low financial loss.
7	It is possible to occur because buffering the bandwidth with unwanted data is a straightforward process. However, the impact of DoS is catastrophic because it will shut down a service on the prison and will demand high recovery costs.

8	There are different paths of malware to be installed; Thus, it is always likely to happen. However, installing malware will always have a catastrophic impact on the services and prison systems.
9	Social engineering is an almost certain attack because it does not require any previous knowledge in technology. Although no practical knowledge needed, the impact is major since there is a physiological manipulation that will end up by the attacker having access to an asset.
10	Considering that some people will leave the default password, this threat is possible to happen. Furthermore, the impact behind it is major because the prisoner will gain access to the internal server.
11	One of the OWASP vulnerabilities is cross-site scripting XSS, which is used to implement session hijacking by allowing outsiders to steal the session token. Hence, the probability of this attack to happen is likely. Moreover, the impact of this attack is major since there will be privilege escalation without the knowledge of anyone.

Table 7 shows a summarized ranked vulnerability risk worksheet based on the risk factor.

Table 7: Ranked Vulnerability risk worksheet

ID	Asset	Vulnerability	Impact	Likelihood	Risk factor	Risk Owner
1	DB	Unprotected DB.	Major	Almost certain	Extreme risk	ISM
2		Absence of input validation.				IST
3	IAP	Uneducated personnel.				POS
4	DB	Unencrypted Network				NT
5	Internal server	OS vulnerability.	Catastrophic	Likely		ISA
6	DB	Weak session management.	Major			IST
7	DB	Usage of default password.		Possible		CISO
	Internal server					
8	Individual prisoners' cells	Cell's window.	Catastrophic			PSO
9	Prison open space	Weak physical security.				PSO

10	Router	Low-bandwidth network				NA
11	All the assets	Forces of nature		Unlikely		CIO
12	EAP	Uneducated personnel.	Major	Almost certain	High	IE
13	IAP	Guards losing keys.	Moderate	Likely		POO
	server room					
14	DB	Vulnerable cloud schedular.	Major	Rare		CISO
15	Video/audio system.	Using UDP	Insignificant	Unlikely	Low	IST

2.4 Risk Controls

This section shows how the prison can maintain the confidentiality, integrity, and the availability of their environment. This will be met through managing the identified risks based on ISO/IES 27001 (2018).

2.4.1 Risks Defended

This section will discuss all the risks that has been defended against. This strategy was chosen based on risk-handling process as shown in Figure 6.

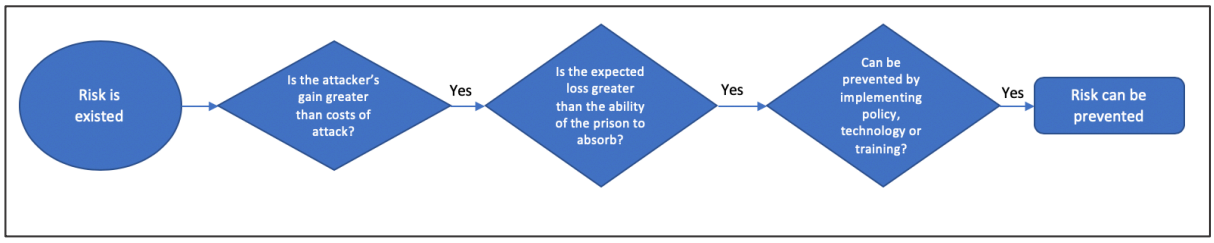

Figure 6: Defense Risk-handling process

Table 8 shows the controls that has been assigned for some risks to defend against them.

Table 8: Risks Defended

Risk ID	Description	Control/Procedure	ISO 27001 Control
1	Unauthorized access to DB due to unprotected DB.	• Apply an effective encryption and hashing mechanism. This will ensure the confidentiality and integrity of the DB. • Initiate access control list that specify the access right for each user.	A9.1.1 A9.2.2 A10.1.1
2,6	Unauthorized access to the DB through the	• Create a system-specific security policy (SysSSP) to provide guidance on how to configure a system	A12.1.4 A12.6.2

	absence of input validation and weak session management	securely (SCP). As a result, Nieles et al. (2017) publication of NIST 800-12r has been used as a director. See Appendix A.	A14.2.1 A14.2.8
3,12	Unauthorized access to server because of successful social engineering	• Offer a customized third-party training on social engineering that should be taken in place periodically.	A7.2.2
4	Data leakage from DB through unencrypted network.	• Apply an effective encryption. • Use Dynamic Bandwidth. • Create a network configuration policy (NCP), as shown in Appendix B.	A9.1.2 A13.1.1 A13.1.2 A13.1.3
10	Server breakdown owing to low-bandwidth networks.		
5	Server breakdown due to the use of vulnerable OS.	• Ensure the OS is regularly patched. • Create a server configuration policy (SCP) as shown in Appendix C.	A12.2.1 A12.6.1 A14.2.9 A16.1.3
7	Unauthorized access to internal server and DB because of default passwords.	• The usage of strong password is should be forced. • Create a password protection policy (PPP) as shown in Appendix D.	A9.4.3
9	Illegal equipment's retrieved through the open space by a drone.	• A jammer should be used to interrupt any communication between the pilot and the drone by exploding noise at the public radio frequencies of the drone, which are either 2.4GHz or 5.8GHz. Subsequently, when the drone is disturbed by a jammer's signal, the jammer offers the following two options: ○ First, the jammer can change the route of the drone to go back to the pilot with tracking ability. ○ Second, it can force the drone to land on a specific spot stated by the jammer (Pietro et al., 2019).	A11.1.4 A11.1.6
13	Unauthorized access to server room due to the possibility of guards losing keys.	• Apply a multifactor authentication such as fingerprint.	A11.1.1 A11.1.2 A11.1.3 A11.1.5

2.4.2 Risks Terminated

This section will discuss the terminated risks. This strategy was chosen based on risk-handling process as shown in Figure 7.

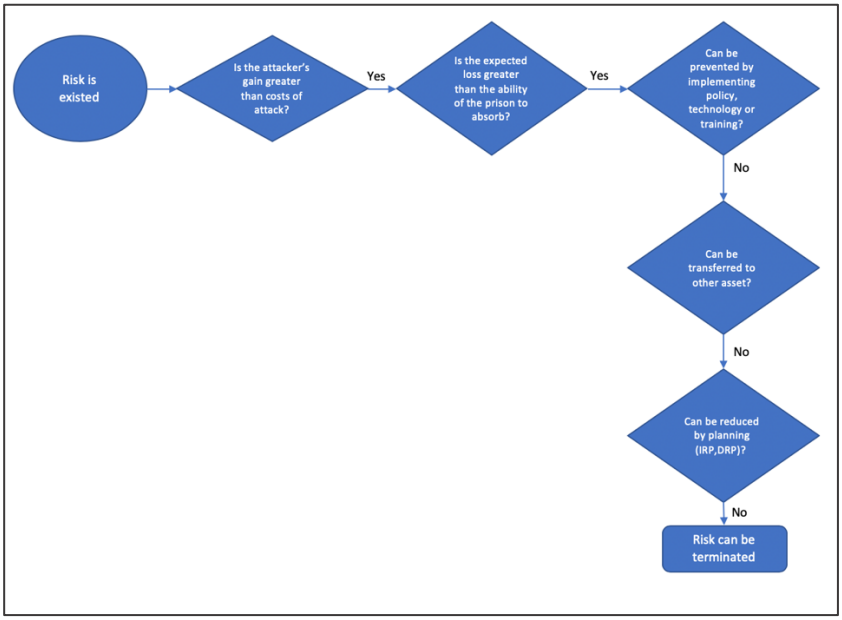

Figure 7: Termination Risk-handling process

Table 9 shows the procedure to handle with the terminated risk.

Table 9: Risk Terminated

Risk ID	Description	Control/Procedure	ISO 27001 Control
8	Prisoners might get drugs from a drone passing their cells window.	• Terminate the risk by removing the cell's windows owing to the fact that its challenging to ensure that each prisoners' cells are secured and protected by a PSO.	None

2.4.3 Risks Mitigated

This section will discuss the mitigated risks. This strategy was chosen based on risk-handling process as shown in Figure 8.

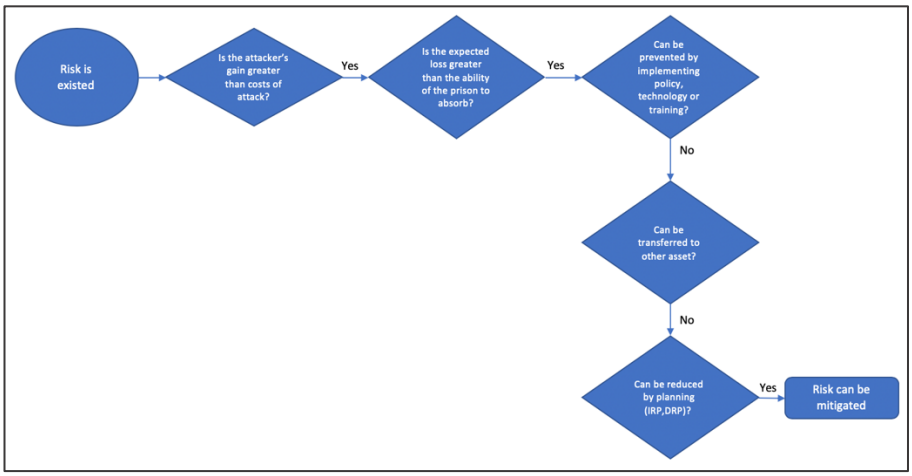

Figure 8: Mitigation Risk-handling Process

Table 10 shows the procedure to handle with the mitigated risk.

Table 10: Risk Mitigated

Risk ID	Description	Control/Procedure	ISO 27001 Control
11	Assets damage because of forces of nature such as earthquake, fire and floods.	• Initiate Disaster recovery plan.	A11.1.4 A12.3.1 A17.1.1 A17.1.2 A17.1.3

2.4.3.1 Disaster Recovery plan

The best approach to respond to this risk is to mitigate it by establishing a Disaster Recovery plan DRP based on ISO/IEC 24762 (2008) as shown in Appendix E. The roles and responsibilities of the DR team is shown in table 11.

Table 11: DRP Assigned Roles

DR team	Assigned employee
DR leader	CIO
DR Manager	CISO
Network Manager	NSM
Server Manager	NT
System Manager	ISM

2.4.4 Risk Transferred

This section will discuss the transferred risks. This strategy was chosen based on risk-handling process as shown in Figure 9.

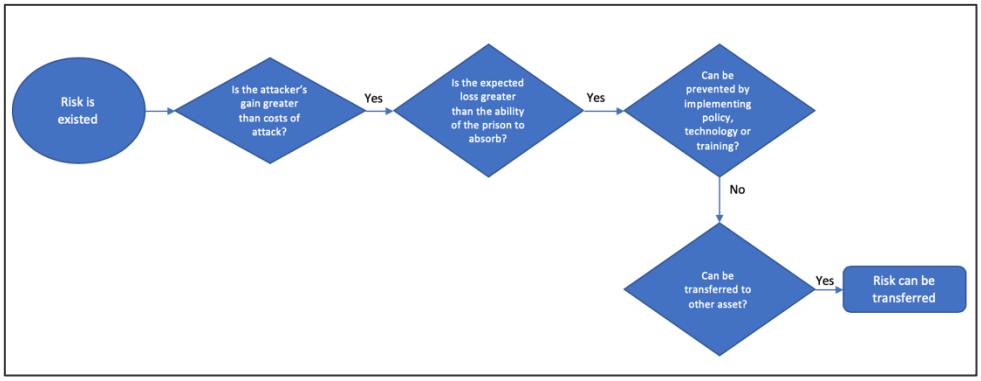

Figure 9: Transferred Risk-handling process

Table 12 shows the procedure to handle with the transferred risk.

Table 12: Risk Transferred

Risk ID	Description	Control/Procedure	ISO 27001 Control
14	Denial of service on the cloud service due to vulnerable cloud schedular. On other words,	• Transfer the risk to the third-party cloud provider. • Back-up DB regularly.	A12.3.1 A13.2.4 A14.2.7

	this allows malicious customers to gain an enhanced cloud service at the cost of other customers. By this threat the malicious customer is able to exploit up to 98% of the cloud CPU (Masdari & Jalali, 2016).	• Sign a non-disclosure agreement to guarantee that the confidentiality of DB is assured.	

2.4.5 Risks Accepted

This section will discuss the accepted risks. This strategy was chosen based on risk-handling process as shown in Figure 10.

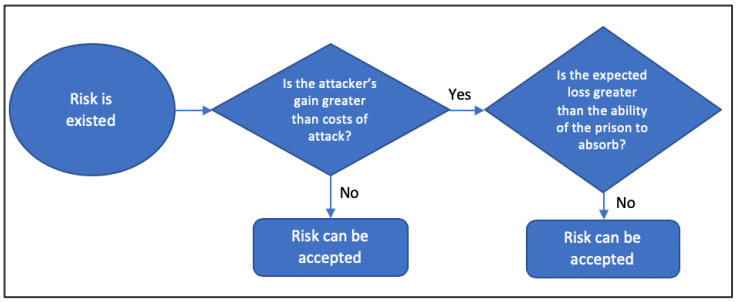

Figure 10: Accepted Risk-Handling Process

Table 13 shows the procedure to handle with the accepted risk.

Table 13:Risk Accepted

Risk ID	Description	Control/Procedure	ISO 27001 Control
14	DoS attacks on video/audio system due to the usage of UDP protocol. Using UDP places the system in the risk of a UDP flood attack. This attack is a DOS attack that is implemented by sending a variety of spoofed UDP packets to the system. Thus, in response to that, the system will be forced to send a variety of ICMP packets, which makes the system unreachable (Bardas et al., 2016).	• Accept the risk since it will only damage the video/audio system for a while. Besides, if it was replaced with TCP protocol, it wouldn't make the users convenient as it will wait for each dropped packets to re-transmitted and then transmit the new one, which will disturb the video streaming concept.	None

2.5 Threat Model after Controlling risks

Figure 11 is the threat model after deploying controls on them.

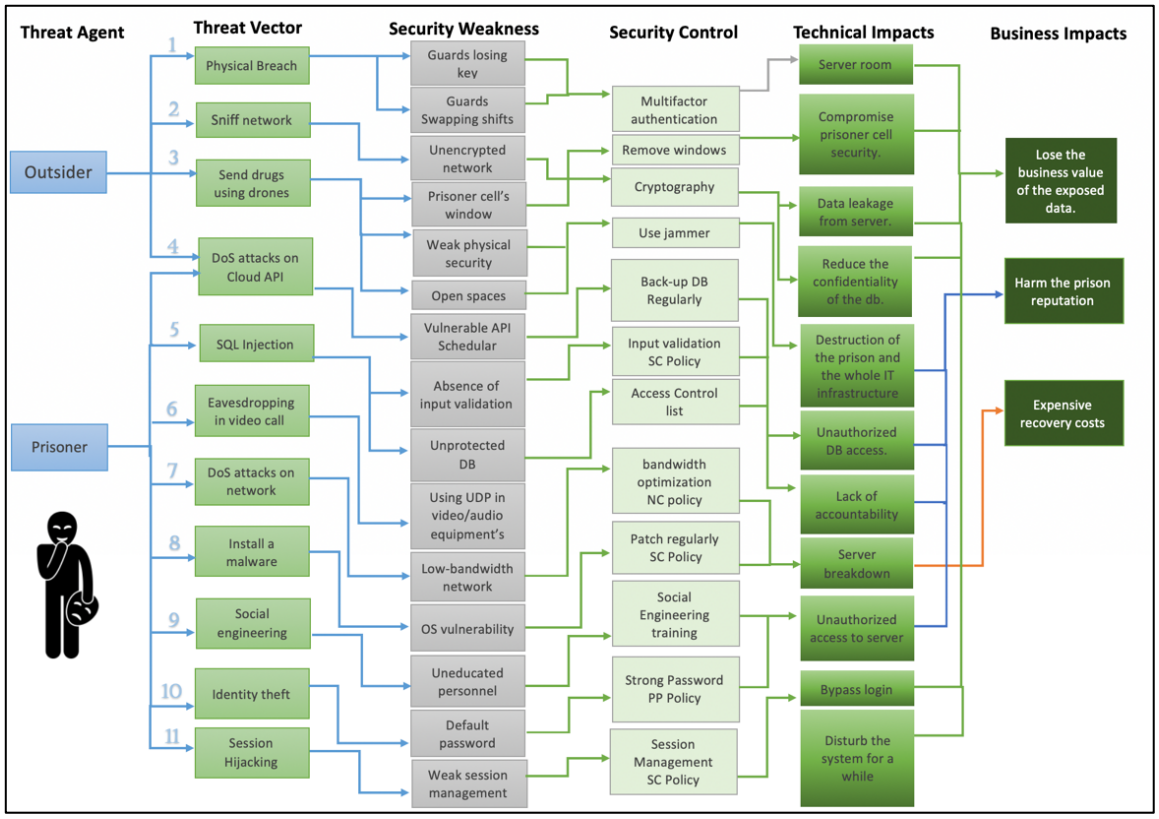

Figure 11: Threat Model with Controls

3 Performance Monitoring & Communication

There should be ongoing exchanging of information between the asset owner and risk owner. As a result, a successful agreement on the decision of how to manage the risk will be established. In addition, an ongoing monitor to ensure the prison context complies with the risk assessment outcome. This should ensure that all the policies are reviewed and enforced. Moreover, there should be internal audit planned annually to ensure that it confirms with the International Standards. Appendix F shows the statement of applicability against ISO/IES 27001 (2018). Furthermore, Figure 12 shows the status of the security controls.

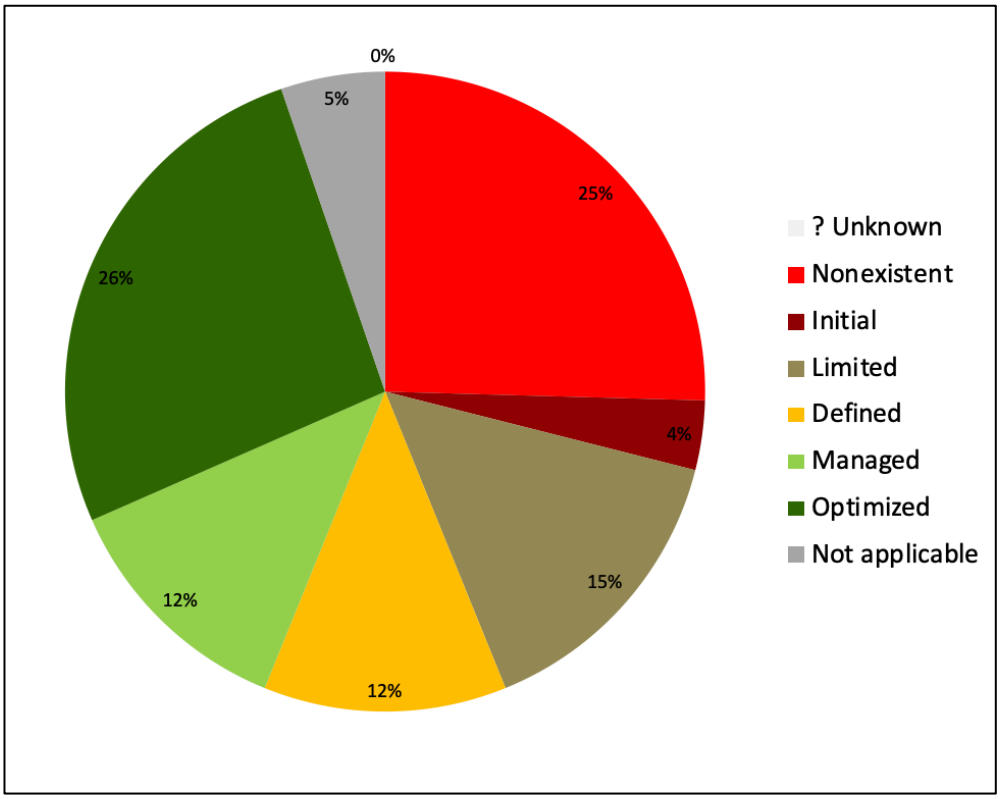

Figure 12:ISO 27001 Controls Status

Moreover, all the risks should be registered and monitored regularly. For example, table 14 shows how risk 1 and 2 were registered.

Table 14: Risk 1 and 2 Registration

Risk ID	Asset impacted	Risk Owner	Asset Owner	Risk statement	Likelihood	Impact	Risk factor	Risk control decision	Control area measures
1	DB	ISM, CISO	SMO	Unauthorized access to DB.	Almost certain	Major	Extreme Risk	Defense	A5.1.1 A10.1.1 A10.1.2 A9.2.2
2	DB	IST	SMO	• Data Leakage • Unauthorized access to DB	Almost certain	Major	Extreme Risk	Defense	A14.2.1 A14.2.8 A12.6.2 A12.1.4

4 Conclusion

To conclude, this report offers a comprehensive demonstration of the risks that come along with ACME AG innovation on HMP beechnut prison. In this report, risks were identified, the risk factor was calculated, and a decision was made to manage each risk. Furthermore, an effective DR plan was established to prevent and minimize the consequences of risk occurrence.

5 References

Bardas, A., Zomlot, L., Sundaramurthy, S., Ou, X., Rajagopalan, R. and Eisenbarth, M. (2014). Classification of UDP Traffic for DDoS Detection. In: *Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats*. San Jose: USENIX Association Berkeley.

GOV.UK. (2019). *Working for HMPS*. [online] Available at: https://www.gov.uk/government/organisations/hm-prison-service/about/recruitment. [Accessed 17 Oct. 2019].

ISO 31000. (2018)." *Risk Management. Guidelines".* International Organization for Standardization ISO. Geneve: BSI

ISO/IEC 24762. (2008)." *Information technology. Security techniques. Guidelines for information and communications technology disaster recovery services".* International Organization for Standardization ISO. Geneve: BSI.

ISO/IEC 27001. (2017)." *Information technology. Security techniques. Information security management systems. Requirements".* International Organization for Standardization ISO. Geneve: BSI.

ISO/IEC 27005. (2018)." *Information technology. Security techniques. Information security risk management".* International Organization for Standardization ISO. Geneve: BSI.

ISO/IEC 27014. (2013)." *Information technology. Security techniques. Governance of information security".* International Organization for Standardization ISO. Geneve: BSI.

Masdari, M. and Jalali, M. (2016). A survey and taxonomy of DoS attacks in cloud computing. *Security and Communication Networks*, 9(16), pp.3724-3751.

Nieles, M. Dempsey, K. Pillitteri, Y. (2017). *An Introduction to Information Security*. [online] nistspecialpublication800-12r1. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf [Accessed 17 Oct 2019].

Pietro, R., Oligeri, G. and Tedeschi, P. (2019). JAM-ME: Exploiting Jamming to Accomplish Drone Mission. In: *2019 IEEE Conference on Communications and Network Security (CNS)*. Washington DC: IEEE.

Whitman, M. and Mattford, H. (2013). *Management of information security*. 4th ed. Canada: Nelson Education.

6 APPENDICES

6.1 Appendix A: System Configuration Policy

Free Use Disclaimer: *CISO and CIO created this policy for HMP Beechnut prison for all systems. All the content of this policy could be used freely by the prison.*

Last Update Status: *1st version.*

1. Overview

Having an unsecured and vulnerable system without knowing how this system was built or designed can put the prison on excessive disclosure of data.

2. Purpose

The purpose of this policy to outline standards for the basic configuration of any system that will operate in HMP Beechnut prison. An efficient implementation of this policy will reduce the risk of unauthorized exposure or access to HMP Beechnut data and systems. Moreover, it will ensure that all the security objectives, which are confidentiality, integrity, availability, and authorization, are met.

3. Scope

This policy should be adhered by all the employees, vendors, and contractors. Besides, the policy should be applied to all the systems operated, owned, or leased by HMP Beechnut. This policy underlines specific requirements for the configuration of the system.

4. Policy

4.1 General Requirements

4.1.1 All the installed systems must be owned by a group to administrate the system.

4.1.2 For compliance, security, and maintenance reasons, authorized users should monitor the system.

4.2 Configuration Requirements

4.2.1 A proper design lifecycle approach should be used, such as agile.

4.2.2 The system should be operated in a secure environment.

4.2.3 All the ports that will not be utilized by the system must be disabled.

4.2.4 All the access to the system should be logged and protected through access control mechanisms.

4.2.5 The system should apply the least privilege and need-to-know principles.

4.2.6 The communication between the system and the server should be protected by an TLS\SSL channel.

4.2.7 Restrict the installation of a software to the system owner.

4.2.8 The system should be tested before installing it.

4.3 Confidentiality Requirements

4.3.1 All the data stored for the system must be encrypted.

4.4 Integrity Requirements

4.4.1 All the data should be hashed.

4.5 Availability Requirements

4.5.1 The availability ensured as long as the system is installed, connected to the internet, and the users have a connection to the system's database.

4.6 Authentication Requirements

4.6.1 All the inputs should pass through a validation process to prevent SQL injection and Cross-site scripting.

4.6.2 There should be precise session management to prevent session hijacking.

4.6.3 All the passwords should adhere to the password protection policy.

4.7 Monitoring

4.7.1 All the security events, such as authentication, should be logged and should be reviewed by the CISO. Security events could be:

- Unauthorized login attempts
- Vulnerability scanning

4.7.2 Penetration tests should be carried out regularly to determine the system's security efficiency.

5. Policy Compliance

5.1 Compliance Measurement

Policy compliance will be verified through internal and external audits and feedback to the owner of this policy.

5.2 Non-Compliance

Any employee who violates this policy might be exposed to penalization action.

6. Related Standards, Policies, and Processes

- Password Protection Policy.

7. Definitions and Terms

None.

8. Revision History

No revision, 1st version.

6.2 Appendix B: Network Configuration Policy

Free Use Disclaimer: *CISO and NSM created this policy for HMP Beechnut prison specified for networks. All the content of this policy could be used freely by the prison.*

Last Update Status: *1st version.*

1. Overview

Vulnerable network configuration can lead to an excessive number of malicious acts.

2. Purpose

The purpose of this policy is to certify that all the network devices are appropriately configured to ensure that all the information asset's confidentiality, integrity, and availability are assured during network transmission.

3. Scope

This policy applies to all the network devices within HMP Beechnut prison. In addition, all employees, agents, contractors, and providers must adhere to this policy when providing a new network device.

4. Policy

4.1 General Requirements

4.1.1 Any network device that exists in HMP Beechnut prison should pass through the following:

- Installed, configured, and maintained by a qualified network technician.
- Use Cryptography.
- Maintain a fixed MAC address that can be logged.
- The device should be protected by a password that follows the password protection policy.
- The password should be maintained in an encrypted form.
- Telnet service should be disabled.
- The network should be monitored regularly to ensure proper bandwidth optimization.
- There should be a firewall placed between the internal and external network to prevent any suspicious packets.

4.1.1.9 There should be a Network Intrusion Detection System NIDS within the internal network.

5. Policy Compliance

5.1 Compliance Measurement

The compliance of this policy may be verified by monitoring the network and establishing reports.

5.2 Non-Compliance

Any personnel who violate this policy could be exposed to penalties.

6. Related Standards, Policies, and Processes

- Password policy protection.

7. Definitions and Terms

None.

8. Revision History

No revision, 1st version.

6.3 Appendix C: Server Configuration Policy

Free Use Disclaimer: *CISO and CIO created this policy for* HMP Beechnut *prison's internal server. All the content of this policy could be used freely by the prison.*

Last Update Status: *1st version.*

1. Overview

A significant entry point to various threats is a vulnerable server.

2. Purpose

The policy intends to minimize the threats against the internal server by outlining standards to act as a baseline while maintaining internal server security.

3. Scope

This policy should be adhered by all the employees, vendors, and contractors of servers.

4. Policy

4.1 General Requirements

4.1.1 The server should be registered in the prison system, including the following information:

- Server administrator
- Hardware version
- Operating System version
- Server main functionality

4.2 Configuration Requirements

4.2.1 Any services that will not be utilized must be disabled.

4.2.2 There should be a prober access mechanism to ensure all the access is logged and tracked.

4.2.3 Any recent OS patches should be installed on the server.

4.2.4 Authorized access should be authenticated over a secure channel.

4.2.5 The server should be located in a secure room.

4.2.6 All the removeable media ports should be disabled and closed.

4.3 Monitoring

4.3.1 All the physical access to the server room should be monitored and logged.

4.3.2 All the logs should be protected from unauthorized access and controlled by an administrator.

4.3.3 Ensure no port scanning implemented to the server.

5. Policy Compliance

5.1 Compliance Measurement

The responsible team could ensure compliance with the policy by internal and external audits and monitoring the access to the server physically.

5.2 Non-Compliance

Any personnel who violate this policy could be exposed to penalties.

6. Related Standards, Policies, and Processes

None.

7. Definitions and Terms

None.

8. Revision History

No revision, 1st version.

6.4 Appendix D: Password Protection Policy

Free Use Disclaimer: *CISO and CIO created this policy for HMP Beechnut prison. All the content of this policy could be used freely by the prison.*

Last Update Status: *1st version.*

1. Overview

The use of weak or default passwords can be the entry point for different threat actors. Thus, all the employees, contractors, vendors who have access to HMP Beechnut prison systems should take further steps while selecting their passwords.

2. Purpose

This policy outlines a standard for developing and maintaining strong and secure passwords.

3. Scope

This policy implies to all the personnel who have access to prison systems, networks, and facilities.

4. Policy

4.1 Password development

4.1.1 All users should use a unique password for each system.

4.1.2 The password should contain at least eight characters.

4.1.3 The characters should include capital-lower letters, numbers, special symbols.

4.2 Password Change

4.2.1 The password should be changed every 90 days.

4.3 Password Protection

4.3.1 Passwords must not be written down in any notes.

4.3.2 Passwords should not be shared with anyone.

4.3.3 Passwords must be stored in a secure form “Hash”.

4.4 System Development

4.4.1 The systems should not store or transmit the passwords in cleartext.

4.5 Multi-Factor Authentication

4.5.1 A Multi-factor authentication should be considered whenever and wherever it is possible.

5 Policy Compliance

5.1 Compliance Measurement

The responsible team could ensure compliance with the policy by internal and external audits.

5.2 Non-Compliance

Any personnel who violate this policy could be exposed to penalties.

6 Related Standards, Policies, and Processes

None.

7. Definitions and Terms

None.

8. Revision History

No revision, 1st version.

6.5 Appendix E: Disaster Recovery Plan

Introduction

This document is a disaster recovery plan (DRP) for HMP Beechnut prison. It includes procedures and practices needed to limit the corruption to the prison assets from a human-made or natural hazard.

Version Information & changes

Any foreseeable changes of this DRP should be recorded in table 15.

Table 15: DRP Version

Role	Data of change	Version Number	Notes
DRP leader	22/10/19	1.0	First version of DRP

Policy statement

The prison should implement a disaster recovery plan should include all the following process:

- Information on when, how, and who should be contacted?
- Information on where, how, and which data should be backed up?
- Information on how and when the data can be recovered from a disaster?
- It should cover all the critical prison hardware, software, and networks.
- It should include all the staff roles and responsibilities.
- A periodic test of the DRP should be implemented, and a results report should be submitted.
- The DRP should be periodically reviewed and updated.
- The DRP should maintain up to date information.

Objective

The primary objective behind implementing an independent disaster recovery plan is to develop and document an easily understood plan which will support the prison to recover effectively from an unforeseeable disaster. Besides, the main objective of DRP is to mitigate all the consequences of a disaster. This plan highlights the need to have an off-site location.

Scope

The scope of the prison DRP consider all the following aspects:

- Database.
- Network connectivity.
- Internal server.
- Video/audio system.
- Backup systems.

Internal Contact info

Table 16:Internal Contact Information

Position	Contact Number
CEO	-
COO	
CIO	
CFO	
CISO	
POS	
IE	

SAO	
POO	
ISM	
AA	
PSO	
NSM	
ISA	
IST	
NT	

External Contact info

Table 17: External Contact Information

Name	Contact Number
UK Government	-
Social Research Center	
Nation X	

DRP team Teams & Responsibilities

On the occasion of a disaster, a variety of personnel will be essential in the process of supporting the IT facilities to be restored to its usual functionalities. The different personnel are the following:

- Disaster Recovery Lead
  - He/she is the decision-maker to anything related to the DRP.
  - Monitor the process of DR.
- Disaster Manager
  - He/she should be the first person who should take action on the occasion of a disaster.
- Network Manager
  - He/she is accountable for evaluating the damage caused by a disaster to the network connectivity.
- Server Manager
  - He/she is accountable for evaluating the damage caused by a disaster to the server.
  - Re-start the server if necessary.
- System Manager
  - He/she is accountable for ensuring that all the prison systems function as required during and after a disaster.

Emergency services information

Table 18: Emergency Services Information

Name	Phone number
Police	999,112
Ambulance	
Fire	
Insurance agency	-
Cloud provider	
Internet service provider (ISP)	

Video/audio equipment's supplier		
HVAC supplier		
Electricity supplier		
Off-site storage	Account number	*******
	User ID	*******
	Password	*******

Backup strategy

All the information assets and their back-up strategy are listed in table 19 below. A fully mirrored recovery site has been chosen as the back-up strategy because the disruption of one of these assets has a significant impact on the prison. This strategy allows protecting the process by having a duplicate site that enables a prompt transferring from the live site to the back-up site. Although the DB stored in the cloud, there is a significant need to have a back-up image in the event of cloud failure.

Table 19: Back-up Strategy

Information Asset	Asset Classification	Backup strategy	Role	Backup frequency
DB	Confidential	Fully mirrored off-site	Disaster Manager	12:00 AM every day Daily backups are copied to external hard desk and transferred to an off-site weekly.
Internal Server	Confidential	Fully mirrored off-site	Server Manager & Network Manager	
Visual system	Internal	Fully mirrored off-site	System Manager	

Alternate site

In the event of a disaster, there should be a hot site equipped with the necessary facilities, hardware, and software for the prison to proceeds with their functions. A hot site has been chosen since HMP Beechnut prison is class B prison and needs to occupy the prisoner as soon as possible after a disaster. This site should be in a zone with great accessibility to help in moving the prison faster.

Threat assessment

Table 20 shows the threats to the prison functions and activities.

Table 20: DR Threat Assessment

	Disaster scenario		Likelihood (1-5)	Impact (1-5)	Consequences/ Remedial Action
1	Natural	Unable to access the prison due to fire, flood instantaneously but **can be** accessed in the next 48hr.	3	3	Only 1st floor equipment's will be destroyed. A fire and smoke detectors are installed on all floors.
2		Unable to access the prison due to Tornado, electrical storms	4	5	

		instantaneously and **cannot** be accessed in the next 48hr.			
3		Power failure	3	2	An auto standby power generator is installed.
4	Human-made	Serious information security incidents.	1	4	
5		Prisoner escape	2	5	
Likelihood: 1= very low, 5=very high				Impact: 1=low impact, 5= high impact	

Risk assessment

The risks have been classified based on table 21.

Table 21: DR Risk Assessment Classification

Likelihood	**1- Low** **2- Medium** **3- High**
Impact	1- Low 2- Medium 3- High
Total	Likelihood X Impact
Category	1-2 Low 3-4 Medium 5-6 High

From the previous threat assessment, table 22 shows the risks identified after those threats.

Table 22: DR Risks Identified

Risk	Likelihood	Impact	Total	Category
Complete building loss	1	3	3	Medium
Internal Server failure	2	3	6	High
Visual system failure	1	2	2	Low
Website system failure	2	2	4	Medium
Internet connectivity failure	1	3	3	Medium
Prisoner escape	2	3	6	Medium

Disaster recovery procedure

On the occurrence of any disaster, these three steps are implemented immediately:

- The DR team should be notified by using their contact numbers.
- DR lead should activate the DRP.
- If one of them is not available, then there should be an alternative person from the contact list.

Scenario 1&2: Unable to access the prison due to fire, flood instantaneously but can be or cannot be accessed in the next 48hr.

Assembly Points

- If the fire requires the site to be evacuated, then these two are the assembly points:
- Primary: the parking of the prison
- Secondary: the parking of the opposite building.
- If the disaster required the attendance of fire personnel, then permission should be gained from the authority to enter the site.
- All the equipment should be checked and tracked against the asset inventory. Any lost equipment should be recorded.

Table 23 indicate the recovery procedure if the network was intact or not.

Table 23: Recovery Procedure

Responsible	Network is intact	Responsible	Network is not intact
Server Manager	Should check all the connections to and from the internal server.	Network Manager	Should notify the DR team and the network connectivity vendor.
System Manager	Should ensure no further updating of data in all the prison systems and DB.	Network Manager	Should check any alarms produced by the Intrusion detection system, if any.
DR team	The hot site of the prison will be activated.		
DR team	A standby of specific hardware or software must be installed.		
DR team	A back-up restore must be carried out from the most recent file.		
System Manager	All systems or hardware users must be informed on the back-up information.		
DRT	All users should confirm that the hardware/software function as expected.		
DRT	Once the hardware/software is available, all the users are requested to change their password immediately.		
Disaster Recovery Manager	All the checklists should be checked to ensure proper completion of the DR procedure.		
DR team	Encase the prison can be accessed after 48hr, then users should guide all the personnel to the prison.		

Scenario 3: Power failure

- The DR manager will ensure that the standby generator is turned on.
- The network manager should ensure that internet connectivity operated as required.
- The system manager must ensure and document all the system losses to the DR manager.
- The server manager must ensure that the internal server is back on the operation as expected.

Scenario 4: Serious information security incidents

- The system manager will prompt the users to log out immediately from the system.
- The network manager will check the Intrusion detection system to determine the incident originator.
- The system manager must restore the system from the most current backup.
- Require all the users to change their passwords instantaneously.

Scenario 5: Prisoner escape

Table 24 shows the procedure if a prisoner escape.

Table 24: Escape Procedure

Responsible	Successful escape	Unsuccessful escape
Movement detection alert starts.		
DR leader	Force some of the Physical security officers (PSO) and physical operation officers (POO) to search throughout the prison physical boundary.	
PSO	Search throughout the prisoner's cells.	
PSO	Watchtower should search throughout all the prison internally and externally.	
DR leader	Inform the HM prison service.	
POO	Check the CCTV system.	
DR Manager	Check any missing assets.	
DR leader	Move the case to HM office	Move escaped prisoners to solitary confinement.

Plan Testing & Maintenance

This document is an initial DRP which requires a decent test in order to tackle all the possible concerns that may occur.

Maintenance

Any significant update or upgrade on the system must perceive it as a reason to update the DR plan. The DR lead will be accountable for updating the entire DR plan. Thus, he will have the right to request as much information as required to do so.

Maintenance of the DR plan includes:

- Up-to-date DR team list.
- All the DR plan procedures must be appropriate to implement in prison.
- Any change in the prison objective, goals, or vision should be reflected in DRP.
- The DR plan should satisfy all the law's requirements.
- If one of the DR team quits, then the DR lead should point out a new member for the DR team.

Testing

To ensure that the DR plan is practical, the implementation of the DR plan test should be in place. This test passes through two phases to ensure that the DR plan is still valid. Testing will include the following:

Phase one: weekly DR plan rehearsal

It requires all the DR team members to go through all the documented procedures verbally, identify possible gaps and weaknesses in the plan. This provides a revision of the plan with different people, which allows the DR leader to implement changes on the plan.

Phase two: monthly failover testing

All the systems and the internal server are brought in an isolated environment. Hence, there will be no impact on the functionality of the prison. This test will ensure the following:

- The system manager should ensure effective system operation.
- The network manager must ensure that the network connectivity is operated as expected.
- The server manager must ensure that the internal server is secured from any physical interruption.
- The DR team should ensure that DR team followed the procedure by using the checklist as shown in table 25.

Table 25: DR Checklist

	Procedure	Y/N	Notes
1	Have the DR team been contacted?	Y/N	
2	Has permission been established to firemen if needed?	Y/N	
2	Did all the equipment's have been checked against asset inventory?	Y/N	
3	Is there any lost or damaged asset?	Y/N	
4	Have the systems restored completely?	Y/N	
5	Have all the users been notified about the points of the system been restored	Y/N	
6	Confirmation that no further updating after the occurrence of a disaster.	Y/N	
7	Did all the users passwords changed?	Y/N	
8	Have the DR team identified the originator?	Y/N	
9	Check if all the systems and hardwires are operational as expected.	Y/N	
10	Check if all the prisoners are in their cells	Y/N	

- The fire and smoke detectors are tested weekly. Besides, there will be monthly evacuation to the assembly points.
- The standby power generated must be tested weekly.

Any weaknesses discovered through one of these phases should be reflected in the DR plan by the DR lead.

6.6 Appendix F: Statement of Applicability

Table 26: Statement of Applicability

Section	Information security control	Status	Notes
A5	**Information security policies**		
A5.1	**Management direction for information security**		
A5.1.1	Policies for information security	Defined	
A5.1.2	Review of the policies for information security	Defined	
A6	**Organization of information security**		
A6.1	**Internal organization**		
A6.1.1	Information security roles and responsibilities	Optimized	
A6.1.2	Segregation of duties	Optimized	
A6.1.3	Contact with authorities	Optimized	
A6.1.4	Contact with special interest groups	Initial	
A6.1.5	Information security in project management	Defined	
A6.2	**Mobile devices and teleworking**		
A6.2.1	Mobile device policy	Not applicable	
A6.2.2	Teleworking	Not applicable	
A7	**Human resource security**		
A7.1	**Prior to employment**		
A7.1.1	Screening	Not applicable	
A7.1.2	Terms and conditions of employment	Not applicable	
A7.2	**During employment**		
A7.2.1	Management responsibilities	Optimized	
A7.2.2	Information security awareness, education and training	Managed	
A7.2.3	Disciplinary process	Initial	
A7.3	**Termination and change of employment**		
A7.3.1	Termination or change of employment responsibilities	Not applicable	
A8	**Asset management**		
A8.1	**Responsibility for assets**		
A8.1.1	Inventory of assets	Optimized	
A8.1.2	Ownership of assets	Optimized	
A8.1.3	Acceptable use of assets	Limited	
A8.1.4	Return of assets	Not applicable	
A8.2	**Information classification**		
A8.2.1	Classification of information	Optimized	
A8.2.2	Labelling of information	Initial	
A8.2.3	Handling of assets	Managed	
A8.3	**Media handling**		
A8.3.1	Management of removable media	Defined	
A8.3.2	Disposal of media	Nonexistent	
A8.3.3	Physical media transfer	Nonexistent	
A9	**Access control**		
A9.1	**Business requirements of access control**		
A9.1.1	Access control policy	Defined	
A9.1.2	Access to networks and network services	Optimized	
A9.2	**User access management**		
A9.2.1	User registration and de-registration	Limited	
A9.2.2	User access provisioning	Optimized	
A9.2.3	Management of privileged access rights	Defined	
A9.2.4	Management of secret authentication information of users	Limited	
A9.2.5	Review of user access rights	Nonexistent	
A9.2.6	Removal or adjustment of access rights	Nonexistent	
A9.3	**User responsibilities**		
A9.3.1	Use of secret authentication information	Managed	
A9.4	**System and application access control**		
A9.4.1	Information access restriction	Optimized	
A9.4.2	Secure log-on procedures	Limited	
A9.4.3	Password management system	Optimized	

A9.4.4	Use of privileged utility programs	Limited	
A9.4.5	Access control to program source code	Nonexistent	
A10	**Cryptography**		
A10.1	**Cryptographic controls**		
A10.1.1	Policy on the use of cryptographic controls	Optimized	
A10.1.2	Key management	Nonexistent	
A11	**Physical and environmental security**		
A11.1	**Secure areas**		
A11.1.1	Physical security perimeter	Optimized	
A11.1.2	Physical entry controls	Optimized	
A11.1.3	Securing offices, rooms and facilities	Optimized	
A11.1.4	Protecting against external and environmental threats	Optimized	
A11.1.5	Working in secure areas	Optimized	
A11.1.6	Delivery and loading areas	Optimized	
A11.2	**Equipment**		
A11.2.1	Equipment siting and protection	Defined	
A11.2.2	Supporting utilities	Managed	
A11.2.3	Cabling security	Nonexistent	
A11.2.4	Equipment maintenance	Nonexistent	
A11.2.5	Removal of assets	Nonexistent	
A11.2.6	Security of equipment and assets off-premises	Not applicable	
A11.2.7	Secure disposal or reuse of equipment	Nonexistent	
A11.2.8	Unattended user equipment	Limited	
A11.2.9	Clear desk and clear screen policy	Nonexistent	
A12	**Operations security**		
A12.1	**Operational procedures and responsibilities**		
A12.1.1	Documented operating procedures	Optimized	
A12.1.2	Change management	Limited	
A12.1.3	Capacity management	Nonexistent	
A12.1.4	Separation of development, testing and operational environments	Optimized	
A12.2	**Protection from malware**		
A12.2.1	Controls against malware	Optimized	
A12.3	**Backup**		
A12.3.1	Information backup	Optimized	
A12.3	**Logging and monitoring**		
A12.4.1	Event logging	Optimized	
A12.4.2	Protection of log information	Limited	
A12.4.3	Administrator and operator logs	Limited	
A12.4.4	Clock synchronisation	Nonexistent	
A12.5	**Control of operational software**		
A12.5.1	Installation of software on operational systems	Defined	
A12.6	**Technical vulnerability management**		
A12.6.1	Management of technical vulnerabilities	Optimized	
A12.6.2	Restrictions on software installation	Optimized	
A12.7	**Information systems audit considerations**		
A12.7.1	Information systems audit controls	Limited	
A13	**Communications security**		
A13.1	**Network security management**		
A13.1.1	Network controls	Managed	
A13.1.2	Security of network services	Managed	
A13.1.3	Segregation in networks	Managed	
A13.2	**Information transfer**		
A13.2.1	Information transfer policies and procedures	Nonexistent	
A13.2.2	Agreements on information transfer	Nonexistent	
A13.2.3	Electronic messaging	Nonexistent	
A13.2.4	Confidentiality or nondisclosure agreements	Optimized	
A14	**System acquisition, development & maintenance**		
A14.1	**Security requirements of information systems**		
A14.1.1	Information security requirements analysis and specification	Nonexistent	

A14.1.2	Securing application services on public networks	Limited	
A14.1.3	Protecting application services transactions	Limited	
A14.2	**Security in development and support processes**		
A14.2.1	Secure development policy	Optimized	
A14.2.2	System change control procedures	Nonexistent	
A14.2.3	Technical review of applications after operating platform changes	Nonexistent	
A14.2.4	Restrictions on changes to software packages	Defined	
A14.2.5	Secure system engineering principles	Managed	
A14.2.6	Secure Development Environment	Limited	
A14.2.7	Outsourced development	Managed	
A14.2.8	System security testing	Defined	
A14.2.9	System acceptance testing	Defined	
A14.3	**Test data**		
A14.3.1	Protection of test data	Nonexistent	
A15	**Supplier relationships**		
A15.1	**Information security in supplier relationships**		
A15.1.1	Information security policy for supplier relationships	Nonexistent	
A15.1.2	Addressing security within supplier agreements	Nonexistent	
A15.1.3	ICT supply chain	Nonexistent	
A15.2	**Supplier service delivery management**		
A15.2.1	Monitoring and review of supplier services	Nonexistent	
A15.2.2	Managing changes to supplier services	Nonexistent	
A16	**Information security incident management**		
A16.1	**Management of information security incidents & improvements**		
A16.1.1	Responsibilities and procedures	Optimized	
A16.1.2	Reporting information security events	Optimized	
A16.1.3	Reporting information security weaknesses	Limited	
A16.1.4	Assessment of and decision on information security events	Managed	
A16.1.5	Response to information security incidents	Optimized	
A16.1.6	Learning from information security incidents	Defined	
A16.1.7	Collection of evidence	Not applicable	
A17	**Information security aspects of BCM**		
A17.1	**Information security continuity**		
A17.1.1	Planning information security continuity	Limited	
A17.1.2	Implementing information security continuity	Limited	
A17.1.3	Verify, review and evaluate information security continuity	Initial	
A17.2	**Redundancies**		
A17.2.1	Availability of information processing facilities	Limited	
A18	**Compliance**		
A18.1	**Compliance with legal and contractual requirements**		
A18.1.1	Identification of applicable legislation and contractual requirements	Nonexistent	
A18.1.2	Intellectual property rights	Nonexistent	
A18.1.3	Protection of records	Managed	
A18.1.4	Privacy and protection of personally identifiable information	Managed	
A18.1.5	Regulation of cryptographic controls	Defined	
A18.2	**Information security reviews**		
A18.2.1	Independent review of information security	Defined	
A18.2.2	Compliance with security policies and standards	Managed	
A18.2.3	Technical compliance review	Managed	