INDIVIDUAL ASSIGNMENT

NAME (TP NUMBER)	**:**	Koo Wai Kit (TP081761)
INTAKE CODE	**:**	APUMF2406CYS
MODULE TITLE	**:**	Security Audit and Assessment (102024-YWR)
MODULE LECTURER	**:**	Yogeswaran A/L Nathan
PROJECT TITLE		Security Audit and Assessment: Individual Assignment Section 2 (Implementation & Critical Evaluation of Methods for Auditors to Conduct Proper Security Auditing Techniques)
DATE ASSIGNED	**:**	21 October 2024
DATE COMPLETED	**:**	3 February 2025

Contents

1. Abstract 3
2. Introduction to the Industry Selected 3
3. Audit Plan 4
   3.1 Objectives 4
   3.2 Scope 4
   3.3 Methodology 5
      3.3.1 Effectiveness of Selected Methodology 6
      3.3.2 Limitations and Challenges in Implementation 6
4. Sample Security Audit Checklist 6
5. Security Audit Report 12
   5.1 Potential Nonconformities 12
      5.1.1 Inadequate monitoring of third party vendors and supply chain risks 12
      5.1.2 Insufficient controls over employee access and data handling 13
      5.1.3 Limited scope of data protection and privacy assessments for certain services 13
   5.2 Recommendations for Improvements 14
      5.2.1 Strengthening Third-Party Vendor and Supply Chain Risk Management 14
      5.2.2 Enhancing Employee Access Controls and Data Handling Policies 15
      5.2.3 Expanding Data Protection and Privacy Assessments Across All Services 15
6. Conclusion 15
7. References 16

List of Tables

Table 1: PayPal's security audit checklist 7

1. Abstract

This report proposes a security audit plan and checklist for the digital payment industry based on PayPal as a reference model. PayPal's security posture is audited against ISO/IEC 27001, and key areas such as authentication, encryption and transaction integrity are evaluated. The methodology is a structured approach involving planning, document review, field work, analysis and reporting in order to check if the security standards were complied with and if there are any vulnerabilities. Key findings suggest nonconformities in third party vendor management, employee access controls and data protection policies. The report provides recommendations for strengthening PayPal's security resilience in order to achieve better compliance and protect sensitive financial data in digital transactions.

2. Introduction to the Industry Selected

With traditional face-to-face transaction models giving way to online platforms which are known as convenient and efficient to a great extent, the digital payment industry has undergone a remarkable change. The industry has undergone this rapid evolution which has changed the operations of financial transactions while leaving the industry exposed to sophisticated cyber threats and vulnerabilities in areas like authentication, encryption and network integrity (Solat, 2017). Thus, having robust security measures and doing thorough security audit had become necessary to protect the sensitive financial data and secure consumers' trust in an increasingly digital economy.

The purpose of this report is to work on the digital payment industry to develop an audit plan and checklist based on existing information security management standards. Because it involves various stakeholder like banks, merchants, payment processors and fintech companies, security audits for this ecosystem should not only check for technical risks but also integrate the security practices across all actors in the ecosystem (Ishrat, 2020).

In this report, I will discuss PayPal as a reference point for the digital payment industry to create an audit plan and checklist. PayPal is a major player in the industry and therefore needs to evaluate technical risks and security practise integration among its stakeholders including banks, merchants and payment processors. Notably, PayPal already meets security standards like PCI DSS and ISO/IEC 27001 for the protection of its digital payment systems (Paypal, 2024). For this report, however, I will simulate the process of creating an audit plan and

checklist as if auditing PayPal's security controls against ISO/IEC 27001, and provide insights into the auditing process and best practises for securing digital payment platforms.

3. Audit Plan

The audit plan provides a process to evaluate PayPal's security posture as a representative model for the digital payment industry. This section describes the objectives, scope and methodology used to audit PayPal's digital payment system against ISO/IEC 27001, and address the critical weaknesses. The methodology's strengths and weaknesses concerning effectiveness, alignment with ISO/IEC 27001, as well as the challenges of implementation are also evaluated.

3.1 Objectives

The key to this audit is to determine the level of security within PayPal's digital payment systems, identifying weaknesses, ensuring compliance to ISO/IEC 27001, and reducing the risks posed by cyber threats. Specifically, the audit aims to:

a. Assess the efficiency of PayPal's current security controls in ensuring sensitive financial data is protected.
b. Verify compliance with relevant standards and regulations such as ISO/IEC 27001.
c. Identify technical and procedural weaknesses in PayPal's digital payment processes.
d. Recommend actionable measures to boost security resilience and reduce risks of fraud.
e. Strengthen overall trust and reliability in PayPal's payment transactions through rigorous security assessment.

3.2 Scope

PayPal is used as a reference model for the audit to evaluate the security posture of digital payment systems. The review analyses security components of PayPal's platform by looking at how elements like user authentication, data encryption and transaction integrity are handled. The analysis takes into account the broader digital payment ecosystem, but it focuses specifically on testing PayPal's conformity to ISO/IEC 27001. Due to the assignment constraints, the evaluation is simplified to give an overview of PayPal's security practises as a benchmark for the industry without going into exhaustive details.

3.3 Methodology

The structure of the audit methodology for evaluating PayPal's information security management system (ISMS) is based on ISO/IEC 27001 standard. The process consists of the following phases:

a. **Planning**: The audit process starts with a full understanding of PayPal's operational environment and the particular objectives of the audit. This includes identifying the critical information assets, processes and systems that are to be evaluated. This helps to focus the audit on whether PayPal's ISMS is effective in protecting sensitive financial data.

b. **Document Review**: In this phase, the audit team will carefully scrutinise PayPal's ISMS documentation. This also includes reviewing information security policies, procedures, risk assessment and incident response plan. The objective is to confirm that these documents are not only exhaustive and up to date but also in line with ISO/IEC 27001 requirements. This review gives a review of how information security is managed in the organisation.

c. **Fieldwork**: The techniques used in the fieldwork phase include evaluating the effectiveness of ISMS policies and procedures. Interviews with key personnel are done to determine their understanding of the security measures as well as their adherence to the security measures. Observations of operational processes are undertaken to confirm the practical implementation of the security controls. Technical testing will look at potential weaknesses in systems, such as vulnerability scanning with tools like OpenVAS, while an analysis on the network is performed with tools like Wireshark to ensure data integrity and confidentiality during transactions (Chesbrough, 2021).

d. **Analysis**: The data collected during fieldwork is analysed for identifying any non-conformities or areas for improvement. The result of this analysis is to analyse how effective the existing security controls are and also how much the organization is compliant with ISO/IEC 27001 standards. This will serve as the foundation on which the actionable recommendations will be based.

e. **Reporting:** The findings of the audit are compiled into a complete report that documents and classifies identified vulnerabilities, determines the effectiveness of existing security approaches, and provides recommendations for remediation. This report is a roadmap for PayPal to improve its information security posture.

3.3.1 Effectiveness of Selected Methodology

This audit methodology for evaluating PayPal's ISMS is to provide a complete assessment in accordance with the ISO/IEC 27001 standard. The methodology progresses through the phases of planning, document review, field work, analysis, and reporting systematically to ensure a thorough evaluation of the design and operational effectiveness of security controls. This structured process helps to understand where vulnerabilities could be and where improvements can be made, making PayPal more secure. ISO/IEC 27001 emphasizes the importance of regular audits as it is one of the means of demonstrating the efficiency of the organization's security controls as well as a tool to measure the ongoing compliance to the ISO standards (Martinez, 2024).

3.3.2 Limitations and Challenges in Implementation

There are several challenges to implementing the audit methodology for PayPal's ISMS. Due to a lack of visibility to proprietary systems and technologies such as PayPal's unique algorithms and other technologies, the technical analysis can be limited. Moreover, PayPal's platform is dynamic and has a lot of updates and addition of features which may make audit findings outdated very quickly after being performed. Manual document reviews and personnel interviews are resource intensive as well, and pose scalability limitations to very large-scale, multi-jurisdictional audits. Furthermore, the methodology provides a remedy to the known vulnerabilities, but it may not cover new attacks powered by AI, or other risks that will likely be imposed by quantum computing. Despite these limitations, the methodology offers a solid basis to measure compliance with ISO/IEC 27001 in the digital payment sector.

4. Sample Security Audit Checklist

Before the security audit, firms should take some measures to ensure a strong safeguarding framework. It includes knowing regulatory requirements, setting up internal policies and appointing a safeguarding officer to oversee compliance. Customer funds must be properly segregated from financial risks and the risk must be regularly assessed to identify vulnerabilities. Thorough documentation of safeguarding activities and continuous training of employees strengthen the overall awareness within the firm. Finally, regular compliance is maintained by keeping updated on any regulatory changes (Shipleys LLP, 2023). These principles will serve as a basis for the development of PayPal's security audit checklist in line with ISO/IEC 27001 requirements.

Table 1 below presents PayPal's security audit checklist, which covers key security measures, their associated ISO/IEC 27001 clauses and controls, and the evidence needed to show compliance. A total of 31 checklist items are categorized based on their respective security domain. It should be noted that this checklist is a simplified version of the complete information security management framework of PayPal and is not a complete list of everything PayPal has to cover.

Table 1: PayPal's security audit checklist

Security Domain	**Security Measure**	**ISO/IEC 27001 Clause**	**ISO/IEC 27001 Control**	**Evidence**
Network security	Implement robust firewall configurations and intrusion detection/prevention systems (IDS/IPS)	8.1 Operational Planning and Control	A.1.8.20 Network security	Firewall configuration policies, IDS/IPS logs, penetration test reports
	Enforce network segmentation to isolate critical systems from public networks	8.1 Operational Planning and Control	A.1.8.22 Segregation of networks	Network topology diagrams, segmentation policies
	Encrypt all network communications with TLS/SSL	8.3 Information Security Risk Treatment	A.1.8.24 Use of cryptography	TLS/SSL certificates, encryption policies
	Monitor and log all network traffic for anomalies	9.1 Monitoring, Measurement, Analysis and Evaluation	A.1.8.16 Monitoring activities	Network monitoring logs, SIEM reports
	Enforce multi-factor authentication (MFA) for all	8.3 Information	A.1.8.5 Secure authentication	MFA implementation reports,

	critical systems	Security Risk Treatment		authentication logs
Identity and Access Management (IAM)	Restrict and monitor privileged access	8.3 Information Security Risk Treatment	A.1.8.2 Privileged access rights	Access control lists, privilege audit logs
	Implement role-based access control (RBAC) and perform periodic access reviews	8.3 Information Security Risk Treatment	A.1.5.18 Access rights	Access review reports, user access control policies
	Secure user endpoint devices with strong authentication controls	8.1 Operational Planning and Control	A.1.8.1 User endpoint devices	Device authentication logs, endpoint security reports
Application Security	Secure application development using a secure software development lifecycle (SDLC)	8.1 Operational Planning and Control	A.1.8.25 Secure development life cycle	Secure coding guidelines, security testing reports
	Perform regular security testing, including penetration testing and code reviews	9.1 Monitoring, Measurement, Analysis and Evaluation	A.1.8.29 Security testing in development and acceptance	Penetration test reports, code review logs
	Enforce secure coding practices to prevent OWASP Top 10 vulnerabilities	8.3 Information Security Risk Treatment	A.1.8.28 Secure coding	Secure coding guidelines, developer training records

	Limit access to source code repositories	8.3 Information Security Risk Treatment	A.1.8.4 Access to source code	Access control lists, repository audit logs
Data Security and Encryption	Maintain regular, encrypted backups of critical data	8.3 Information Security Risk Treatment	A.1.8.13 Information backup	Backup logs, encryption policies, restoration tests
	Implement data leakage prevention (DLP) mechanisms	8.3 Information Security Risk Treatment	A.1.8.12 Data leakage prevention	DLP policies, audit logs
	Ensure secure data deletion and disposal	8.3 Information Security Risk Treatment	A.1.8.10 Information deletion	Data destruction certificates, secure wipe logs
	Mask or anonymize sensitive customer data	8.3 Information Security Risk Treatment	A.1.8.11 Data masking	Data masking policies, database audit logs
Security Monitoring and Incident Response	Monitor and log all security-relevant activities in a centralized SIEM system	9.1 Monitoring, Measurement, Analysis and Evaluation	A.1.8.15 Logging	SIEM logs, security event reports
	Ensure continuous security monitoring with real-time alerts for suspicious activities	9.1 Monitoring, Measurement, Analysis and Evaluation	A.1.8.16 Monitoring activities	SOC monitoring reports, anomaly detection logs
	Establish and test an incident response	8.3 Information	A.1.5.24 Information security	Incident response

	plan (IRP) regularly	Security Risk Treatment	incident management planning and preparation	policies, tabletop exercise reports
	Ensure timely response and remediation of security incidents	10.2 Nonconformity and Corrective Action	A.1.5.26 Response to Information Security Incidents	Incident response reports, remediation logs
Business Continuity and Disaster Recovery (BCDR)	Develop and maintain a business continuity and disaster recovery (BCDR) plan	8.1 Operational Planning and Control	A.1.5.30 ICT readiness for business continuity	Disaster recovery test results, BCP documentation
	Ensure redundancy of critical systems to prevent downtime	8.3 Information Security Risk Treatment	A.1.8.14 Redundancy of information processing facilities	High-availability system documentation, failover test results
	Perform regular disaster recovery (DR) drills	8.3 Information Security Risk Treatment	A.1.5.29 Information security during disruption	DR drill reports, recovery time objective (RTO) analysis
Employee Security Awareness and Physical Security	Ensure all employees undergo security awareness training	7.3 Awareness	A.1.6.3 Information security awareness, education, and training	Training records, employee acknowledgment forms
	Implement clear desk and clear screen policies	8.1 Operational Planning and Control	A.1.7.7 Clear desk and clear screen	Office security policies, compliance audit reports

	Enforce secure remote working policies, including VPN and endpoint security	8.1 Operational Planning and Control	A.1.6.7 Remote working	VPN logs, remote access security guidelines
	Control physical access to data centers and critical infrastructure	8.1 Operational Planning and Control	A.1.7.1 Physical security perimeters	Access logs, surveillance camera footage
	Ensure secure disposal or reuse of IT assets and sensitive media	8.3 Information Security Risk Treatment	A.1.7.14 Secure disposal or re-use of equipment	Asset disposal logs, data destruction certificates
Compliance and Regulatory Requirements	Ensure compliance with legal, regulatory, and contractual obligations	5.31 Legal, Statutory, Regulatory, and Contractual Requirements	A.1.5.31 Legal, statutory, regulatory, and contractual requirements	Compliance audit reports, regulatory documentation
	Conduct independent security audits and assessments	9.2 Internal Audit	A.1.5.35 Independent review of information security	Third-party audit reports, security certifications
	Monitor compliance with internal security policies and industry best practices	9.2 Internal Audit	A.1.5.36 Compliance with policies, rules, and standards for information security	Internal audit reports, policy compliance reviews

5. Security Audit Report

This section details the results of the security audit performed on PayPal's systems, including potential nonconformities and possible improvements.

5.1 Potential Nonconformities

There are three potential nonconformities identified by reviewing online documents and web pages of PayPal, including their "2023 Global Impact Report," "Code of Business Conduct & Ethics," and "PayPal Privacy Statement."

5.1.1 Inadequate monitoring of third party vendors and supply chain risks

While PayPal states that it works with third parties that share its commitment to business ethics and has a Third Party Code of Conduct & Ethics, the company also acknowledges that it cannot always control greenhouse gas emissions outside of its direct control and relies on third party vendors for many goods and services. They are working with more than 300 of their top suppliers to communicate their climate-related risk management priorities (PayPal, 2024). However, if that level of engagement does not apply to all vendors that can have access to sensitive data or systems, or if the risk assessment of those vendors is not stringent enough and ongoing, this could be a very serious risk. Third party information security is a requirement of ISO 27001, and any breach could result in data breaches or service disruptions.

In addition, the report mentions a third party vendor seeking to access customer data beyond the original scope, which was denied, but this serves as a reminder of a possible control and oversight gap (PayPal, 2024). That can lead to major breaches if similar situations occur with other vendors that are not identified.

Security controls from the sample audit checklist associated with the nonconformity of inadequate monitoring of third party vendors and supply chain risks are as follows:

a. Enforce multi-factor authentication (MFA) for all critical systems.
b. Restrict and monitor privileged access.
c. Implement role-based access control (RBAC) and perform periodic access reviews.
d. Ensure compliance with legal, regulatory, and contractual obligations.
e. Conduct independent security audits and assessments.
f. Monitor and log all security-relevant activities in a centralized SIEM system.

5.1.2 Insufficient controls over employee access and data handling

It is emphasized in the "Code of Business Conduct & Ethics" that confidential and proprietary information, and company assets must be protected. It says employees should never check a PayPal account without a business reason and should tell their manager if they have a business reason to look at a customer account that belongs to a friend, family member or professional contact (PayPal, 2024). These policies are good but if the implementation and enforcement of these policies are not sound, it may result in unauthorised access and internal misuse of customer data, which is a key requirement of ISO 27001.

Similarly, the "Code of Business Conduct & Ethics" forbid employees from sharing credentials to get access to company systems, however if the company does not enforce and audit user access permissions and logs, then such a system will be exposed to both malicious and unintentional misuse. For example, a customer support agent can check a customer account just for curiosity and not for a business purpose, even though not allowed, proves that it is possible to circumvent access controls (PayPal, 2024).

Furthermore, although employees are not allowed to use company devices for personal reasons, sometimes they do, and if the devices are lost, it can result in leaks if not handled properly. In addition, the policies of how information should be shared with third parties are also specified, although it is a complicated process with multiple steps and approvals (PayPal, 2024). If these steps are not followed consistently, then the data can be shared incorrectly.

Security controls from the sample audit checklist associated with the nonconformity of insufficient controls over employee access and data handling are as follows:

a. Enforce multi-factor authentication (MFA) for all critical systems.
b. Restrict and monitor privileged access.
c. Implement role-based access control (RBAC) and perform periodic access reviews.
d. Secure user endpoint devices with strong authentication controls.
e. Monitor and log all network traffic for anomalies.
f. Implement data leakage prevention (DLP) mechanisms.

5.1.3 Limited scope of data protection and privacy assessments for certain services

While PayPal has an extensive data management and privacy programme, the "PayPal Privacy Statement" says that it does not apply to excluded services, including Venmo and Hyperwallet. This implies that the company's security and privacy controls may not be applied in the same

way. A general approach to data retention is also described in the "PayPal Privacy Statement" and, while it says they will respect data subject rights, it is not clear whether such practises are applied uniformly across services and subsidiaries (PayPal, 2024).

The importance of a unified and comprehensive approach to information security is stressed by ISO 27001. When there is a lack of alignment between different services or products, especially when these services or products are processing highly sensitive data such as financial transactions, it becomes vulnerable to attack by malicious actors. The way PayPal handles personal information with Fastlane is specifically stated, which implies that it is not part of the normal processes and needs a special process (PayPal, 2024). This may suggest that the company provides a lot of services but not all of them are at the same stage of maturity.

Security controls from the sample audit checklist associated with the nonconformity of limited scope of data protection and privacy assessments for certain services are as follows:

a. Monitor and log all security-relevant activities in a centralized SIEM system.
b. Implement data leakage prevention (DLP) mechanisms.
c. Ensure compliance with legal, regulatory, and contractual obligations.
d. Conduct independent security audits and assessments.
e. Maintain regular, encrypted backups of critical data.
f. Ensure secure disposal or reuse of IT assets and sensitive media.

5.2 Recommendations for Improvements

5.2.1 Strengthening Third-Party Vendor and Supply Chain Risk Management

To mitigate risks of third party vendors, PayPal should establish a continuous monitoring programme for vendor security compliance, monitoring all vendors and not just the top suppliers for cyber risks. A risk assessment framework of different tiers should be established to classify vendors based on the sensitivity of the data that they have access to, and more stringent security controls should be applied to high risk vendors. Furthermore, contractual agreements should require strict compliance with cybersecurity requirements such as periodic auditing, security awareness training, and requiring obligatory reporting of any attempted unauthorized access to the customer’s data.

5.2.2 Enhancing Employee Access Controls and Data Handling Policies

PayPal should adopt a zero-trust access model to ensure that no unauthorised employee has access to sensitive data, and that access to the data is granted on a need-to-know basis and continuously verified. Automated user behaviour analytics (UBA) can be implemented to detect suspicious access patterns like employees viewing accounts not related to their job function. Also, the company would have to undertake additional efforts in improving endpoint security and this includes encrypting data storage, allowing remote wipe if a device is lost or stolen, and enforcing stricter access to data on sharing policies for their employees to employ best security practices.

5.2.3 Expanding Data Protection and Privacy Assessments Across All Services

PayPal should make the security and privacy framework applicable to all subsidiaries and services, such as Venmo and Hyperwallet, to ensure a unified and comprehensive approach to data protection. Encryption, data retention, privacy controls should be standardized among all platforms through the establishment of a cross-service data protection policy. The company should also do regular privacy impact assessments to check if its security controls are working well on every service and make sure the data of the customer is always protected, no matter what service the customer is using.

6. Conclusion

PayPal's digital payment system security audit emphasises the significance of effective security measures in safeguarding financial transactions and adhering to ISO/IEC 27001. The audit's findings consisted of vulnerabilities such as weak vendor risk management, lack of employee access controls, and inconsistencies in data protection. This highlights the urgent need of continuous security improvement to cope up with evolving cyber threats and to safeguard users' data. Through strengthening these areas, PayPal can become more resilient against cyberattacks, meeting global security standards.

As cyber threats become more sophisticated, the broader digital payment industry is subject to similar challenges as PayPal. As digital transactions are gaining more uses, payment service providers have to use proactive security measures, conduct regular security checks and follow international compliance standards. The strengthened cybersecurity practices within the industry will not only promote consumer trust but they will also play an important role in strengthening the stability and security of the whole of digital financial ecosystem.

7. References

Chesbrough, A. (2021, March 25). *Top 5 open-source tools for network vulnerability scanning*. BreachLock. https://www.breachlock.com/resources/blog/top-5-open-source-tools-for-network-vulnerability-scanning/

Ishrat, Z. (2020). Compendious research of Escrow Payment - Focusing on Future Considerations, Trends and Applications. *European Journal of Business and Management Research*, *5*(4). https://doi.org/10.24018/ejbmr.2020.5.4.347

Martinez, J. (2024, September 30). *Iso 27001 audit: everything you need to know*. https://www.strongdm.com/blog/iso-27001-audit?utm_source=chatgpt.com

PayPal. (2024, November 27). *Paypal privacy statement*. https://www.paypal.com/us/legalhub/paypal/privacy-full

Paypal. (2024, May 1). *2023 global impact report*. https://s202.q4cdn.com/805890769/files/doc_downloads/2024/05/2023-PayPal-Global-Impact-Report.pdf

Paypal. (2024). *Code of business conduct & ethics*. https://s205.q4cdn.com/875401827/files/doc_governance/2024/May/code-of-business-conduct-ethics-2024_external.pdf

Shipleys LLP. (2023, June 6). *An 8-point checklist to help payment and e-money firms' safeguarding audit compliance*. https://www.shipleys.com/resources/an-8-point-checklist-to-help-payment-and-e-money-firms-safeguarding-audit-compliance/

Solat, S. (2017). Security of electronic payment systems: A comprehensive survey. *arXiv preprint arXiv:1701.04556*.