# ***Controls and compliance checklist***

***Prepared by:*** Basma Mounir Mahmoud Ayash

***Date:*** July 2025

***Course:*** Google Cybersecurity Professional Certificate

## *About this Document :*

This checklist represents one possible solution for the Botium Toys activity in the Google Cybersecurity Professional Certificate program. The goal is not to match a fixed answer, but to demonstrate critical thinking in selecting relevant controls and compliance practices to help the organization reduce risk and meet regulatory standards.

## *Executive Summary:*

This document presents a comprehensive cybersecurity controls and compliance checklist developed as part of the **Google Cybersecurity Professional Certificate**.
It evaluates the security posture of a fictional company (Botium Toys) by identifying gaps and recommending appropriate security controls and compliance best practices.
The checklist addresses critical areas such as access control, data encryption, incident response, backup strategies, and physical security. It also aligns with standards such as **PCI-DSS**, **GDPR**, and **SOC 1/2**, ensuring that the organization meets regulatory requirements and reduces the risk of security incidents or legal penalties.
This work demonstrates my ability to assess risks, select relevant security controls, and apply cybersecurity principles in a practical, business-focused context.

## Controls assessment checklist

| Yes | No | Control | *Explanation* | *Recommendation* |
|---|---|---|---|---|
| | X | Least Privilege | *Some employees have admin rights they don't need* | *Review all roles and remove excess access.* |
| | X | Disaster recovery plans | *The company currently lacks any documented disaster recovery plans. In the event of a major incident, this could lead to data loss, prolonged downtime, and damage to the organization's reputation.* | *Develop formal disaster recovery plans and conduct recovery tests every three months to minimize risks, reduce potential losses, and maintain the organization's credibility.* |
| X | | Separation of duties | *Responsibilities and sensitive tasks are distributed among multiple individuals, reducing the risk of misuse or human error.* | *Implementing the Separation of Duties principle helps reduce the risk of misuse, fraud, and individual errors. It also enhances monitoring and transparency, thereby strengthening the overall security posture of the organization.* |
| | X | Firewall | *The absence of a firewall or misconfigured settings can allow malicious traffic from the internet to access the internal network,* | *Implement a properly configured and regularly updated firewall to monitor and filter incoming and outgoing traffic, ensuring protection against external* |

| | | | | |
|---|---|---|---|---|
| | | | *increasing the risk of cyberattacks.* | *threats.* |
| | X | Intrusion detection system (IDS) | *Devices on the network exhibit potential malicious activities and unauthorized system changes, exposing the network to security risks.* | *Activate monitoring systems for network and system traffic (such as an IDS) to generate immediate alerts for administrators to take necessary actions and protect the network.* |
| | X | Backups | *The absence or weakness of a backup system increases the risk of losing critical data in case of attacks like ransomware or technical failures, affecting business continuity.* | *Establish a regular backup system with copies stored securely off-network, and conduct periodic restoration tests to ensure data recovery effectiveness.* |
| X | | Antivirus software | *Early detection of malware such as viruses, malware, and ransomware helps prevent their spread and protects systems from damage or breaches by removing or isolating them.* | *Maintain system, network, and organizational security by deploying effective antivirus software that detects threats like viruses, malware, and ransomware early and isolates them promptly to prevent propagation.* |

| | | | | |
|---|---|---|---|---|
| | X | Manual monitoring, maintenance, and intervention for legacy systems | *Legacy systems often lack modern security updates and support, increasing the risk of vulnerabilities and attacks if not manually monitored and maintained consistently.* | *Perform manual monitoring and regular maintenance on legacy systems, with prompt intervention to address issues or vulnerabilities, alongside planning for system replacement or upgrades to enhance security.* |
| | X | Encryption | *Encryption is not currently implemented for data transmission, leaving information vulnerable to interception. Implementing encryption would provide essential protection to ensure data confidentiality during sending and receiving.* | *Implement encryption for data in transit to minimize the risk of interception and prevent successful breaches, as encrypted data cannot be understood without the appropriate decryption key. Use standard encryption protocols such as **AES** for data at rest and **TLS** for data in transit to ensure data confidentiality and enhance overall security.* |
| X | | Password management system | *A Password Management System helps securely store and generate strong passwords, while allowing secure sharing within the team without revealing* | *Implementing a Password Management System ensures encrypted and secure password storage, enables strong password generation, and allows access control, thereby improving* |

| | | | | |
|---|---|---|---|---|
| | | | *the actual credentials, reducing the risk of exposure or misuse.* | *security and minimizing risks associated with manual password handling.* |
| | X | Locks (offices, storefront, warehouse) | *Lack of proper locks on offices, storefronts, or warehouses increases the risk of unauthorized physical access to equipment or sensitive data, compromising the organization's physical security.* | *Install secure, certified locks in offices and critical areas such as storage rooms and server rooms, with controlled access and logging to prevent intrusion or theft.* |
| X | | Closed-circuit television (CCTV) surveillance | *Internal and external surveillance cameras have been installed in the company, enhancing monitoring capabilities and asset protection.* | *The CCTV system provides recordings that can be reviewed for investigating breaches, thefts, or suspicious activities. Regular review of footage is recommended to ensure system effectiveness.* |
| | X | Fire detection/prevention (fire alarm, sprinkler system, etc.) | *The absence of an effective fire detection and prevention system increases the risk of severe damage to the facility, potentially causing* | *Install fire alarm systems alongside automatic sprinkler systems in critical areas to ensure early detection and immediate response to fires, with regular maintenance and* |

| | | | | |
|---|---|---|---|---|
| | | | *significant financial and human losses. system.* | *testing of these systems.* |

## Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

| Yes | No | Best practice | *Explanation* | *Recommendation* |
|---|---|---|---|---|
| | X | Only authorized users have access to customers' credit card information. | *Access to customers' credit card information is restricted to authorized users only, minimizing the risk of unauthorized access and protecting sensitive data.* | *Ensure strict access controls are implemented so that only authorized personnel can access credit card information. Regularly review and update user permissions to maintain security compliance.* |
| | X | Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment. | *Credit card information is currently unencrypted, and all employees have unrestricted access to internal data, including customers' credit card* | *It is essential to implement strong encryption for all credit card data at rest and in transit, along with restricting access permissions so that only authorized personnel can view this data. Strict access controls and regular* |

| | | | | |
|---|---|---|---|---|
| | | | *information, exposing the data to risks of unauthorized exposure or misuse.* | *permission reviews should also be enforced.* |
| | X | Implement data encryption procedures to better secure credit card transaction touchpoints and data. | *Data encryption procedures have not been implemented to better secure credit card transaction touchpoints and related data, exposing the data to risks of interception or breaches.* | *Strong encryption procedures must be implemented to protect credit card transaction touchpoints and related data during transmission and storage. It is recommended to use standardized protocols such as **TLS** for data in transit and **AES** for data at rest to reduce the risk of interception and breaches.* |
| | X | Adopt secure password management policies. | *Secure password management policies have not been adopted, increasing the risk of weak or reused passwords, which exposes systems to potential breaches.* | *It is essential to adopt strict password management policies including strong password creation, regular changes, restricting password sharing, and encouraging the use of password management tools.* |

General Data Protection Regulation (GDPR)

| Yes | No | Best practice | *Explanation* | *Recommendation* |
|---|---|---|---|---|
| | | E.U. customers' data is kept private/secured. | *E.U. customers' data is kept private and* | *Maintain continuous enforcement of security and privacy* |

| | | | | |
|---|---|---|---|---|
| X | | | *secured in accordance with data protection and privacy requirements, ensuring personal information is safeguarded from unauthorized access or use.* | *policies compliant with the General Data Protection Regulation (GDPR), with regular reviews to ensure data protection and privacy preservation.* |
| X | | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. | *A clear plan is in place to notify E.U. customers within 72 hours in the event of a data breach, as required by GDPR, ensuring transparency and timely incident response.* | *Regularly test and update the data breach notification procedure to ensure readiness, accuracy, and compliance with GDPR timeframes.* |
| | X | Ensure data is properly classified and inventoried. | *Data is not currently classified or inventoried properly, which makes it difficult to determine where sensitive information resides, increasing the risk of unauthorized access or unintentional exposure.* | *Establish and maintain a comprehensive data classification and inventory system to identify, label, and manage sensitive data according to its level of risk and sensitivity. This will support access control, protection, and compliance efforts.* |
| | | Enforce privacy policies, procedures, | *Privacy policies, procedures, and* | *Develop and enforce clear privacy policies* |

| | | | | |
|---|---|---|---|---|
| | X | and processes to properly document and maintain data. | *processes are not currently enforced, leading to inconsistencies in how data is documented, handled, and maintained. This increases the risk of non-compliance and data misuse.* | *and procedures to ensure consistent documentation, handling, and maintenance of data in compliance with privacy regulations such as GDPR. Provide training to employees and regularly audit processes.* |

System and Organizations Controls (SOC type 1, SOC type 2)

| Yes | No | Best practice | *Explanation* | *Recommendation* |
|---|---|---|---|---|
| X | | User access policies are established. | *User access policies are established, providing clear guidelines on how access to systems and data is granted, modified, and revoked. This helps ensure that only authorized users can access sensitive information.* | *Continue enforcing and reviewing access policies regularly to adapt to organizational changes and maintain the principle of least privilege. Conduct periodic audits to ensure compliance.* |
| | | Sensitive data (PII/SPII) is confidential/private. | *Sensitive data, including PII and SPII, is not currently* | *Implement strong data classification, encryption, and* |

| | | | | |
|---|---|---|---|---|
| | X | | *treated as confidential or protected appropriately, which significantly increases the risk of data breaches, identity theft, and non-compliance with privacy regulations such as GDPR.* | *access control measures to ensure all PII/SPII is handled as confidential. Establish privacy policies and train employees to safeguard sensitive information.* |
| X | | Data integrity ensures the data is consistent, complete, accurate, and has been validated. | *Data integrity is maintained, ensuring that information remains consistent, complete, accurate, and properly validated throughout its lifecycle. This supports reliable decision-making and compliance with regulatory standards.* | *Continue implementing data integrity controls such as input validation, error-checking, and audit trails. Regularly review data handling processes to prevent corruption or unauthorized modifications.* |
| | X | Data is available to individuals<br><br>authorized to access it. | *Currently, all employees have access to data regardless of their role, which increases the risk of data misuse,* | *Implement role-based access controls (RBAC) to ensure that only employees who need access to specific data for their job functions can* |

| | | | | |
|---|---|---|---|---|
| | | | *unintentional exposure, and potential security breaches. Access is not restricted based on job responsibilities.* | *access it. Enforce the principle of least privilege and conduct regular access reviews.* |

---

## *Author's Note :*

This checklist was developed independently by *Basma Mounir Mahmoud Ayash* as part of the **Google Cybersecurity Professional Certificate**. The activity demonstrates my ability to analyze an organization's security controls, identify compliance gaps, and provide practical recommendations based on industry standards.