Assignment Guidance and Front Sheet

This sheet is to be populated by the Module Tutor, checked by the Programme Team, and uploaded to Moodle for students to fill in their ID and submit with their assessment.

Student ID or IDs for group work	**U2136249**

Module Title & Code	WM244 - Information Security Management
Module Owner	Dr Olga Angelopoulou
Module Tutor	Dr Olga Angelopoulou
Module Marker	tbc
Assesment type	CW2: Information Security Framework of Policies
Date Set	10.10.22
Submission Date (excluding extensions)	14.03.23
Marks return date (excluding extensions)	20 working days from the date of the submission
Weighting of mark	50%

Assessment Detail	**Please refer to the Case Study and Useful Sources sections.** You are required to create a framework of policies in the format of one (1) page table that are UK Government compliant for the given organisation's IT infrastructure. The framework of policies you create must pass UK Government-based requirements. You should write an executive report of no more than two (2) pages that discusses 3 high-priority security controls for your organisation and any potentially optional elements of the framework. It is imperative that the executive report should have a professional look and be precise. After

	all it will be submitted to the firm’s executive team as the result of your work. Also, it should include your justification behind your decisions. Any relevant notes of your work must be submitted as an appendix.
Additional details	There is no word count for this coursework as long as you adhere to the requirements of the submission: a. One page table b. Up to two pages report c. Any additional work/ notes submitted in an appendix You should use a clear font in a font size that would be readabe when printed in A4 size paper. Recommended font sizes: - Table: font size 9-11pt - Report: font size 10-12pt If you utilise any appendices, then you should refer the reader to the relevant appendix within your report, otherwise the appendix will not be considered.
Module learning outcomes (numbered)	1 - Adopt a responsible attitude to the social, ethical, legal and regulatory consequences that flow from professional engagement in security management. 2 - Evaluate the overall coherence of an organisation's management of cyber security, recommending remediation where needed.
Learning outcomes assessed in this assessment (numbered)	1,2
Marking guidelines	You will be marked based on the following criteria:

	1. *Completeness of the framework of policies* *2. Consideration of issues/ Security controls* *3. Justification of arguments* *4. Presentation and design* **Please also refer to the University Marking Scale (attached below).**
Submission guidance	You must use the Harvard referencing system as per the University regulations. All submissions should be made in PDF format via Tabula https://tabula.warwick.ac.uk.
Academic Guidance	This coursework aims to guide you on writing a professional report in a non-verbose manner. Additional guidelines if necessary will also be provided in a class briefing session.
Resubmission details	The University policy is that students should be given the opportunity to remedy any failure at the earliest opportunity. What that "earliest opportunity" means in terms of timing and other arrangements is different depending on Programme (i.e. Undergraduate, Full Time Masters, Part Time Postgraduate, or Overseas). Students are advised to consult your Programme Team or intranet for clarity.
Late submission details	If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late" means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late.

Information Security Policy Framework (ISPF)

Global Finance Enterprise

Policy Framework
Version 1.0

Feb 15, 2023

Company Sensitive and Proprietary
For Authorized Use Only

Table of Contents

List of Tables

Document Revision History

Date	Description	Version	Author
15/02/2023	Document Publication	1.0	information security manager
22/03/2023	Table 1	2.0	information security manager

Information Security Policy Framework	
1. Purpose:	Information is an asset, and its security is of utmost importance. The risk of theft, misuse, loss, and corruption of information is a constant threat that requires proper management. Inadequate education and training, as well as breaches in security controls, can put information at risk. Information security incidents can result in financial loss, embarrassment and non-compliance with standards and legislation. To address these risks, Global Finance has developed a comprehensive Information Security Policy Framework with the 'Information Risk Management Policy' and 'Data Protection Policy' to provide a set of risk-based information security controls necessary to protect the organization's valuable information assets.
2. Objective:	This framework sets out the senior management commitment to information security and establishes a framework for governance, responsibility and accountability for information across Global Finance.
3. Scope:	The Information Security Policy and its supporting controls, processes and procedures apply to all information used and all individuals who have access at Global Finance.
4. Compliance Monitoring	Compliance with the security controls in this framework will be monitored by the Information Security Team, and reported to the Information Governance Board.
5. Review	A review of this policy will be undertaken annually or as required by the information security manager (ISM) and approved by the Chief Information Security Officer (CISO)
6. Policy Statement	It is Global Finance’s security policy to ensure that information is protected from a loss of: • **Confidentiality** – Information will be only accessible to authorised individuals. • **Integrity** – The accuracy and completeness of information will be maintained. • **Availability** – Information will be accessible to authorised users and processed when required.

Table 1: Information Security Policy Framework for Global Finance IT Infrastructure. V2.0-R1

Policy Area	**Policy**	**UK Government Requirements**	**Description**	**Control(s)**	**Standard(s)**
Access Control	Authentication and Access Control Policy	Access to systems and data must be granted on a need-to-know basis. To comply with HMG Security Policy Framework (SPF) and Data protection Act.	Access to the computing environment must be granted based on the principle of least privilege, restricted to authorized personnel and to minimize the risk of unauthorised access or breach of information.	Implement a system of access control to information based on job role and need-to-know such as Multi-factor authentication (MFA). (Appx. B(1))	➢ NCSC Cloud Security Principles. ➢ ISO/IEC 27001:2013 6.1.3. ➢ GDPR Article 32(1)(b).
Data Protection and Privacy	Data Protection and Privacy Policy	Confidentiality, integrity, and availability of information must be ensured to comply with GDPR.	Personal data must be encrypted both in transit and at rest.	Encrypt sensitive data both in transit and at rest and secure deletion of data when it is no longer required. (Appx. B(2))	➢ ISO/IEC 27001 ➢ GDPR Articles 5, 25, 32.
Security Incident Management	Incident Management and Response Policy	Reporting and handling of security incidents must be prompt and efficient.	Incidents must be reported, investigated, and responded to in a timely and effective manner.	Develop and implement an incident response plan that outlines procedures for reporting, investigating, and responding to incidents. (Appx. B(3))	➢ ISO/IEC 27001:2013 16.1.6 ➢ GDPR Article 33.
Network Security	Network Security Policy	Ensure the security and reliability of the network infrastructure.	Firewalls must be installed and configured to restrict traffic, and network traffic should be monitored for any unauthorized activity.	Firewalls, Intrusion Detection and Prevention Systems. (Appx. B(4))	➢ NCSC's Network Security ➢ ISO/IEC 27001:2013 14.1.2, 14.2.1 ➢ Cyber Essentials
Physical Security	Physical and Environmental Security Policy	Physical access to the computing environment must be restricted to comply with DPA.	Physical access to information systems and equipment must be controlled and monitored.	Implement physical security controls such as access controls, CCTV, and monitoring to ensure that only authorised personnel have access to information systems and equipment. (Appx. B(5))	➢ ISO/IEC 27001:2013 15.1 ➢ Cyber Essentials
Personnel Security	Personnel Security Policy	Organizations shall implement security policies and processes that include background checks, an insider threat program, and a program to drive the security culture.	Implement vetting and screening procedures for personnel, including contractors and third-party vendors.	Background checks, Security awareness training. (Appx. B(6))	➢ NCSC's Personnel Security ➢ ISO/IEC 27001 ➢ Cyber Essentials Plus,
Business Continuity	Business Continuity and Disaster Recovery Policy	Ensure that all systems are secure and up-to-date.	implement policies and procedures to appropriately handle security incidents and reduce damage to sensitive assets and critical information systems	Disaster Recovery plan, Business Continuity Plan. (Appx. B(7))	➢ NCSC's Business Continuity ➢ ISO/IEC 27001.

Executive Summary

As Global Finance prepares to embark on a high-priority, high-visibility project for the UK government, it is imperative to implement appropriate security controls to ensure the confidentiality, integrity and availability of the organisation's information assets. This report highlights the three most crucial high-priority security controls the organisation must implement to protect its assets and meet UK Government standards.

Context

As technology continues to advance, the reliance on digital systems and data has increased significantly, with this reliance comes an increased risk of cyber-attacks and data breaches (United Nations, 2020). It is essential for organisations to have an effective information security policy framework (ISPF) to provide an structure approach for managing and protect sensitive data and assets, including software and hardware from cyber threats. By having a comprehensive ISPF, and organisation can identify and mitigate potential risks and ensure compliance with regulatory requirements, neglecting so it can lead to significant financial losses, reputational damage, and legal penalties (Central Digital & Data Office, 2022).

High-Priority Security Controls for Global Finance

After a thorough analysis of Global Finance IT infrastructure and UK government requirements, the following three security controls have been identified as high-priority:

Access Control: Multi-Factor Authentication (MFA)

As part of the UK Government's Cyber Essentials scheme, MFA is mandatory for access control to secure sensitive data access (Department for Digital, Culture, Media & Sport, 2014). Access control is critical to protect the organisation's data and systems from unauthorised access; it determines who is allowed to access data and resources, keeping confidential information – such as customer data and intellectual property – from being stolen by threat actors (Microsoft, 2021). This control is essential for the ERP application (Oracle), which contains sensitive information.

Multi-factor authentication (MFA) is a security control that requires users to provide two or more forms of identification before accessing a system or application. It gives an additional layer beyond traditional username and password authentication. According to Microsoft, MFA can block 99.99% of account compromise attacks (Maynes, 2019). As Global Finance enterprise expands, the attack surface is also increasing; implementing MFA can prevent phishing attacks and significantly reduce the risk of unauthorised access to Global Finance systems and data (OneLogin, 2021) and comply with UK Government standards such as GDPR.

Incident Management: Regular Security Awareness Training

Employees are considered to be the weakest link in a company's security posture, in 2022 Verizon's Data Breaches Investigations Report showed 82% of data breaches involve a human element (Verizon, 2022), these incidents range from employees exposing information directly, such as misconfiguring a database, to indirectly making an error that enables threat actors to access the organisation's systems. Regulatory frameworks such as HIPAA and SOC2 require companies to provide awareness training to be compliant. Training in password hygiene, phishing awareness and data handling help educate employees on the risks of cyberattacks and how to identify and respond to them (Rende, 2023).

While providing awareness training ensures compliance with UK government requirements, it is vital to ensure that the training is adequate and relevant to each employee's role within the organisation; this can be done through monitoring and regular and targeted security training (CybSafe, 2022). Targeted training can be achieved by assessing each employee's role and responsibilities to tailor the training context to their specific needs. Adding regular training helps reinforce the importance of security practices and monitoring through regular assessments, such as simulated phishing attacks, helps identify any knowledge gaps and allows training to be provided to those employees who need it the most, helping the organisation to mitigate the risk of human error and improve overall security posture (Mimecast, 2020).

Data Protection: Vulnerability Assessments and Software Updates

Data protection is crucial to safeguard the organisation's data from authorised access, use, disclosure, destruction or system failure (ICO, 2022). Security controls such as regular patching and vulnerability assessments ensure that all software and systems, such as the Microsoft Exchange Server – used for email communication - are up-to-data with the latest patches avoiding system exposures to potential security threats.

In 2021, the average cost of a data breach was £4.43 million (Statista, 2022). Vulnerability assessment and penetration testing are vital to identify potential security weaknesses in Global finance's IT systems and software applications. Along with this, regular testing helps identify vulnerabilities that cybercriminals could exploit.

Conclusion

In conclusion, implementing the three high-priority security controls outlined in this report will provide Global Finance with a strong foundation for ensuring its assets' confidentiality, integrity and availability to meet UK Government compliance requirements. The security landscape is constantly evolving, so it is crucial for the organisation to continuously reassess and update its security controls to ensure ongoing protection against emerging threats.

APPENDIX A. ACRONYMS

Acronyms	Definition
AC	Authentication Category
AP	Assurance Profile
API	Application Programming Interface
ATO	Authorization to Operate
C&A	Certification & Accreditation
COTS	Commercial Off the Shelf
AO	Authorizing Official
FedRAMP	Federal Risk and Authorization Management Program
FIPS PUB	Federal Information Processing Standard Publication
FISMA	Federal Information Security Management Act
GSS	General Support System
IaaS	Infrastructure as a Service (Model)
IATO	Interim Authorization to Operate
ID	Identification
IT	Information Technology
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
POC	Point of Contact
RA	Risk Assessment
R1	Revision 1
SA	Security Assessment
SAR	Security Assessment Report
SDLC	System Development Life Cycle
SP	Special Publication
SSP	System Security Plan
VLAN	Virtual Local Area Network
HIPAA	Health Insurance Portability and Accountability Act
SOC2	Systems and Organization Controls 2

APPENDIX B. DETAILED SECURITY CONTROLS

1. Access Controls
    1. Access controls are applied to all systems, applications, and data.
    2. Regular review of access rights to ensure they are appropriate and necessary for users' job roles.
    3. Use of multi-factor authentication for all accounts.
    4. Implementation of role-based access control to restrict access to sensitive data.
    5. Segregation of duties to prevent a single individual from having too much control.
2. Data Protection
    1. Encryption of sensitive data both in transit and at rest.
    2. Regular backup and recovery processes to ensure data is available in the event of loss or corruption.
    3. Secure deletion of data when it is no longer required.
    4. Employee training on data protection regulations, best practices, and the organisation's policies.
3. Incident Management
    1. Defined incident management process and procedures for all employees.
    2. Regular training for all employees on how to recognise and report security incidents.
    3. Regular testing of the incident management process to ensure its effectiveness.
4. Network Security
    1. Implementation of firewall and intrusion detection / prevention systems to prevent unauthorised access.
    2. Regular testing and maintenance of network security controls.
    3. Use of secure protocols for remote access to the network.
5. Physical Security
    1. Restricted access to computing facilities.
    2. Secure storage of backup media and portable devices.
    3. Regular maintenance and testing of physical security controls.
6. Software Security
    1. Patch management for all software and operating systems.
    2. Implementation of application whitelisting to prevent the installation of unauthorised software.
    3. Regular security testing of all software applications.
7. System Security
    1. Regular maintenance of systems to ensure they are running the latest security patches and updates.
    2. Implementation of security configurations for all systems.
    3. Regular security testing of all systems.

APPENDIX C. REFERENCES

Cabinet Office (2013). *Security policy framework: legal guidance*. [online] GOV.UK. Available at: https://www.gov.uk/government/publications/security-policy-framework-legal-guidance.

Cabinet Office (2014). *Security requirements for List X contractors*. [online] GOV.UK. Available at: https://www.gov.uk/government/publications/security-requirements-for-list-x-contractors.

Cabinet Office (2016). *Security policy framework, May 2018*. [online] GOV.UK. Available at: https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework.

Central Digital & Data Office (2022). *Transforming for a digital future: 2022 to 2025 roadmap for digital and data*. [online] GOV.UK. Available at: https://www.gov.uk/government/publications/roadmap-for-digital-and-data-2022-to-2025/transforming-for-a-digital-future-2022-to-2025-roadmap-for-digital-and-data.

Central Digital and Data Office (2016). *Government technology standards and guidance*. [online] GOV.UK. Available at: https://www.gov.uk/guidance/government-technology-standards-and-guidance [Accessed 20 Mar. 2023].

CybSafe (2022). *7 reasons why security awareness training is important*. [online] CybSafe. Available at: https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/#:~:text=It%20helps%20employees%20to%20understand.

Department for Digital, Culture, Media & Sport (2014). *Cyber Essentials Scheme: overview*. [online] GOV.UK. Available at: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

GDPR (2018). *General Data Protection Regulation (GDPR)*. [online] General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/.

ICO (2022). *The benefits of data protection laws*. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/sme-web-hub/the-benefits-of-data-protection-laws/#:~:text=As%20well%20as%20being%20the.

Maynes, M. (2019). *One simple action you can take to prevent 99.9 percent of attacks on your accounts*. [online] Microsoft Security Blog. Available at: https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/.

microsoft (2021). *What is Access Control? | Microsoft Security*. [online] www.microsoft.com. Available at: https://www.microsoft.com/en-gb/security/business/security-101/what-is-access-control.

Mimecast (2020). *What is Security Awareness Training and Why is it Important?* [online] Mimecast. Available at: https://www.mimecast.com/content/what-is-security-awareness-training/#:~:text=Security%20awareness%20training%20helps%20to.

NCSC (2019). *NCSC CAF guidance*. [online] Ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/collection/caf.

OneLogin (2021). *What is Multi-Factor Authentication (MFA)? | OneLogin*. [online] One Login. Available at: https://www.onelogin.com/learn/what-is-mfa#:~:text=Why%20is%20MFA%20Important%3F.

Rende, J. (2023). *Council Post: How Providing Staff Awareness Training Improves A Company's Security Posture*. [online] Forbes. Available at: https://www.forbes.com/sites/forbestechcouncil/2023/01/27/how-providing-staff-awareness-training-improves-a-companys-security-posture/ [Accessed 22 Mar. 2023].

Statista (2022). *UK businesses: average cost of security breaches 2019*. [online] Statista. Available at: https://www.statista.com/statistics/586788/average-cost-of-cyber-security-breaches-for-united-kingdom-uk-businesses/.

United Nations (2020). *The Impact of Digital Technologies | United Nations*. [online] www.un.org. Available at: https://www.un.org/en/un75/impact-digital-technologies.

Verizon (2022). *DBIR Data Breach Investigations Report*. [online] Available at: https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf.