T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Cyber Security

Assignment 3 – Distinction

Guide standard exemplification materials (GSEMs)

v1.0: Specimen assessment materials
31 August 2023
603/6901/2

Internal reference: DSS-GSEM-19

T Level Technical Qualification in Digital Support Services
Occupational specialism assessment (OSA)

Cyber Security

Guide standard exemplification materials (GSEMs)

Assignment 3

Contents

Introduction

The material within this document relates to the Cyber Security occupational specialism sample assessment. These exemplification materials are designed to give providers and students an indication of what would be expected for the lowest level of attainment required to achieve a pass or distinction grade.

The examiner commentary is provided to detail the judgements examiners will undertake when examining the student work. This is not intended to replace the information within the qualification specification and providers must refer to this for the content.

In assignment 3, the student must perform a security risk assessment on the site and network, recommending physical, administrative and technical controls.

Write an information security policy document, considering the kinds of controls that should be included in an information security policy.

Create a report to recommend a range of actions that could be taken to provide disaster recovery support from a service outage due to denial of service (DoS) attacks, whilst protecting systems and data, to support a network recovered and be fully operational within 3 days of a major disaster.

After each live assessment series, authentic student evidence will be published with examiner commentary across the range of achievement.

Assignment 3

Task 1: security risk assessment

Time limit

2 hours 30 minutes

You can use the time how you want but all parts of the task must be completed within the time limit.

Your manager has asked you to undertake a risk assessment and validate the company's network with regards to cyber security.

(30 marks)

Instructions for students

To help you complete this task a breakdown of the current company infrastructure and security measures has been provided in the additional document ('Company overview'). You will need to refer to this document throughout the task.

Your manager has asked you to evaluate the network with regards to cyber security to ensure that company resources and data are fully protected.

Perform a security risk assessment on the site and network, recommending physical, administrative and technical controls. Explain why your recommendations will protect the network.

Using the provided risk assessment template, you should undertake your risk assessment.

You should consider:

- the information provided in the company overview document
- the security on the servers and computers
- security risks that could occur because of lack of auditing/monitoring
- prioritisation of the remediation actions
- potential impact of damage
- RAG rate – low, medium or high rating

You will have access to the following:

- word processing software
- the internet
- risk assessment template (more lines can be added as required)

Evidence required for submission to NCFE

- completed risk assessment template

Student evidence

Task 1: Risk Assessment

Please find the risk assessment below.

ID	Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Action	Control type
1	Unlocked main gate	There is a risk that unauthorised access to the office could be obtained by a threat actor.	Office	High	Medium	Medium	Secure main gate with access control, this could be a barrier with swipe card access control and/or security guard/car park attendant.	Preventative Unrestricted external access could allow unauthorised people access to the office.
2	Use of dummy CCTV cameras	There is a risk that only using dummy CCTV cameras would result in no evidence of any incident.	Office	Medium	Medium	Medium	Purchase and installs CCTV cameras for all entrances as a minimum.	Preventative Although dummy CCTV cameras can be a deterrent, they lack CCTV footage should an incident occur.
3	Access to anyone from the car park as it is a thoroughfare	There is a risk that unauthorised access will be	Office	Medium	Medium	Medium	Covered by securing main gate, this could be a barrier with swipe card access control	Preventative Allowing through access increases footfall which in turn

		gained from the car park.					and/or security guard/car park attendant.	increases the possibility of unauthorised access.
4	Unlocked main entrance	There is a risk that an unsecured main entrance could afford unauthorised access especially as the reception is only manned part time.	Office	Medium	High	Medium	Install access control on main entrance, for example key card and / or swipe access or biometric	Preventative Unsecured access and lack of a full-time receptionist could allow unauthorised access.
5	Additional access for workers not controlled and gives access to hot desk area	There is a risk that having no access control of the additional access could allow unauthorised access to the hot desk area.	Office	Medium	High	Medium	Access control for additional access, for example key card and / or swipe access or biometric	Preventative Uncontrolled access could result in a threat actor gaining access to the hot desk area.
6	Fire door left open to cool	There is a risk that leaving the fire door open not only gives unauthorised access to the building but also the server room.	Office	Medium	Medium	Medium	Alarm for fire door and not to be left open.	Preventative Unmonitored, open access to any area is not a good idea.

7	No entrances alarmed	There is a risk that lack of alarms on entrances could result in unauthorised entry when entrances are not being controlled by staff.	Office	Medium	High	Medium	Look at a burglar/fire alarm system to cover all areas including window and door sensors.	Deterrent As entrances have no CCTV and are not monitored some form of alarm is needed to indicate unauthorised access.
8	Open windows not closed and have been occasionally left open throughout the night	There is a risk that windows being open outside of operational hours could result in unauthorised access.	Office	High	High	High	Covered in risk 7 above relating to an alarm system, also potentially window locks.	Deterrent Windows open when no one is on premise is an easy ingress point for a thief.
9	Part-time reception	There is a risk that only having reception manned part time throughout operational hours could result in unauthorised access.	Office	Medium	Medium	Medium	Look at either having reception manned during business hours or installing an access control system with intercom.	Corrective

10	Reception computer logged in	There is a risk that leaving the reception computer logged on could result in unauthorised access to IT resources. This is exacerbated by the fact all users have admin access.	Office	High	High	High	Always log out of system, look at auto screen lock.	Preventative
11	Server room single point of failure	There is a risk that having all server and IT infrastructure linked to a single server room could result in extended downtime if the server room suffered a catastrophic event such as flood or fire.	IT infrastructure	High	High	High	Provision another server area in a separate part of the building.	Corrective

12	Single servers no redundancy	There is a risk that having single servers for key business applications and services such as File and Print could result in extended downtime of that service should a server fail.	IT infrastructure	High	High	High	Look at disaster recovery (DR)/failover for the servers either physical or cloud.	Corrective
13	Network ports locked?	There is a risk that having network ports available in the hot desk area could allow a threat actor to connect their own device and compromise the network.	IT infrastructure	Medium	Medium	Medium	Disable unused network ports.	Preventative
14	Public wireless access password protected	There is a risk that provisioning public wireless with no login credential required could allow a threat actor	IT infrastructure	Medium	Medium	Medium	Protect public wireless with a password.	Preventative

		inside or outside the building to connect and compromise the network.						
15	Joiner’s process – no leavers process	There is a risk that having no movers and leavers process could result in staff who move or leave having access to areas they should not have access to.	IT infrastructure	Medium	Medium	Medium	Look at creating a joiners/movers/leavers policy covering return of assets and removal of system access for movers/leavers.	Corrective
16	No mention of an asset register	There is a risk that the lack of an asset register could result in equipment not being returned and/or being stolen.	IT infrastructure	Low	Low	Low	Create an asset register containing a minimum of asset description, serial number, assigned to, and date assigned.	Corrective An asset register would ensure all assets were recorded along with current owner.
17	Policies	There is a risk that the lack of any IT policies could result in staff behaving	Staff	Medium	Medium	Medium	Create an IT policy along with any ancillary policies, for example, internet usage.	Corrective Format IT policies help to ensure staff

		inappropriately, impacting company reputation.						are aware of do's and don't's.
18	ID badges	There is a risk that not mandating the wearing of ID badge in the office could result in unauthorised people gaining access to the office and any assets including customer information.	Staff	Low	Low	Low	Make wearing an ID badge in the office mandatory and coach staff to challenge anyone not wearing a badge.	Corrective With a small team individuals know each other but as the team grows ID badges ensure anyone on premise is identified and unauthorised personnel are also identified.
19	Access to cloud areas from personal devices	There is a risk that allowing staff to access cloud systems from home via personal devices could result in company data loss.	Staff	High	High	High	Look at restricting cloud access to genuine company issued devices.	Corrective Cloud access from non-company-controlled devices is a high risk as the devices used may not have anti-virus installed.

20	Full data backups – are there incremental backups?	There is a risk that not having full incremental backup could result in data being irretrievably lost if deleted or the subject of an attach such as ransomware.	Data	Medium	Medium	Medium	Promote movement of data to the cloud and for data that must be stored onsite implement cloud backup.	Corrective Backups are an important defence against ransomware so frequent backups (daily as a minimum) would protect against this.
21	Lack of a password policy	There is a risk that having no password guidelines or enforced policy on content or length could result in staff setting insecure passwords that could be cracked. This is especially so if the staff member has cloud access.	Security	Medium	Medium	Medium	Create password policy on the system to force password length and change of password regularly.	Corrective Complex passwords should be mandatory as tools like Mimikatz make password cracking easy if passwords are not complex. In addition, passwords should be changed at least every 90 days.

22	Local admin risk	There is a risk that allowing local admin access to staff could allow them to install malware, install unauthorised applications and download data.	Security	High	High	High	Remove local admin access for all staff except IT-provision of laptops with a standard image containing only authorised software.	Corrective Local admin rights give the user (and any software they run) the ability to do anything on the system. This includes the inadvertent execution of a virus.
23	Lack of anti-virus	There is a risk that the lack of antivirus could result in assets being compromised by malware and potentially ransomware.	Security	High	High	High	Purchase and install anti-virus on all endpoints.	Corrective Lack of anti-virus could allow multiple attack vectors including ransomware.
24	Lack of firewall	There is a risk that the lack of a firewall could allow unauthorised access to systems such as external file-share, external email. In addition,	Security	High	High	High	Install a firewall to protect the internal IT network and control external access.	Preventative Lack of ingress/egress controls can result in data loss.

		a lack of a firewall would make compromise of the on-site systems much easier.						
25	Mobile phones unrestricted	There is a risk that having unrestricted mobile devices could not only allow staff to download and install malware but could also compromise company data. In addition, if a device was lost whoever found it would have access to all data.	Security	Medium	Possible	Medium-High	Look at provisioning phones with an endpoint security solution such as Intune.	Preventative An unrestricted mobile device with access to corporate systems and data could allow a threat actor to breach the network and steal data.

26	No role-based access control (RBAC) – staff have access to everything	There is a risk that not enforcing a RBAC policy could allow staff access to data they should not be allowed to see.	Security	Medium	Medium	Medium	Ensure roles exist for all staff and align with the lowest privilege permissions required for the role. Use this as a RBAC template and ensure staff are assigned roles on joining and moving.	Corrective It is important to ensure anyone with an admin role cannot mix this with another role to compromise systems. For example. a database administrator who has access to a finance system front-end and back-end could enter a transaction in the front-end and change the figure in the database.
27	No ticketing system	There is a risk that not employing an IT ticketing system will result in full details of any issue not being recorded or resolved in a timely manner. It will also result in	All	Low	Low	Low	Implement a basic IT ticketing system to allow the recording of incidents and their remediation.	Corrective Incidents should be recorded to ensure remediation actions can be investigated to see whether a policy or procedure needs changing. Also, there could be a root cause that, if

		an inability to conduct any kind or root cause analysis or identify common issues.						remediated, would prevent multiple incidents occurring again.
28	No mandatory training	There is a risk that not requiring staff to attend/complete mandatory training could result in then not following company policy. It could also result in an inability to discipline any staff who contravened any guidelines.	Staff	Medium	Medium	Medium	Pull together a set of mandatory training either face-to-face or virtual, and ensure all staff complete the training and this is noted on their HR record.	Corrective For audit purposes and to ensure staff are aware of their responsibilities, there should be proof that they have read and understood IT policies.
29	Rise in cyber attacks	There is a risk that a rise in cyber attacks has occurred as threat actors have identified the company as an easy target due to lack of firewall and other controls.	Security	High	High	High	Implement a firewall as per risk 24.	Preventative Aligned with other issues, this is a very high risk; threat actors perform initial scanning and then intensify if they see a potential threat vector.

30	No 2-factor authentication (2FA)	There is a risk that not mandating 2FA, especially for cloud services, could result in accounts being compromised by phishing and other means.	Security	Medium	High	High	Look into implementing 2FA especially for cloud-based systems.	Preventative Phishing/vishing can give a threat actor login and password details, aligned with cloud access this is a high risk. Mandating 2FA protects against this as the threat actor will not have the physical device to enter the additional code to gain access.
31	3 days operational after incident	There is a risk that the required return to normal operations within 3 days of a major incident cannot be achieved with the current setup.	DR	High	High	High	Look at creating a disaster recovery plan aligned with the 3-day downtime limit, including recovery time objective (RTO) and recovery point objective (RPO).	Corrective If access is needed within 3 days there should be measures in place to ensure this, currently there are not.

32	Server room next to fire exit that is left open	There is a risk that the server room is at risk as the fire exit next to it is left open on hot days due to lack of air conditioning.	IT infrastructure	High	High	High	Install air conditioning on the server room and access control.	Corrective The server room is the main data store; a compromise of the server room would be a very high impact.

Task 2: security guidelines recommendations

Time limit

2 hours

You can use the time how you want but all parts of the task must be completed within the time limit.

Willow Technology are a new and growing company and therefore requires guidance in identifying the security policies required to meet compliance and regulatory needs. Your manager has identified that the current information security policy document is generic and untested. They have asked you to consider what measures could be implemented to make this policy more secure and robust and write a report of recommendations.

(20 marks)

Instructions for students

To assist your manager in writing an information security policy document, you must consider the kinds of controls that should be included in an information security policy. You should submit a report that includes recommendations for controls that could be included in an information security policy.

Your report should include:

- a justification of the user and administrative controls to be implemented
- a description of how each control will be enforced within the business
- considerations of any frameworks, legislation, regulations or standards related to each control (where appropriate)
- justification for your recommendation for:
  - managing information security incidents
  - the security and protection of data
  - upgrading policies in line with business expansion
- full references for any online sources used

You will have access to the following:

- word processing software
- the internet

Evidence required for submission to NCFE

Report containing recommendations and justification for controls that could be included within the information security policy for Willow Technology.

Student evidence

Task 2: information security guideline recommendations

1. Introduction

Willow Technology have identified that the current information security policy document is generic and untested. This report seeks to consider what measures could be implemented to make this policy more secure and robust, giving recommendations for potential changes. The introduction of a robust information security management system (ISMS) that covers the main principles of ISO 27001 would be recommended, but Control Objectives for Information and Related Technologies (COBIT) and Service Organisation Controls (SOC 2) standards could also be highly effective.

2. Gaps in current policy

Looking at the current policy the following should be considered.

2.1. Purpose

There should be a section included to indicate the purpose of the policy aligned with the collection, analysis, storage, communication and reporting of information collected.

It should also state which other policies the information security policy sits alongside so they can be referenced.

2.2. Objectives

There should be a list of the organisation's security objectives including:

- information risk management
- identity and access management
- physical, procedural, and technical controls
- contractual and legal obligations
- teaching and training of staff
- individuals' information security responsibilities (staff and 3rd party)
- security incident management

2.3. Scope

There should be a section outlining the scope of the policy to ensure there is understanding of what and who is covered by the policy.

2.4. Compliance monitoring

There should be a section outlining which teams will monitor compliance and who they report compliance to.

2.5. Review

There should be a section on how and when the policy will be reviewed and the approval route.

2.6. Policy statement

There should be a policy statement covering details of how the policy will deal with:

- confidentiality
- integrity
- availability
- standards used

3. Controls that should be included

3.1. Information security policies

The overarching information security policy will by its nature be very high level; therefore, it needs a set of lower-level, more granular policies. This should be mentioned along with who will approve the composite policies.

3.2. Organisation of information security

This section should define how a suitable set of governance arrangements will be put in place to ensure effective management of information security. It should indicate the allocation of responsibilities to identify who will implement and operate information security within the company.

It should also cover:

- who the executive chair will be
- the establishment of a cross business function governance board
- which information security specialists will be involved
- who the information asset owners (IAO) are
- who the information asset managers (IAM) are

3.3. Human resource security

Creating policies is pointless unless there is a route to ensuring the policies are known and followed. There needs to be a communication to staff as part of human resources (HR) that they must read and acknowledge the policies relevant to them, preferably with some form of acknowledgement by them and a record of this.

Control	Justification	Enforcement
Onboarding process	• ensure background checks are conducted • ensure job role is assigned • ensure role based access control (RBAC) permissions align with job role • ensure any issued equipment is assigned to the user in the configuration management database (CMDB)	No job starts without confirmation of all requirements.

Mandatory training	• ensure new starter is made aware of mandatory training and when it is due to be completed • ensure they confirm in writing that they have completed the training	HR chase or automated system set up to track.
Role change process	• ensure new job role is assigned • ensure RBAC permissions align with job role and old permissions are removed	New job role cannot start until HR approve.
Offboarding process	• ensure all system access removed • ensure login is disabled • ensure all equipment is returned as per CMDB • ensure email response setup to redirect queries to new contact	Manager must ensure all items are completed.

3.4. Asset management

There must be an undertaking to ensure all assets are documented and accounted for including: -

- software
- hardware
- electronic information processing equipment (physical and virtual)
- service utilities
- people

Owners need to identify for each asset who will be responsible for the maintenance and protection of the asset. Assets should be classified according to criticality, sensitivity, and legal requirements.

Control	Justification	Enforcement
Configuration management database (CMDB)	• ensure all assets have a configuration information (CI) entry in CMDB • ensure all CIs have an owner	No assets can be used without a CMDB entry.
Active Directory (AD)	• ensure new starters are added to AD	No AD account, no system access.

3.5. Access control

This should cover physical and data access and be aligned to RBAC.

Control	Justification	Enforcement
Job role assignment	• ensure all employees have a job role aligned with AD	No job role, no permissions.
AD groups	• ensure all data access and system access is controlled by membership of an AD group	No AD group membership no system access.

3.6. Cryptography

Cryptography should be implemented to ensure the confidentiality, authenticity and integrity of information systems.

Control	Justification	Enforcement
Encryption in flight	• ensure all system-to-system, confidential data transit is covered by an encryption standard such as transport layer security (TLS) • where TLS cannot be supported, ensure the actual data is encrypted	All data transfers to be engineered with encryption in flight.
Encryption at rest	• all confidential data stored at rest to be encrypted with a strong cypher such as Advanced Encryption Standard (AES) 256	All confidential data identified and confirmation sought that it is encrypted with a strong cypher.

3.7. Physical and environmental security

This should cover how protection against unauthorised access, damage, and interference will be provided by layered internal and external security controls.

Control	Justification	Enforcement
Physical perimeter security	• ensure all ingress points are secured so only authorised staff can use • ensure CCTV cameras are in place and prominently marked	Site security to check regularly.
Access control	• ensure all entrances to the building have access controls • ensure all staff have an ID badge and wear it	Checks by site security.
Alarms	• install burglar alarm including passive infra-red (PIR), window and door sensors	Set and checked by site security.

3.8. Operations security

This should include documented operating procedures for procedures such as, formal change control, controls against malware, capture and analysis of logging, vulnerability management, and patch management.

Control	Justification	Enforcement
Standard operating procedures	• ensure all critical systems have safe operating procedures covering functionality	Implemented as part of any change control.
Change control	• ensure all proposed change is registered as a change request and approved before being implemented	Change control system.
Security controls	• ensure anti-virus is installed on all assets • ensure vulnerability scanning is implemented • instigate a formal patch management process • instigate the capture and analysis of system logs	Regular checks carried out by IT department.

3.9. Communications security

This should include the measures in place to ensure the secure transfer of information in the internal as well as any external networks.

Control	Justification	Enforcement
Implement transport layer security (TLS)	• ensure all critical systems have safe operating procedures covering functionality	Implemented as part of any change control.

3.10. System development and maintenance

This should include the adoption of a security focused development framework such as DevSecOps as well as the formal separation of development, test and production environments. It should also cover how the use of production data in test is managed, if allowed.

Control	Justification	Enforcement
Implement DevSecOps	• ensures all development has security as part of the process	Use a formal DevSecOps platform.
Environment segregation	• ensure dev, test and production environments are separate with no interconnections other than data transfer	Network segmentation.

Data obfuscation	• ensure all data used in dev and test is either test data or obfuscated live data	Data obfuscation process.

3.11. Supplier relationships

This should cover how suppliers are onboarded and deal with what access they need to information and how they will be allowed to access.

Control	Justification	Enforcement
Implement supplier tiering	• classify suppliers according to reliance on their systems, tier 1 having more stringent checks	Procurement segmentation checks.
Supplier due diligence checks	• ensure suppliers supply details of their checks, for example vulnerability management	Procurement segmentation checks.

3.12. Information security incident management

This should cover the use of a security incident management platform where suspected breaches of information security are recorded, investigated and remediated.

Control	Justification	Enforcement
Implement a security incident management process and possibly system	• keeps all security incidents securely in one place allowing investigation	Security team checks.

3.13. Information security business continuity management

This should cover what measures are in place to protect information in the event of a disaster, security failure, loss of service, loss of utilities, and other events affecting the functioning of the business.

Control	Justification	Enforcement
Business continuity plan (BCP)	• formalises a plan should a business disaster occur	Regular walkthrough of BCP.

3.14. Compliance

This should cover the compliance with any associated information systems management statutory and contractual requirements. This covers data protection legislation and the Payment Card Industry Data Security Standard (PCI DSS). It will also cover the requirements for standards and best practise, including IT health checks, internal staff compliance checks and pen tests.

This section should also include who will review the document and how often as well as the next review date.

Control	Justification	Enforcement
Compliance matrix	• lists all legislation and regulations required by the company and aligns with systems/controls that underpin the requirements	12 monthly check

4. Frameworks

Information security management system (ISMS)

The introduction of a robust information security management system (ISMS); this could be used to create policies (for example, information security policy, acceptable use policy) to ensure an organisation is compliant with security and privacy standards and can be the starting point of gaining ISO27001 certification as discussed below.

Control Objectives for Information and Related Technologies (COBIT)

Control Objectives for Information and Related Technologies (COBIT) and Service Organisation Controls (SOC 2) standards can be a very effective framework used in helping organisations to develop procedures and internal frameworks for governance and management of IT systems.

Service Organisation Controls (SOC 2)

Service Organisation Controls (SOC 2) could be used in assessing an organisation’s security, availability, processing integrity, confidentiality and privacy controls.

Standards and regulations

ISO 27001 is a global information security management system (ISMS) standard and is perfectly suited to Willow when implementing the controls mentioned earlier in this task. It aims to secure people, processes and technology using the confidentiality, integrity and availability (CIA) triad. ISO 27001 covers the 13 main areas below and would ensure Willow has the correct physical and digital security infrastructure throughout the whole business:

1. Information security policies
2. Organisation of information security
3. Human resources security
4. Asset management
5. Access control
6. Cryptography
7. Physical and environmental security
8. Operational security
9. Communications security
10. System acquisition, development and maintenance

11. Supplier relationships
12. Information security incident management
13. Information security aspects of business continuity management

Compliance

Willow can also use information provided by National Cyber Security Centre (NCSC) Cyber Essentials portal. This is a government backed scheme that supports organisations to protect against cyber attacks and provides accreditation to organisations.

Legislation

Health and Safety at Work Act

This covers things such as the transport of equipment and the protection of employees as their carry out their roles. Personal protective equipment (PPE) needs to also be considered when it comes to protecting employees. The Health and Safety at Work Act can relate to any future infrastructure changes and/or changes to current physical infrastructure.

Manual handling

Applies to Willow employees when moving or installing new equipment related to securing the physical and digital systems; correct training is required to ensure that no one is hurt when carrying out tasks.

Equality Act

Willow must consider all protected characteristics are covered to ensure their physical and digital infrastructure is inclusive to everyone. This can include existing infrastructure and new infrastructure, and it can be something as simple as making secure areas accessible to wheelchair users and biometric systems are located so that wheelchair users can access them.

Data Protection Act (DPA) 2018

Willow will need to act in accordance with the DPA 2018. To ensure that they meet their obligations under the DPA 2018 and to ensure that they protect their networks and data (including company confidential data) adequately, there needs to be a range of controls (administrative and physical) across the company. Willow should have a range of preventative, detective, corrective, deterrent, directive, compensating and recovery controls that will maximise the protection of the infrastructure to protect from a wide range of physical and digital risks.

Computer Misuse Act

The Computer Misuse Act (CMA) was first introduced in 1990 and it has been updated a number of times; it provides a law to govern the way that individuals can lawfully access data on computer systems. This act criminalised any unauthorised access to data and the practice of modifying stored information without the permission of the owner. This act is important to Willow because they store business information on their systems and this needs to be protected from hacking, computer fraud, blackmail and viruses. If Willow fail to comply with the Computer Misuse Act they could get fined and potentially imprisoned.

Waste Electronic and Electrical Equipment (WEEE)

Willow will need to be aware of WEEE legislation when disposing of digital equipment that is required when security recommendations are implemented; this equipment can include, laptops, PCs, storage drives such as hard disk drive (HDD) and solid state drive (SSD). Safe disposal protects the environment but also ensures data is permanently destroyed and the company will reduce or eliminate the risk of any unauthorised person from handling company data.

5. Summary and next steps

This document has suggested the update required to the information security policy, but in order to be successfully implemented it requires the following:

- formal review and amendments
- approval that it contains enough to start looking at reviewing the policy
- an executive sponsor
- creation of the formal information security policy document
- approval of the information security policy
- an estimate of financial costs for each option
- the approval for the financial costs
- a timetable for the delivery of the component parts
- engagement of project management office to discuss planning and delivery

Online sources used

Below are the links that I used whilst compiling my report.

What Is Operational Security? OPSEC Explained | Fortinet. https://www.fortinet.com/resources/cyberglossary/operational-security

Three pillars of cyber security – IT Governance UK Blog. [online] IT Governance UK Blog. Available at: https://www.itgovernance.co.uk/blog/three-pillars-of-cyber-security

Confidentiality, Integrity, Availability (CIA Triad) — The Backbone of Cybersecurity. https://medium.datadriveninvestor.com/confidentiality-integrity-availability-cia-triad-the-backbone-of-cybersecurity-8df3f0be9b0e>

Why the GDPR applies to your business — regardless of your EU footprint - PR Daily. https://www.prdaily.com/why-the-gdpr-applies-to-your-business-regardless-of-your-eu-footprint/

ISO 27001 Implementation Checklist – https://www.businesstechweekly.com/legal-and-compliance/iso27001-certification/iso-27001-implementation

Information Security Policies: Why They Are Important To Your Organization. https://linfordco.com/blog/information-security-policies/

Physical and Environmental Controls. https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/physical-and-environmental-controls

ISO 27001 vs SOC 2 Certification: What’s the difference?.

https://www.itgovernance.eu/blog/en/iso-27001-vs-soc-2-certification-whats-the-difference#:~:text=Both%20frameworks%20are%20recognised%20globally,27001%20is%20much%20more%20popular.

What is COBIT? A framework for alignment and governance | CIO. https://www.cio.com/article/228151/what-is-cobit-a-framework-for-alignment-and-governance.html

The National Cyber Security Centre. https://www.ncsc.gov.uk

Task 3: disaster recovery document

Time limit

2 hours

You can use the time how you want but all parts of the task must be completed within the time limit.

Recently, there has been service outage due to denial of service (DoS) attacks near the site of the Willow Technology office. Your manager is concerned that further attacks in the future could adversely affect the business. They are considering how well the business would cope if this were to happen. They are concerned the business, as a new and growing company, does not have all policies or procedures in place yet to deal with this kind of emergency.

(20 marks)

Instructions for students

To help you complete this task, a breakdown of the current company infrastructure and security measures has been provided in the additional document ('Company overview'). You will need to refer to this document throughout the task.

Your manager has asked you to recommend a range of actions that could be taken to provide disaster recovery support from a service outage due to DoS attacks in a timely manner, whilst protecting systems and data. Your manager would like to have the business network recovered and fully operational within 3 days of a major disaster. The business is willing to invest a substantial budget of approximately £150,000 for this project, as it is estimated that an hour of downtime would cost the business £10,000 per year. You should focus on justifying recommendations that allow for disaster recovery and restoring operations ahead of concerns.

You need to write a disaster recovery document that includes:

- your recommendations in the case of service outages
- an explanation of how the actions you have taken will better protect the company

You will have access to the following:

- word processing software
- the internet

Evidence required for submission to NCFE

- disaster recovery document

Student evidence

Task 3: service outage – disaster recovery plan

Introduction

I have been asked to recommend a range of options that could be taken to provide a timely and effective disaster recovery provision against service outages. There is a requirement to recover the business network within 3 days of a major incident being declared.

The company are prepared to invest £150,000 for this project. This is based on the fact that one hour downtime is estimated at £10,000 loss per year. This allows for a budget calculated on the savings made through reducing potential 15 hours downtime per year. Another consideration is that the network must be fully recoverable and operational within a 3-day period.

This document will seek to pull together and cost measures that will:

- minimise the impact of disruptions from infrastructure failure
- minimize the impact of disruption from cyber attack (such as DOS/distributed denial of service (DDOS))
- give full recovery of the business network within 3 hours of a major incident being declared
- limit the extent of disruption and damage from any description
- establish alternative means of operation in advance of any disruption
- train personnel with emergency procedures to cope with a disruption
- provide for smooth and rapid restoration of service following any disruption

Service outage causes

Service outages are normally caused by disruption to infrastructure or intentional disruption from a cyber incident.

Infrastructure

In this digital age, companies have a heavy reliance on IT infrastructure as it underpins their digital services and applications. Infrastructure can be split into the following areas:

- physical security
- hosting – servers and services
- end user computing – desktops and laptops
- networking – network switches and edge devices such as firewalls

Physical security

There are several areas where the lack of physical security could contribute to service outages by allowing physical access to the building and IT Infrastructure. Although these would not assist in the recovery of the system, consideration could be given to these as they may prevent the outage from happening. For this reason, costings are provided as optional.

- CCTV cameras are dummy – we should install CCTV cameras in at least 3 areas to cover all ingress and egress
- reception has no access control – we should install access control on the main reception door
- fire doors are not alarmed – install fire door alarms.
- windows are often left open and have no locks – install window locks

Area	Cost (optional)
CCTV	£7,500.00
CCTV monitoring	£2,500.00
Access control	£8,500.00
Fire door alarms	£7,250.00
Windows locks	£2,500.00

Hosting

Hosting mainly entails servers, both physical and virtual. The company have a reliance on several servers that do not seem to have adequate backup or disaster recovery. Failure of these devices will therefore cause service disruption and, depending upon the type of failure, could take more than 3 days to recover.

The following measures should be considered:

- extending the current backup by linking to cloud backup
- purchasing an additional server to be sited in a different area of the office or off site if possible
- installing Hyper-V virtualisation platform onto both servers
- creating virtual servers on both Hyper-V servers
- creating replicas, offline copies of each virtual server stored on the other server capable of failover if the main virtual machine (VM) fails

Costings

Measure	Cost	Notes
Extend backup to cloud	£200 per month - £2,400 per annum	Arconis provides secure backup of the servers to cloud.
New server	£2,000	Dell rack mount server with 24TB storage.
Hyper-V and host licensing	£0	2 VMs allowed on each server so no additional cost unless more than 2 VMs
Replication	£0	Part of the Hyper-V platform

End user computing

Recommendations for recovery to end user devices within the allocated timescale include:

- store data securely and preferably in a secure, cloud-based solution allowing quick and easy recovery
- have an endpoint management system to manage user access and simplify application and device management

It is also recommended that laptops and desktops need protection. This is not a recovery option but rather a preventative measure. As such these costings are optional.

- have a firewall to prevent unauthorised site access
- have anti-virus to defend against malware

Costings

Measure	Cost	Notes
Cloud storage	£16.60 per month +VAT per user 30 users = £498 per month = £5,976 per annum	Microsoft 365 Business Premium includes OneDrive storage plus many other apps.
Endpoint management	£0	InTune is part of the Microsoft 365 Business Premium license.
Anti-virus (optional)	£4.95 per user per month + VAT 30 users = £148.50 = £1,782.00 per annum	Trend Micro Anti-Virus solution for malware protection at the end user/device level.
Firewall (optional)	£8.99 per endpoint per month = £3,236.40 per annum	Crowdstrike is a firewall as a service (FWaaS) so there is no need to purchase additional hardware.

Networking

Network redundancy

Before looking at network recovery we should first consider network redundancy, the following could be implemented:

- getting internet provision from 2 diverse suppliers using diverse routes with last mile separation; we currently have provision from BT so look at Virgin Media for an additional line – this will allow traffic to use the other supplier if a DDOS attack happens as it will have a different IP
- internet connections to come into the building using separate routers and separate cabling ingress points, as far apart as possible
- get each router provisioned with a 4G backup and install an antenna, if necessary, to get the best signal

As a preventative measure we would also recommend:

- ensure that there are additional switches to safeguard against hardware failure. This would also allow quick recovery
- make sure routers and switches are housed in secure and suitable areas to prevent accidental or intended tampering

Network disaster recovery

The following should be present in the network disaster recovery plan as this will assist in the quick recovery of the system:

- **emergency contacts and actions -** List of IT network emergency team members and their contact information at the front of the plan for fast access. A list of initial emergency response actions should also be up front
- **instructions for activating the plan** - Describing the circumstances under which the contingency plan will be activated, including outage time frames, who declares a disaster, who is contacted and all communication procedures to be used
- **emergency management procedures -** step-by-step procedures on how networks will be reconfigured, and data accessed, what outside help might be needed and how staff will be accommodated for each different kind of potential disaster
- **checklists and diagrams -** checklists that prioritise hardware and software restoration and network flow diagrams that make it easy for technical support staff to quickly access information they may need.
- **data collection -** the information that might be needed before officially declaring a network disruption, including network performance data and staff, and first responder reports
- **disaster declaration -** Identified actions to take once the network emergency team determines it's necessary to declare a network disaster, including how the decision is communicated, who is contacted and what additional damage assessments are needed
- **disaster recovery -** instructions on restoring network operations, connectivity, devices, and related activities

Costings

Measure	Cost	Notes
Recommended		
Additional Internet provider	£60 per month + VAT = £720 + VAT per annum	Virgin Media Voom Gig1 fibre connection
Optional (no additional cost)		
Routers	£0	Part of the internet service provider (ISP) provision
Intrusion protection	£0	Part of Crowdstrike
Firewall	£0	Part of Crowdstrike
Optional		
2 x locked comms cabinets	£800.00	To house switches and ensure they are guarded against unapproved access.
Switch	£6,450 + VAT	1 x additional Cisco Catalyst plus stacking cables
Additional server room	£25,000.00	Secure server room with air conditioning.
Secure existing server room	£12,000.00	Secure structure, install air conditioning, Uninterruptible Power Supply (UPS) and access control.

Cyber incident

The following are identified potential cyber incidents that could result in service outage, so consideration has been given to preventative measures that could be included within the costings.

- **malware -** the provision of Trend Micro anti-virus as part of the end user computing provision will guard against malware
- **phishing –** implementation of 2-factor authentication (2FA) where a mobile device registered to each user has an application registered with the company that provides a changing-digit number. Access to the company systems will then require a username, password **and** the key (which changes every 30 seconds). If using Microsoft 365 licensing the best product would be an Azure Active Directory (AD) license costing £7.50 per user per month plus VAT
- **password attack** – as this risk is normally associated with phishing the above recommendation of Azure AD would help to protect against this

Denial of service

A denial of service (DoS) attack is an attempt to make a system unavailable to the intended users, such as preventing access to a website. A successful DoS attack consumes all available network or system resources, this usually results in a slowdown or crash of the targeted system.

A distributed denial of service (DDOS) uses many different sources to flood the target system, therefore, more sophisticated strategies are needed to mitigate this type of attack as simply blocking one source will not work as there are multiple sources.

1.2.4.1. DOS/DDOS mitigation

There are many measures that can be put in place to defend against DOS/DDOS attack and help protect the system and this could be introduced though the use of Firewall as a service (FWaaS) which would be better suited to cloud services recommended so far as quick recovery mechanisms. This would allow for access control, URL filtering, threat, and intrusion prevention. FWaaS does vary in price but example pricing starts at £200 per month and can grow considerably.

Summary

Costs

So far, the recommendations above would easily fit within the £150,000 budget and includes additional considerations that are not required for recovery but could be implemented as part of a preventative measure to ensure the infrastructure is protected prior to an incident.

A further recommendation of an all-in-one resilience platform would allow for automated services such as backups, disaster recovery, easy management, protection for operating systems, files, systems and settings as well as the ability to transfer workloads between public, private and hybrid clouds. Costings for this can vary considerably and are usually based on the amount of storage required. For example, some systems work on a £50 per month per terabyte whilst other systems offer an all-in-one solution costing at approximately £1000 per year. The total cost for this would need to be calculated based on business usage although even using the standard £1000 would still remain within budget and offer a quick and reliable recovery solutions.

The key recommendation would include:

- development of a recovery plan which clearly identifies the key contacts, the current infrastructure and services and how these are used within business operations
- assess the resilience of both the hardware and the software within the organisation and ensure redundancy is implemented where possible
- implementation of data protection and recovery mechanisms through automatic backup procedures on and off site, utilising cloud services where possible
- implement disaster recovery software solution if possible

Overall costing

Breakdown below taken from figures highlighted throughout the report.

Recommended

Measure	Cost
Extend backup to cloud	£200 per month - £2,400 per annum
New server	£2,000
Hyper-V and host licensing	£0
Replication	£0
Cloud storage	£16.60 per month +VAT per user 30 users = £498 per month = £5,976 per annum
Endpoint management	£0 (available as part of Microsoft 365)
Additional Internet provider	£60 per month + VAT = £720 + VAT per annum
All-in-one resilience platform	£1000
Total cost	**£12,096**

As many of the costing included here require a yearly subscription this costing would provide a solution for the next 10 years whilst remaining within budget.

Optional costs

These option costs are only included as a preventative measure if required.

Area	Cost
CCTV	£7,500.00
CCTV monitoring	£2,500.00
Access control	£8,500.00
Fire door alarms	£7,250.00

Windows locks	£2,500.00
Anti-virus	£4.95 per user per month + VAT
Firewall	£8.99 per endpoint per month = £3,236.40 per annum
Routers	£0
Intrusion protection	£0
Firewall	£0
2 x locked comms cabinets	£800.00
Switch	£6,450 + VAT
Additional server room	£25,000.00
Secure existing server room	£12,000.00
Azure Active Directory	£7.50 per user per month plus VAT

Examiner commentary

Overall, this student has produced a risk assessment that provides a thorough justification for each recommendation they have identified. The student clearly justifies the need for an information security policy and highlights user and administrative controls that could be implemented as part of this. The student concludes with a disaster recovery plan which includes a wide range of options, costings and considerations.

Task 1

The student has produced a detailed risk-assessment showing understanding of how cyber security procedures and protection techniques address the control and mitigation of risk. It included the identification of main asset types and their threats, and the techniques to protect against them. The student has produced a detailed explanation showing a comprehensive understanding of risk assessment in cyber security and for each asset category; they have listed the main accompanying threats to vulnerabilities, have estimated the subsequent likelihood of occurrence and the potential resulting damage, and has shown knowledge of quantitative estimates of the potential risk. The student has completed the template table to show a good understanding of how the risk assessment could reduce the risk of attack that demonstrates a thorough justification of each recommendation – the student could improve this by including more detailed contingency measures in the action column, for example they identify the dummy CCTV cameras with an action to install working CCTV cameras but failed to explain how these would be utilised (recording saved to the cloud). In some instances, it would have improved the response to have seen how the risk rating had been determined, for example risk 1 is identified as high risk / medium likelihood with overall risk as medium.

Task 2

The student has given an excellent explanation and justification for the need of information security policies and the role of regulatory compliance, given examples of regulatory frameworks and has indicated the type of data security policies that the business should include, taking into consideration both the people elements and the technology elements. This could have been improved with further analysis of all sources' credibility.

Task 3

The student has given excellent explanation and justification for the proposed recommendations in the case of service outages that has included a comprehensive, in-depth explanation of the types of distributed denial of service (DDoS) attacks and how compensating protection techniques could frustrate these attacks. Although this demonstrates a very good level of understanding by the student this could have been a distraction if provided as a report to an organisation as their focus would have based around the requirements and not this additionality.

Breaking the costings up into individual tables following each proposal worked well, as it allowed the reader to focus on the costs involved for individual security elements, for example hosting. This would allow them to better identify how the budget is spent. In the final summary table total costing was calculated at approximately £12,000 which was well under budget although this is justified as a ten-year plan. However, there might have been other options that would have utilised the budget more efficiently which may explain why the student has extended beyond the assessment requirements by considering physical security measures.

Overall grade descriptors

Grade	Demonstration of attainment
Pass	The student is able to develop a project proposal to research and compare the current software available and justify their recommendations.
	The student is able to install supplied software onto a device and ensure it is all correctly configured.
	The student is able to identify and explain the difference between cyber attacks and software issues, and how a cyber attack could take place.
	The student is able to investigate the issues on the virtual machine provided and explain the most effective remedial action to take to mitigate any problems.
	The student is able to evaluate a network with regards to cyber security.
	The student is able to ensure that company resources and data are fully protected.
	The student is able to perform a security risk assessment of the site and the network.
	The student is able to recommend physical, administrative, and technical controls.
	The student is able to create a disaster recovery plan including recommendations in the case of service outages.
	The student is able to explain how remedial actions will protect the company, which includes considerations for security, manageability and upgradeability in relation to cyber security policies.
Distinction	The student is able to develop an in-depth project proposal to research and compare the current software available and comprehensively justify their recommendations.
	The student is able to install supplied software onto a device, demonstrating excellent capabilities in ensuring it is all correctly configured.
	The student is able to comprehensively identify and explain the difference between cyber attacks and software issues, and evidence a detailed understanding of how a cyber attack could take place.
	The student is able to thoroughly investigate the issues present on the virtual machine provided and fully justify the most effective remedial action to take to mitigate any problems.
	The student is able to carry out an in-depth evaluation of a network with regard to cyber security and identify areas of improvement.

	The student is able to perform an in-depth security risk assessment of the site and the network, identify areas of concern and give a rationale for each.
	The student is able to recommend physical, administrative, and technical controls and justify their recommendations.
	The student is able to create an in-depth disaster recovery plan, including justifications for recommendations in the case of service outages.
	The student is able to demonstrate in-depth knowledge and give a thorough explanation of how remedial actions will protect the company, which includes considerations for security, manageability and upgradeability in relation to cyber security policies.

Document information

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education. NCFE is currently authorised by the Institute to develop and deliver the Technical Qualification in Digital Support Services.

Owner: Head of Assessment Design

Change History Record

Version	Description of change	Approval	Date of issue
v1.0	Published final version	June 2023	31 August 2023