# T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

# Cyber Security

Assignment 3 – Pass

Guide standard exemplification materials (GSEMs)

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

Internal reference: DSS-GSEM-20

## 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

| ID | Threat | Vulnerability | Asset | Impact | Likelihood | Risk | Action | Control type |
|---|---|---|---|---|---|---|---|---|
| 1 | Unlocked main gate | There is a risk that access can be gained onto the company premises. This could provide easy access and exit from the company premises by criminals | Physical equipment | Medium | Medium | Medium | Secure main gate with access control. | Preventative<br>Unrestricted external access |
| 2 | Car park access | There is a risk that access can be gained onto the company premises. This could provide easy access and exit from the company premises by criminals | Physical equipment | Medium | Low | Low | Covered by securing main gate. | Preventative |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 3 | Unlocked main entrance | There is a risk that an unsecured main entrance could give unauthorised access. Anyone could get access to the inside of the building, making the interior significantly less secure. | Physical equipment | Medium | High | Medium | Ensure door is locked when reception is not manned. | Preventative<br>Unsecured access |
| 4 | Additional access not controlled | There is a risk that having no access control of the additional access could allow unauthorised access to the hot desk area. | Physical equipment | Medium | High | Medium | Access controls for additional access, . | Preventative<br>Uncontrolled access |
| 5 | Fire door left open to cool | Anyone could get access to the inside of the building, making the interior significantly less secure. | Physical equipment | Medium | Medium | Medium | Alarm for fire door to be installed. | Preventative<br>Unmonitored, open access to any area is not a good idea. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 6 | No entrances alarmed | There is a risk of unauthorised access. | Physical equipment | Medium | Medium | Medium | Install alarm | Deterrent<br>Alarm is needed to indicate unauthorised access. |
| 7 | Open windows not closed | There is a risk that windows being open outside of operational hours could result in unauthorised access. | Physical equipment | Medium | Medium | Medium | Install alarm | Deterrent<br>Windows open when no-one is on premise is a security risk. |
| 8 | Fire exit leads into the server room | There is a risk of somebody gaining access to the server | Physical equipment and digital data | Medium | Medium | Medium | Install alarm or self-locking door | Corrective |
| 9 | Due to small IT team, there is no mention of an asset register for the business | It can be easier for assets to go missing or be stolen, keep track of maintenance and upgrade plans and could be required for some compliance standards, for | Physical equipment and digital data | Low | Low | Low | Create an asset register. | Corrective<br>An asset register would ensure all assets were recorded and the company meets compliance standards. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | example, ISO 27001 | | | | | | |
| 10 | ID badges | They could gain access to the computers and could potentially access content or steal the devices. | Staff | Low | Low | Low | Make wearing an ID badge in the office mandatory and link these badges to access control systems for the external and internal areas of the building. | Corrective<br>ID badges ensure anyone on premise is identified. |
| 11 | Backups only taken once per month and stored on site | There is a risk that not having full incremental backup could result in data being irretrievably lost. | Digital Data | Medium | Medium | Medium | Look at movement of data to the cloud. | Corrective<br>Frequent backups (onsite and off-site) (daily as a minimum) would protect against this. |
| 12 | Lack of a password policy | Employees could be using weak passwords leading to risks of data security | Digital Data | Medium | Medium | Medium | Create password policy | Corrective |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 13 | Local admin risk | There is a risk that allowing local admin access to staff could allow them to install software from any source that could result in a malware infection | Security | High | Medium | High | Remove local admin access for all staff except authorised administration accounts on the network. | Corrective |
| 14 | Lack of anti-virus | There is a risk that the lack of anti-virus could result in virus infection. Users could infect devices with malware | Security | High | High | High | Configure windows defender firewall and purchase and install anti-virus on all endpoints. | Corrective |
| 15 | Lack of firewall | Hackers and malicious actors could gain access to systems and data. This can result in data theft, financial loss, and damage to the company's reputation. | Security | High | Medium | High | Configure windows defender firewall on all devices | Preventative<br>Lack of a firewall can result in data loss. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 16 | Mobile phones unrestricted | There is a risk that having unrestricted mobile phones compromise company data. | Security | Medium | Possible | Medium-High | Look at locking down phones. | Preventative<br>An unrestricted mobile device could allow a network breach. |
| 17 | There appears to be no access control so staff could have access to everything | Without access control there is no control over who has access to what resources or data within the business. | Security | Medium | Medium | Medium | Ensure roles exist for all staff and align with the lowest privilege permissions required for the role. | Corrective<br>Access to resources and data will be managed consistently, leading to less errors in access management and increased security. |
| 18 | No IT help desk system | There is a risk that not employing an IT help desk system will result in issues not getting resolved | All | Low | Low | Low | Implement an IT help desk system | Corrective |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 19 | Return to normal operations after incident | 3 day recovery after incidents could be difficult to achieve. | Disaster recovery (DR) | High | Possible | High | Create provisions in disaster recovery plan that ensure that a 3 day recovery after incidents can be achieved, for example, redundancy in IT infrastructure | Corrective |

# 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

### Introduction

Willow Technology have identified that the current information security policy document is generic and untested.

This report will consider what measures could be implemented to make the policy more secure and robust, giving recommendations for potential changes.

When creating a security policy document, it is important that a set of steps are followed that will help ensure the content is correct, an Information Security Management System (ISMS) is used to create policies (for example, information security policy, acceptable use policy) to ensure an organisation is compliant with security and privacy standards.

Some of the steps required when establishing an ISMS include :

- define the scope
- conduct a risk assessment
- develop policies and procedures
- train employees
- continuously improve

### Controls

I have divided the control section into 2 sections to include user controls and administrative controls. I will now cover the main controls that are related to an organisation like Willow.

**User controls**

User controls are designed to ensure that employees, contractors, and other users of the systems can access data at Willow can access only the resources that they require to perform their job functions. User controls can include physical and digital controls and can sometimes use both methods.

By implementing user controls Willow can reduce the risk of accidental or intentional data breaches and prevent unauthorised access to sensitive information and premises.

User controls that Willow could implement

- password policies that ensure passwords are hard to compromise and staff understand how best to keep passwords secure, this can include minimum password length, complexity requirements, and regular password changes - this control can be a document on the network but can be enforced digitally, for example, Active Directory
- two factor authentication requires users to provide an additional form of authentication (for example,, a code sent to their mobile phone via SMS) in addition to a password - this control can be enforced digitally, for example, Active Directory and will be important for the remote workers security at Willow
- access controls which limit user access to specific systems, applications, or data based on their job responsibilities - this can be achieved at Willow through Role Based Access Controls (RBAC) - this control can be enforced digitally, for example, Active Directory

- tailgating controls to prevent an intruder gaining unauthorised access to premises and buildings at Willow, this can be achieved through alert employees, barrier systems and mantraps
- locking screens to preventing unauthorised access of a staff member's account while away from the computer - this can be controlled through group policy objects (GPO) in Windows Server
- encryption of mobile data to ensure confidential data cannot be accessed in the event of theft or other loss of the device - this can be achieved through the use of VPN technology at Willow
- installation of firewall, antivirus or other antimalware software to reduce the risk of malicious malware or viruses accidentally being installed on devices at Willow - this digital control can be implemented at device level or network or a combination of both
- Bring Your Own Device (BYOD) policies help implement restrictions when undertaking work activities using personally owned devices, this could be an issue at Willow with the remote working aspect of the daily routines currently operating

**Administrative controls**

Administrative controls are policies and procedures that help govern the management of Willow's information security program. They are designed to ensure that information security is integrated into all aspects of Willow's operations and that appropriate safeguards are in place to protect sensitive information.

Administrative controls focus on managing risk, providing security awareness training, and ensuring that security policies and procedures are being followed.

Administrative controls that Willow could implement

Information security policies and procedures, which provide guidance on the organization's information security practices and expectations, for example, business continuity and data protection.

Risk management control and processes which help identify, assess, and manage information security risks, for example, risk assessment strategy.

Incident response procedures which detail the steps to be taken in the event of security incidents, this can be part of the business continuity process.

User education and training to help staff at Willow understand their role in protecting the organisation's information assets and how to use the organisation's security controls effectively. This can include cyber awareness training and taking part in internal phishing campaigns.

Regular security assessments and audits, which help ensure that Willow's security controls are effective and up to date. This can include becoming certified to a standard such as ISO 27001.

**Frameworks**

An information security framework is a structured approach to managing and protecting an organisation's information assets. One of the most common frameworks is detailed below:

**COBIT (Control Objectives for Information and Related Technology)**

COBIT is a framework developed by the Information Systems Audit and Control Association (ISACA) for managing and governing enterprise IT. There are 5 primary areas of COBIT;

1. Governance is focused on the development of IT strategies, policies, and procedures, as well as the establishment of governance structures to ensure that IT aligns with business objectives and complies with legal and regulatory requirements.
2. The management area covers the implementation of IT processes and management practices to ensure the effective and efficient use of IT resources and to enable the delivery of IT services that meet business needs.
3. Operations covers the day-to-day management of IT systems and services, including the monitoring and management of IT infrastructure, the management of IT service delivery, and the management of IT security and compliance.
4. Information covers the management of information as a strategic resource, including the management of data quality, data privacy, and data security.
5. Implementation covers the implementation of IT projects and initiatives, including project management, change management, and IT service delivery.

COBIT is suited to corporate organisations and is used by KPMG, PwC, Accenture, Ernst & Young, Deutsche Bank, JP Morgan and Bank of America. It is also useful and used by smaller organisations and departments and would be beneficial to an SME like Willow.

**Standards**

ISO 27000 information security management – a series of standards to provide best practice for information security management systems, ISO 27001 has 112 controls that are divided into 14 main categories as detailed below;

1. Information security policies
2. Organization of information security
3. Human resource security
4. Asset management
5. Access control
6. Cryptography
7. Physical and environmental security
8. Operations 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
14. Compliance

ISO 27001 can be a suitable framework for Willow who are looking to improve their information security and demonstrate their commitment to protecting sensitive data. Some of the issues raised in the risk assessment can be addressed through ISO 27001 because this framework is aimed at the business as a whole, for example, physical and digital security. ISO 27001 is a flexible framework that can suit the size and needs of any business. The standard is scalable and can be applied to small businesses, as well as large enterprises. It will help Willow identify and manage information security risks through the rigorous risk controls in the standard, this can be particularly important for Willow who have limited resources and may be more vulnerable to cyber attacks.

## Legislation and regulations

### Data Protection Act 2018

The DPA 2018 will require Willow to act in accordance with it, this will include appointing a data protection officer. There must be a variety of administrative and physical controls throughout the company to ensure that they meet their obligations under the DPA 2018 and adequately protect their networks and data (including company confidential data), this can achieved through the recommendation of implementing ISO 27001. To protect the infrastructure from a wide range of physical and digital risks, Willow ought to have a variety of preventative, detective, corrective, deterrent, directive, compensating, and recovery controls as detailed in ISO 27001. These controls will maximize security at Willow and provide the required protection.

### Waste Electronic and Electrical Equipment (WEEE)

When it comes to disposing of digital equipment that is required when security recommendations are implemented, Willow will need to be aware of WEEE legislation; Laptops, personal computers, and storage drives like solid state drives (SSDs) are examples of this kind of equipment that will require safe removal. This will safeguard guarantee information is deleted permanently. Willow will need to keep records of the amount and type of electronic waste they collect and recycle and report this information to the national producer register. Willow must label all devices with the WEEE logo and must arrange for the collection and recycling of electronic waste, either through a national recycling scheme or by setting up their own collection and recycling system.

### Computer Misuse Act

The Computer Misuse Act 1990 is a UK law that makes it illegal to access computer systems without permission or to cause damage to computer systems. Willow must follow this act to ensure that only authorised users have access to their systems to prevent the introduction of viruses or other malicious software,

Willow must ensure that appropriate security measures are in place to prevent damage to computer systems. If Willow fails to comply with the Computer Misuse Act it can result in legal consequences, including fines and imprisonment. Willow must ensure that they comply with the Act to avoid legal liability and reputational damage, in turn, it will help Willow provide the security and integrity of their digital infrastructure, protect sensitive information and avoid legal consequences.

### Summary and next steps

ISO 27001 is the recommended standard that should be implemented by Willow, it will provide guidance on the required controls and managing incidents, details of the correct policies and updating these in line with business requirements whilst providing risk assessment opportunities to ensure the security of systems and data, This can lead to a successful implementation of an Information Security Management System.

The steps now required to achieve ISO 27001 standards certification include;

- define the scope
- conduct a risk assessment
- develop policies and procedures
- train employees
- continuously improve

## 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

# 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

Willow have asked to be provided with recommendations on a range of options that could be taken to provide a timely and effective disaster recovery plan against service outages.

The company are prepared to invest £150,000 for this project.

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

- minimize disruption from cyber attacks such as DOS/distributed denial of service (DDOS)
- allow network recovery
- limit the extent of disruption and damage from any attack
- train personnel with emergency procedures to cope with a disruption
- provide a quick restoration of service

Disaster recovery planning (DRP) will need to include information relating to the following areas:

- define the scope of the incident
- gathering relevant information
- risk-assessing
- creation of the plan
- plan approval
- testing of the plan
- continuous improvement

In the event of a service outage due to cyber attack such as DOS at Willow, we need to ensure that the business is able to keep working while the main system is down. We need to have plans to keep working if the server is damaged and have functionality so staff can access resources.

My main recommendation would be to implement a failover system at a remote site as this would introduce redundancy in the system. The current system that is on premises utilises Windows Server, so a server in Azure cloud could be an option. Alternatively, there could be an option of having a redundant server on the premises that could be utilised if the main server goes down.

Getting the workforce ready to switch to a remote working system is also a recommendation. This would tie in with the first recommendation, for example, if the main system goes down, a redundant system will be utilised, and staff could successfully connect to the redundant server in the cloud.

End devices would need to be configured that would allow users to work from home while the office system is down. The solution should include virtualised desktops. This would allow the team to access through a software client on their personal computer as if they were logged in to a company computer. This will give the team full access to their desktop no matter whether they were working within the office, or remotely. This would support the general working of the office and also ensure that business continuity should continue regardless of

whatever happens to the office with no downtime. Willow would have to provide laptops in this scenario. Providing company laptops would be the ideal solution because these can be configured with the correct security configurations and be in line with controls detailed in the company Information Systems Security System (ISMS). An online storage solution for files could be implemented – such as SharePoint or OneDrive to ensure that everyone can access files regardless of their location.

SharePoint is cloud based meaning we will not be keeping critical data onsite. In the event of a DOS attack at Willow, staff can keep working accessing the data and continue to work. SharePoint is an effective collaborative tool and will keep company data securely in the cloud. This will mean the risk to data is minimal at all times and there will effectively be no drop in service keeping staff working.

A policy should be created that ensures that everyone knows what will happen in the situation where access to the office systems is restricted, this should include a flowchart that explains the steps to be taken and how things should be at each stage. This should also include an emergency call tree to ensure that everyone knows what has happened and what the plans are.

For the business to perform best during an outage, it is important that the IT team have an accurate asset database so that they are aware of who has what equipment and if there are any areas where there may need to be equipment issued for the duration of the emergency. In an ideal situation there will be a plan for a remote working location where people could get together to continue working together, this could be within a client/partner's site or a remote location that had been deemed suitable in advance. With the site out of action we still need to ensure that equipment on site is protected.

By using a failover site like this we can ensure that we always have servers in place and working. By implementing these business continuity recommendations, in the event of DOS (or other disaster) the business is ready and can adapt its working practice with no effective loss of service to our customers. Between the disaster recovery plan and the business continuity plan this should ensure that the business can continue as quickly as possible.

In order to ensure that the business can recover from a DOS or other cyber attack the following will need to be considered:

Backup solution – one needs to be implemented as soon as possible, this should be an off-premises solution, in an ideal world this would be a continuous online backup as attacks can often happen with very short notice and at any point in the day.

I would recommend using a cloud backup solution as this will mean that we back data up remotely and securely to our cloud provider so that we do not have the data onsite and at risk. Whilst having a backup solution is important, the restoration needs to be tested regularly to ensure that the backup has worked successfully and will be able to be restored should the worst happen.

This will also support in identifying how long it will take to restore should they need to. Backups should include a basic disk image including all the configurations and settings applied as well as core software such as antivirus. In the event of a cyber-attack damaging the server we will need a plan for what hardware and data to be restored first.

Part of the disaster recovery policy needs to specify the roles that IT staff will take so that people know what it is that they must do to recover from a disaster. Part of the recovery process will involve potentially sourcing equipment.

To ensure that disaster recovery is done as quickly as possible there should be a flowchart created in order to ensure that the process could be as easy as possible. This should have identified flows and test points to make sure that everything has been followed to ensure the smooth restoration of business.

## My Recommendation

My recommendation includes functionality that would help the business meet the ISO 27001 standard, provide functionality for future expansion and be the start of infrastructure migration to the cloud. This includes on

premises hardware and also includes buying end devices if on premises work is not an option and employees have to work remotely

I suggest a redundant network on premises and a Microsoft Azure cloud based redundant system to be implemented to allow a shared document system to enable collaboration.

**Costings**

Below are the costings for the system to continue operating in the event of a disaster from a cyber attack

| Area | Costs | Notes |
|---|---|---|
| 30 x Azure AD Premium P2 licenses | £7.50 per user per month + VAT.<br>30 users = £225.00 per month = £2,700.00 per annum | Azure AD functionality |
| End user computing | £5,018.40 | Devices that are needed. |
| Networking | £7,170.00 | Infrastructure that is required for communications. |
| Cyber incident | £2,700.00 | Reporting and response management for cyber related incidents. |
| Anti-virus | £4.95 per user per month + VAT<br>30 users = £148.50 = £1,782.00 per annum | Trend Micro anti-virus solution for malware protection at the end user/device level. |
| Firewall | £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. |
| Firewall | £0 | Part of Crowdstrike |
| Routers | £0 | Part of the internet service provider (ISP) provision |
| Intrusion Protection | £0 | Part of Crowdstrike |
| Switches | £3,462.34 | 2 x Cisco Business CBS350-48P-4X Managed Switch \| 48 Port GE \| PoE \| 4x10G SFP+ |
| Internet provider | Full Fibre 150 Mbits Enhanced & Digital Line (Halo) for £47.95 per month | Second line from BT |

| | | |
|---|---|---|
| | £47.95 per month + VAT = £575.40 per annum | |

## DOS/DDOS mitigation

The following measures can be put in place to defend against DOS/DDOS attack:

- contact network service provider to see what assistance they may be able to provide you in the event of a DDoS attack
- consider also establishing relationships with companies who are DDoS protection service providers, such as Crowdstrike
- monitor firewall log files
- apply all vendor patches after appropriate testing
- configure firewalls and intrusion detection/prevention devices to alarm on traffic anomalies
- configure firewalls only to accept traffic detailed in your organization's security policy as required for business purposes

## Summary

The above measures will better protect the company as:

- it introduces methods to make our internal servers resilient and provide redundancy on the network
- it builds resilience into the network
- it also deals with single points of failure in our servers and services by introducing an additional server as well as remote working functionality through Azure
- the details will be gathered before any disaster is declared allowing input from multiple areas
- the documentation will allow the plans to be tested
- through dry runs all participants will have a run through of what they must do and when if a major incident occurs

# Examiner commentary

Overall, the risk assessment demonstrates some understanding of risk mitigation and control measures but would have benefitted from a wider range of threats identified. The student clearly focuses on user and administration controls but lacks depth and justification of choices made. Finally, the student does identify measures that could be introduced as part of a disaster recovery plan; however this is not fully aligned to the costings making it difficult to identify what would be the main recommendations.

**Task 1**

The student has shown a basic understanding of how cyber-security procedures address the control and mitigation of risk. This has included some identification of asset types and their threats, and the techniques to protect against them occurring. This response could have been more comprehensive and included further detail within each asset category. The student has clearly worked through the company overview and identified some of the more common vulnerabilities that are present within the scenario, however some of the more obvious ones have been missed, for example the dummy cameras. There is also a lot of opportunity within this scenario to make assumptions and although these aren't explicitly mentioned within the scenario, some mention of these within the risk assessment would have enhanced the overall student response.

The student has shown a basic understanding of risk assessment in cyber security and the student has also identified some of the assets deployed, the threats that may exploit vulnerabilities, and has given a limited estimate of the subsequent likelihood of occurrence and the potential resulting damage. For example, the car park access is identified as a medium impact but low likelihood although the scenario does say that is used by other people, therefore the likelihood would be higher than low. A deeper explanation of this is needed to gain a higher grade. The student has provided an overview of risk mitigation controls.

The completed risk template table would have benefitted from the identification of more threats with detailed explanation of the vulnerabilities these introduce.

**Task 2**

The student has divided the report into 2 sections focusing on user and administrative controls. Each section identifies some common controls that could be implemented that would help to reduce the risk of data breaches, however these do appear to be very generic, mainly focusing on common factors, for examples passwords and authentication. The student does consider a framework and relevant legislation but does not really justify why these have been chosen as the main focus. It is good to see that ISO 27001 has been identified as a standard for consideration. Overall, this section is a satisfactory response to the requirements of the task but lacks depth and justification throughout.

**Task 3**

The report starts with a basic introduction which outlines the investment available, and the measures required. The narrative focuses on some key points, but this does not flow as well as it could have been better structured. For example, after providing several suggestions the report identifies a number of measures that could be implemented to ensure the business can recover from a cyber attack. It is not clear however, how this would link in with all the suggestions prior to this. The student then provides a table of costings which fall within budget but many of these costings are not mentioned within the narrative, for examples the £7,170 spent on networking and then an additional £3,462 spent on switches. The report does provide mitigation for DDoS and a final summary, but written sections rather than bullet points would have been more appropriate here for a report.

# 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



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 |