INFOSECTRAIN

# THIRD PARTY INFORMATION SECURITY ASSESSMENT CHECKLIST

## BUILD SECURITY GOVERNANCE

INFOSECTRAIN

# Vendor's Information

| Requested information | Response |
|---|---|
| Vendor Name | |
| Name of person and position filling this questionnaire | |
| Completer address of the Vendor | |
| Vendor Telephone Number | |
| Vendor Contact Name & Job Title | |
| Vendor Contact Email | |
| Vendor D&B Number | |
| Is the vendor a public or private company? | |
| How long has the vendor been in business under any name? | |
| Does the vendor hold any Information security related certifications? | |
| Type of legal entity and state of incorporation | |
| Are there any material claims or judgements against the vendor? | |
| If yes, describe the impact it may have on the services in scope of this document? | |
| Has the vendor sufffered a data loss or a security breach in the last 3 years? | |
| If yes, please describe the loss or breach. | |
| What is the physical address of the backup site? | |
| Are there any additional locations where Scooped System and Data is stored? | |
| If yes, please provide each location (address, city, state, or country) | |

*Source: PCI DSS & Shared Security Assessment

INFOSECTRAIN

# RISK Questions

| Vendor Question | Vendor Response (Y/N) | EVIDENCE |
|---|---|---|
| **Information Security Governance** | | |
| **Q1.** Is there a specific position dedicated to information security within the organization (CISO/Information Security Manager )? | | |
| **Q2.** Does the organization have an Information Security Framework? | | |
| **Q3.** Does the organization have an Information Security Strategy? | | |
| **Q4.** Is your organization performing risk assessments on an annual basis? | | |
| **Q5.** Does your organization have an information security program in place? | | |
| **Q6.** If your organization has an information security program, does it apply to all operations and systems that process sensitive data? | | |
| **Q7.** Are relevant staff and managers professionally certified in information security? | | |
| **Q8.** Does organization have security metrics to measure Information Security Program? | | |
| **Q9.** How do you prioritize your organization's most critical assets? | | |
| **Q10.** Has your organization conducted a risk assessment to identify the key objectives that need to be supported by your information security program? | | |
| **Q11.** Has your organization identified critical assets and the functions that rely on them? | | |
| **Q12.** Do you have a process in place to monitor federal, state, or international legislation or regulations and determine their applicability to your organization? | | |
| **Q13.** Does your information security function have the authority it needs to manage and ensure compliance with the information security program? | | |
| **Q14.** Is someone in the information security function responsible for liaising with units to identify any new security requirements? | | |
| **Q15.** Does the information security function report regularly to institutional leaders and the governing board on the compliance of the institution to and the effectiveness of the information security program and policies? | | |
| **Q16.** Is responsibility clearly assigned for all areas of the information security architecture, compliance, processes and audits? | | |
| **Q17.** Does your organization outsource functionalities related to security management? | | |

*Source: PCI DSS & Shared Security Assessment

| Vendor Question | Vendor Response (Y/N) | EVIDENCE |
|---|---|---|
| **Policies and Procedure** | | |
| **Q18.** Does your organization have an Information Security Policy? | | |
| **Q19.** Does your organization document, publish, and enforce security policies? | | |
| **Q20.** Does your organization document and enforce HR policies? | | |
| **Q21.** What is the time interval at which security policies are reviewed and updated? | | |
| **Q22.** Does your organization document and enforce policies for the authorized use of company email, internet, and intranet? | | |
| **Q23.** Does your organization document and enforce policies regarding the storage, use, and disposal of sensitive data? | | |
| **Q24.** Do policies and procedures adhere to and comply with privacy laws and regulations related to the security, concealment, and safeguarding of customer data? | | |
| **Q25.** Is a complete set of your organization's security policies available for review? | | |
| **Q26.** Are the penalties associated with noncompliance to your organization's policies well documented? | | |

*Source: PCI DSS & Shared Security Assessment

| Vendor Question | Vendor Response (Y/N) | EVIDENCE |
|---|---|---|
| **Compliance with Legal Requirements - Identification of applicable legislation** | | |
| **Q27.** Do you have a process to identify new laws and regulations with IT security implications? | | |
| **Q28.** Has the vendor experienced a legally reportable data breach within the past seven years? | | |
| **Q29.** Do you have procedures for the preservation of electronic records and audit logs in case of litigation hold? | | |
| **Q30.** In the event of a security incident, do you provide the consumer with the ability to perform digital forensics? | | |
| **Q31.** Are any information systems audit tools (e.g., software or data files) accessible to any users in any unprotected area? | | |
| **Q32.** Are there procedures to ensure compliance with legislative, regulatory, and contractual requirements on the use of material where intellectual property rights may be applied and on the use of proprietary software products? | | |
| **Q33.** How does your organization stay updated on changes in laws and regulations that impact your business? | | |
| **Q34.** Does your organization implement appropriate security controls to comply with relevant data protection and privacy laws and regulations (e.g., GDPR, CCPA, etc.)? | | |
| **Q35.** Has your organization ever been involved in any legal disputes or infringement claims regarding intellectual property rights? If yes, please provide details. | | |
| **Q36.** Does your organization have policies and procedures in place to prevent corruption, bribery, and unethical practices? | | |
| **Q37.** Does your organization have a formal process for reporting and addressing compliance issues or violations? If yes, please describe the process. | | |
| **Q38.** Can your organization provide documentation, such as certifications, licenses, or audit reports, to demonstrate compliance with relevant laws and regulations? | | |
| **Q39.** Is there a compliance risk management system that addresses the quality and accuracy of reported consumer data? | | |
| **Q40.** How long does your organization retain records related to compliance? What is your organization's process for record retention and disposal? | | |

*Source: PCI DSS & Shared Security Assessment

| Vendor Question | Vendor Response (Y/N) | EVIDENCE |
|---|---|---|
| **Privacy** | | |
| **Q41.** Are identified privacy risks and associated mitigation plans formally documented and reviewed by management? | | |
| **Q42.** Is there a Privacy management program? | | |
| **Q43.** Do you have a privacy policy? If yes, can you provide a copy? | | |
| **Q44.** Are reasonable resources (in time and money) allocated to mitigating identified privacy risks? | | |
| **Q45.** Is personal information collected directly from individuals? If yes, describe. | | |
| **Q46.** Are there controls in place to ensure that the collection of personal information is limited? | | |
| **Q47.** Are there controls in place to ensure that the collection and usage of personal information is limited and in compliance with applicable law? | | |
| **Q48.** Is there a compliance risk management system that addresses the quality and accuracy of reported consumer data? | | |
| **Q49.** Do policies and procedures adhere to and comply with privacy laws and regulations related to the security, concealment, and safeguarding of customer data? | | |
| **Q50.** Does the business area have an inventory of where personal information is collected, stored, processed, or managed? | | |
| **Q51.** Are the penalties associated with noncompliance to your organization's policies well documented? | | |
| **Q52.** Are there documented agreements in place with external organizations, when transferring data between a company entity and an external organization, requiring the external organization to comply with the company's privacy expectations? | | |
| **Q53.** Is there a compliance risk management system that addresses the quality and accuracy of reported consumer data? | | |
| **Q54.** Are there regular privacy risk assessments conducted? If yes, provide frequency and scope. If no, explain the reason. | | |
| **Q55.** Are controls in place to ensure that the collection and usage of personal information is limited and in compliance with applicable law? | | |
| **Q56.** Are you transparent about your data collection and processing practices? | | |
| **Q57.** How do you inform users about any updates or changes to your privacy policy? | | |
| **Q58.** How do you obtain user consent for data collection and processing? | | |
| **Q59.** What security measures do you have in place to protect personal data? | | |
| **Q60.** Is personal data processed or stored outside the country? If yes, how is cross-border data transfer regulated? | | |

*Source: PCI DSS & Shared Security Assessment

| Vendor Question | Vendor Response (Y/N) | EVIDENCE |
|---|---|---|
| **Personnel Security** | | |
| **Q61.** Do you ensure that all potential employees who can access sensitive information undergo background checks? | | |
| **Q62.** Are the employees participating in the required annual information security training? | | |
| **Q63.** Does sensitive or internal data accessible to any subvendor or contractor or third parties? | | |
| **Q64.** Does your organization store, transmit, or access PII (Personally Identifiable Information) or any other type of privacy information? | | |
| **Q65.** Do you have an ongoing training program in place to build skills and competencies for information security for members of the information security function? | | |
| **Q66.** Do you conduct Security awareness training for employees? | | |
| **Q67.** Do you conduct Post Awareness Training Phishing Campaigns? | | |
| **Q68.** Verify that personnel attends security awareness training upon hire and at least annually. | | |
| **Q69.** Interview a sample of personnel to verify they have completed awareness training and are aware of the importance of data security. | | |
| **Q70.** Does your awareness and education plan teach proper methods for managing information Security and personal/private information (Social security numbers, names, addresses, phone numbers, etc.)? | | |
| **Q71.** Are your employees able to identify and protect classified data, including paper documents, removable media, and electronic documents? | | |
| **Q72.** Are employees taught to be alert to possible security breaches? | | |
| **Q73.** Is responsibility clearly assigned for all areas of the information security architecture, compliance, processes and audits? | | |

*Source: PCI DSS & Shared Security Assessment

| Vendor Question | Vendor Response (Y/N) | EVIDENCE |
|---|---|---|
| **Physical Security** | | |
| **Q74.** Does your organization have a designated Physical Security Manager? | | |
| **Q75.** Does organization have any Physical Security Policy? | | |
| **Q76.** Does Controls access to server rooms follows the least privilege and need-to-know practices for those facilities? | | |
| **Q77.** Does Controls access to secure areas. e.g. key distribution management (both physical and electronic), paper/electronic logs, monitoring of facility doors, etc.? | | |
| **Q78.** Are special safeguards in place for computer rooms. e.g. cipher locks, restricted access, room access log, card swipe access control, etc.? | | |
| **Q79.** Are desktops that display confidential information positioned to protect against unauthorized viewing? | | |
| **Q80.** Are all visitors escorted to computer rooms or server areas? | | |
| **Q81.** Are appropriate environmental controls applied where possible to manage equipments, e.g., fire safety, temperature, humidity, battery backup, etc? | | |
| **Q82.** Does Team follow forensically secure data destruction processes for confidential data on hard drives, tapes & removable media when it's no longer needed and at the end of the contract term? | | |
| **Q83.** Does organization have Redundant UPS for Critical Server? | | |
| **Q84.** Does external signage indicating the content or value of the server room or any room containing confidential customer information. | | |

*Source: PCI DSS & Shared Security Assessment

| Vendor Question | Vendor Response (Y/N) | EVIDENCE |
|---|---|---|
| **Contingency Plan** | | |
| **Q85.** Does your Company have a written Policy for BCP? | | |
| **Q86.** Does your Company have a BCP/DR Plan? | | |
| **Q87.** Does your Company have emergency procedures and responsibilities documented and stored securely at multiple sites? | | |
| **Q88.** Does your Company store backup media in a secure manner and controls access? | | |
| **Q89.** How often are backups scheduled? | | |
| **Q90.** Is the BCP/DR Plan tested on a regular basis? | | |
| **Network Security** | | |
| **Q91.** Are logical segmentation used to isolate systems containing sensitive data? | | |
| **Q92.** Examine documented procedures to verify there is a formal process for testing and approval of all network connection | | |
| **Q93.** Inspect if the firewall auto-configuration standards comply with the documented security standards. | | |
| **Q94.** Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to data, including any networks. | | |
| **Q95.** Does your Solutions offer Content security to protect your network from viruses, spam, spyware, and other attacks? | | |
| **Q96.** Is it possible for employees to access sensitive information using their personal devices? | | |
| **Q97.** Are there DLP\EDR\IPS/IDS in use? | | |
| **Q98.** Does a Secure wireless network provide safe network access to visitors and employees on the go? | | |
| **Q99.** Does Compliance validation make sure that any device accessing the network meets your security requirements? | | |
| **Q100.** Are logs generated and retained for critical network devices and security systems? | | |
| **Q101.** Is network traffic continuously monitored for suspicious activities? | | |
| **Q102.** Are firewalls and routers properly configured to control traffic flow? | | |

*Source: PCI DSS & Shared Security Assessment

| Vendor Question | Vendor Response (Y/N) | EVIDENCE |
|---|---|---|
| **Access Control** | | |
| **Q103.** Are physical access controls in place to secure server rooms, data centers, and other critical areas? | | |
| **Q104.** Is there a documented process for granting, modifying, and revoking user access rights | | |
| **Q105**. Are access rights granted based on the principle of least privilege? | | |
| **Q106.** Is it mandatory for users to have complex passwords? | | |
| **Q107.** What is the frequency of the mandatory password change? | | |
| **Q108.** Is it mandatory for all users to have unique user IDs? | | |
| **Q109.** Ensures that critical data, or systems, are accessible by at least two trusted and authorized individuals in order to limit having a single point of service failure. | | |
| **Q110.** Ensures that users have the authority to only read or modify those programs or data which are needed to perform their duties. | | |
| **Q111.** How soon after a worker or contractor gets terminated may access be revoked? | | |
| **Operations Security** | | |
| **Q112.** Is there adequate wireless security in the enterprise? Are access points configured with WPA2 or any higher? | | |
| **Q113.** Are applications security DAST/SAST tests performed on them if the vendor offers applications as part of their service? | | |
| **Q114.** Is the implementation of operating system and application patches in accordance with your policy? | | |
| **Q115.** Are Vulnerability Assessment and Penetration Tests conducted on a quarterly basis at minimum? | | |
| **Q116.** Are Antivirus installed in desktop and server ? | | |
| **Q117.** What is the frequency of updating the antivirus signature files? | | |

*Source: PCI DSS & Shared Security Assessment

| Vendor Question | Vendor Response (Y/N) | EVIDENCE |
|---|---|---|
| **Mobile Managment** | | |
| **Q118.** Does your organization have a media sanitization process? | | |
| **Q119.** Does the vendor support integration with Mobile Device Management (MDM) solutions? | | |
| **Q120.** Can the app enforce organization-specific security policies (e.g., password policies, screen lock)? | | |
| **Q121.** Does the app account for Bring Your Own Device (BYOD) scenarios, where personal and work data may coexist? | | |
| **3rd Party Insurance Coverage - Complete this Section in Consultation with your Risk Management Consultant** | | |
| **Q122.** Is there a written contract between the Organization and the vendor? | | |
| **Q123.** **Does the contract include the organization Indemnification and hold** harmless language in favor of the Organization ? | | |
| **Q124.** Is there a contract term that forbids the vendor or their insurance carrier from waiving the organization reimbursement rights? | | |
| **Q125.** Is the contract structured to mandate the vendor to include the organization as an "Additional Insured" on the vendor's Cyber Liability Policy? | | |
| **Q126.** Does the contract require that the vendor provide the organization with a copy of the endorsement to the vendor's Cyber Liability Policy indicating the organization an "Additional Insured" on the policy? | | |
| **Q127.** Does the vendor have an insurance policy to cover losses ? | | |
| **Q128.** Does the Cyber Liability Policy include 3rd Party Coverage, encompassing Privacy & Security, Media, and Privacy Regulatory requirements? | | |
| **Q129.** Does the coverage encompass loss, theft, or failure to protect PII or confidential information (including violation of any related privacy/security laws/regulations), as well as failure to prevent a security breach and comply with your own privacy policies? | | |
| **Q130.** Does the Cyber Liability Policy offer "Breach Response" services or reimbursement for the cost of breach response services? | | |
| **Q131.** Ensure that subcontractors' insurance policies align with the vendor's obligations. | | |
| **Q132.** Are the limits of the Errors & Omissions Insurance at least $5,000,000 Each Claim and $5,000,000 Annual Aggregate? | | |
| **Q133.** Check the authenticity of the certificates by contacting the insurance provider directly | | |

*Source: PCI DSS & Shared Security Assessment

| | | |
|---|---|---|
| **Q134.** Check if the vendor has an Umbrella or Excess Liability Insurance policy to provide additional coverage above the primary policies. | | |
| **Q135.** Does the vendor use secure communication protocols like HTTPS, TLS, or VPNs when transmitting sensitive data over networks? | | |
| **Q136.** Are SSL/TLS certificates valid and up to date? | | |
| **Q137.** Does the vendor encrypt sensitive data stored in databases or storage systems? | | |
| **Q138.** Does the vendor utilize secure file transfer mechanisms for sharing sensitive data with authorized parties? | | |
| **Q139.** Does the vendor comply with any specific cloud encryption requirements mandated by your organization? | | |
| **Q140.** Are data backups encrypted to protect sensitive information in case of data loss? | | |
| **Q141.** Can the vendor provide documentation regarding their encryption practices and compliance efforts? | | |
| **Q142.** If the vendor uses cloud services, do they encrypt data stored in the cloud? | | |
| **Q143.** Does the vendor use data masking techniques to protect sensitive data during testing and development? | | |

*Source: PCI DSS & Shared Security Assessment

# Found this useful?

To Get More Insights Through our ***FREE***

***Courses | Workshops | eBooks |***

***White Paper | Checklists | Mock Tests***

**Press the 🔔 Icon and Follow**

INFOSECTRAIN