ABN·AMRO

Vendor Security Standard

1. Introduction

ABN AMRO has developed a Vendor Security Standard that defines the control objectives that the vendors of the Bank, need to implement to demonstrate a minimum acceptable level of information security. The control objectives are aligned with ISO 27001 and industry best practices. For the purpose of this Standard, 'ABN AMRO' or 'Bank' means ABN AMRO Bank N.V. or any of its group members that has decided to incorporate this Vendor Security Standard into its agreement with the vendor.

2. Purpose and scope of the standard

The Vendor Security Standard defines the minimum acceptable level of information security controls to be implemented by ABN AMRO vendors to minimise information security risks to the Bank. This standard addresses organisation level security controls on the vendor's internal organisation. Unless ABN AMRO is specifically mentioned, these control objectives are applicable for the vendor organisation and not limited to the services offered to ABN AMRO.

The Vendor Security Standard will be subjected to periodic review and update (if necessary) to ensure reasonable alignment with industry best practices and international security standards. The vendor must ensure its continuous compliance with the control objectives of this standard.

3. Standard principles and rules- Vendor Security Monitoring and Non-Compliancy

The vendor must agree to the following security monitoring activities.

3.1. Due-Diligence – Contracting phase: new vendors

3.1.1. The vendor must cooperate with a due diligence security assessment, addressing at least the security objectives described in this standard.

3.1.2. If the vendor does not meet all control objectives, the vendor is responsible to develop and implement a remediation plan to meet the remaining control objectives. The control objectives described in the Vendor Security Standard and any agreed remediation plans must be included in the contractual agreement with the vendor.

3.2. Continuous Monitoring phase: existing vendors

3.2.1. The vendor must cooperate with an annual security self-assessment, addressing at least the security objectives described in this standard.

3.2.2. In addition to the above continuous monitoring requirements, ABN AMRO, following a risk based approach, might select the vendor for in depth assessments (namely deep-dive assessments) to measure compliance with the control objectives of this standard. The vendor is responsible to cooperate with ABN AMRO in these deep dive assessments. Due care will be taken from ABN AMRO to ensure minimum disruption for the vendor. During the deep-dive assessment, the vendor must show proof of design, implementation and operational effectiveness of the control objectives, as listed in section 4, within their organisation.

3.3. Non-compliancy to the control objectives

3.3.1. In the case of a non-compliance with the control objectives described in section 4, the vendor is responsible to cooperate with ABN AMRO to address any identified non-compliances in a timely manner.

3.3.2. The vendor is responsible to take the necessary action to remediate any identified non-compliance.

4. Control Objectives

The design and operating effectiveness of vendor's (including its subcontractors) internal controls provide reasonable assurance (see also control objective 4.16.1) that the following control objectives are being met:

4.1. Governance

4.1.1. The vendor must have documented and implemented information security policies and topic-specific security policies (e.g., asset management, access control, etc.). These policies must be reviewed by the vendor to ensure applicability and effectiveness at least annually. These policies must be compliant with international standards and industry best practices.

4.1.2. The vendor must have defined and allocated information security roles and responsibilities.

4.1.3. The vendor must identify and ensure that conflicting duties and areas of responsibility are segregated (segregation of duties principle).

4.1.4. The vendor must have an Information Risk Management process in place to identify, respond, treat, monitor, and report on information security risks at least annually. A remediation plan, based on the vendor's risk appetite, must be developed, tracked to completion, and regularly reported to senior management. The process must be based on a documented risk assessment methodology. The vendor must report to ABN AMRO any security risks impacting ABN AMRO and how and when these risks will be treated.

4.1.5. The vendor must have information security risks considered in every project.

4.2. Human Resources Security

4.2.1. The vendor must perform pre-employment screening of all personnel (including full-time, part-time, and temporary workers) and contractors before the start of employment, in accordance with relevant laws and legislations, the role of the personnel, and the classification of information they might have physical and/or logical access to. The pre-employment screening must include at least the following, where allowed by local legislation and applicable for the employee or contractor role: criminal record check and verification of identity, education, and employment history.

4.2.2. The vendor must ensure that all personnel, including contractors and third parties, have signed relevant Confidentiality or Non-Disclosure Agreements (NDAs).

4.2.3. The vendor must provide their employees and relevant contractors with appropriate security awareness education and training at least annually. Information security training and awareness must address at least the following:

- information classification and relative controls
- incident reporting
- data privacy
- phishing and social engineering management
- working from home controls
- security roles and responsibilities
- acceptable use of assets
- physical security controls
- password management.

4.2.4. The vendor must have an established and communicated disciplinary process for personnel who have committed information security policy violations,

in accordance with relevant laws and regulations.

4.3. Identity and access management

4.3.1. The vendor must have documented and implemented Joiners, Movers, and Leavers processes to ensure access to information, assets, and facilities is adequately managed.

4.3.2. The vendor must have controls in place to ensure logical access to information and assets is allowed only upon authorization and on a need-to-know basis (least privilege principle).

4.3.3. The vendor must limit the allocation and use of privileged access rights on a need-to-know basis (least privilege principle). Privileged account use must be monitored and restricted.

4.3.4. The vendor must have a process by which passwords (including temporary) are managed, secured, stored and issued.

4.3.5. The vendor must ensure that each employee or contractor has a unique user account, and the access is revoked as soon as the user does not have the relevant business need.

4.3.6. The vendor must not allow the use of shared accounts. If that is not technically or operationally feasible, controls must be in place to monitor shared accounts and uniquely identify the user accessing the shared account at any given time.

4.3.7. The vendor must register non-personal accounts (e.g., system accounts), assign ownership of these accounts, and never log in using non-personal system accounts for operational tasks.

4.3.8. The vendor must review and revalidate all user and system access rights at least annually. For privileged accounts, review and revalidation must be performed at least quarterly.

4.3.9. The vendor must use multi-factor authentication to access internet-facing and critical systems.

4.4. Information Protection

4.4.1. The vendor must classify information and assets based on confidentiality, integrity and availability. The classification level assigned to ABN AMRO information cannot be less than the corresponding classification provided by ABN AMRO.

4.4.2. The vendor must document and implement an encryption management policy and relevant procedures. Additionally, controls to protect private/public keys must be in place in a way to limit physical and logical access to the keys.

4.4.3. The vendor must have controls in place to protect information in transit, at rest, and during processing, in accordance with the information's classification level.

4.4.4. The vendor must implement adequate data leakage prevention and detection measures to protect against unauthorized disclosure and extraction of information by individuals or systems.

4.4.5. The vendor must have controls in place to prevent installation and/or usage of unauthorized software, applications or SaaS (Software-as-a-Service).

4.4.6. The vendor must ensure malware detection software is installed and regularly scans all applicable systems. The malware detection definition files must be updated at least daily.

4.4.7. The vendor must define and implement remote working and Working From Home (WFH) controls to minimize related information security risks. These controls must include at least, secure remote connection, security awareness on remote working and security incident reporting, device management for mobile devices (including laptops).

4.4.8. The vendor must periodically delete information provided by ABN AMRO if no longer required, as per agreed retention requirements.

4.5. Cloud Security

4.5.1. The vendor must risk assess and document the use of cloud services.

4.5.2. The vendor must address at least the following in all internal or external cloud services agreements:

- security roles and responsibilities
- access controls
- information protection controls, including data retention and encryption controls
- physical security controls
- security incident prevention and detection
- unauthorised usage detection and prevention
- network security controls
- patch and vulnerability management controls
- malware protection
- availability requirements

These controls must be included in the contractual agreements with the vendor's third parties involved in the cloud service and must be cascaded to possible fourth, fifth, etc. parties involved in the cloud service.

4.6. Asset Management

4.6.1. The vendor must define, document, and implement acceptable use policies for all company assets, including information assets.

4.6.2. The vendor must maintain an up-to-date asset inventory of all software and hardware assets, including servers, endpoints, IoT (Internet of Things) and mobile devices including Bring Your Own Device (BYOD). The inventory must be reviewed and revalidated at least annually.

4.6.3. The vendor must have controls in place to enrol mobile devices, including BYOD, to device management.

4.6.4. The vendor must have processes in place to ensure employees or contractors return company or client assets upon change or termination of employment, assignment, contract, or agreement.

4.6.5. The vendor must ensure that storage media are managed throughout their lifecycle, including disposal, in accordance with the classification of the information they contain and best practices.

4.6.6. The vendor must implement controls to ensure sensitive data or licensed software have been securely removed or overwritten before re-use or disposal of equipment.

4.6.7. The vendor must agree on an exit strategy with ABN AMRO addressing among others, secure data disposal, knowledge transfer, data migration, etc.

4.7. Security Incident Management

4.7.1. The vendor must have defined, communicated, and implemented security incident management processes, including relevant roles and responsibilities. These processes must address at least incident reporting, incident response, collection of evidence, and lessons learned.

4.7.2. The vendor must provide a mechanism to all personnel to report security events or incidents in a timely manner. This mechanism must be communicated to all personnel.

4.7.3. The vendor must have controls in place to prevent, detect, respond to, and recover from malware, ransomware, DDoS (distributed-denial-of-service), and other cyber-attacks.

4.7.4. The vendor must configure systems and software to produce security logs for all users, networks, systems and application to be able to detect and analyse security events. These log files must be retained and protected against unauthorized access and tampering. Additionally, the vendor must monitor and analyse those logs to detect any suspected or actual information security incident in a timely manner. Log analysis reports of an incident impacting ABN AMRO must be shared, when requested.

4.7.5. The vendor must monitor and manage security incidents. In case critical security incidents potentially impact ABN AMRO, the vendor must notify ABN AMRO without undue delay after the discovery of the incident.

4.7.6. The vendor must ensure that all systems are synchronized to approved time sources to enable the correlation and analysis of security related events and to support investigations into information security incidents.

4.8. Software & System Development

4.8.1. The vendor must have a documented and implemented secure development policy, which must include at least the rules for the secure development of software and systems within the organization and relevant requirements when this process is outsourced.

4.8.2. The vendor must have segregated development, testing, and production environments.

4.8.3. The vendor must ensure that security requirements and security functionality testing are an integral part of the system and application development or acquisition process. Security requirements and functionality must be reviewed, tested, and approved at each stage of the development or acquisition process.

4.8.4. The vendor must monitor and restrict access to source code, development tools, and software libraries on a need-to-know basis.

4.8.5. The vendor must store source code in source code management systems with clear processes, defined roles, and responsibilities on when the code can be promoted to production and who is responsible to do so.

4.8.6. The vendor must define controls to select or create test data and test environments.

4.8.7. The vendor must not use live/production data for testing or development purposes. If live/production data is required for testing or development purposes, the data must be offered the same level of protection as the production environment, at all layers (e.g., infrastructure, system, application, etc.). Specifically for ABN AMRO data, it must not be used for testing or development purposes unless formally agreed with

ABN AMRO.

4.9. Network Security

4.9.1. The vendor must maintain (an) up-to-date network diagram(s) covering all networks of the organization.

4.9.2. The vendor must implement network segregation to separate critical networks from external-facing and other less sensitive networks.

4.9.3. The vendor must implement web filtering controls to reduce exposure to malicious content.

4.9.4. The vendor must implement secure network perimeter considering the following:

- network firewalls limiting access to sensitive resources
- DoS and DDoS protection mechanisms
- logging and monitoring of network traffic
- network threat detection and protection mechanisms
- vulnerability management controls
- authorisation and authentication controls before accessing network resources, and
- encryption of information in transit.

4.10. Security Operations

4.10.1. The vendor must have change be controlled and subject to a formalized change management process applied throughout the change cycle: requests, prioritisation, approval, scheduling and implementation including communication to affected stakeholders.

4.10.2. The vendor must define processes to securely manage and implement changes to production environment, including emergency changes. These processes must include controls to ensure at least that:

- a rolling back strategy is implemented
- acceptance testing has been performed based on defined criteria
- appropriate authorisations have been granted before migrating to production
- changes are performed by skilled individuals
- the changes do not introduce new vulnerabilities or reduce the security status of the system or application

4.10.3. The vendor must ensure that changes and auditing activities on production systems are performed with minimum impact on operations and business processes. Change and auditing activities impacting ABN AMRO must be previously agreed with ABN AMRO.

4.10.4. The vendor must define and implement hardening configurations to all device types, including servers, endpoints, network devices, mobile and IoT (Internet of Things) devices, in accordance with industry best practices, international standards and applicable legal and/or regulatory requirements. The vendor must review these standards at least annually to ensure their continuous effectiveness. The vendor must audit compliance with the hardening standards at least annually and if required perform corrective actions in a timely manner.

4.10.5. The vendor must ensure that privileged utility programs that can override system and application controls must be restricted and strictly controlled.

4.11. Vulnerability Management

4.11.1. The vendor must perform technical vulnerability assessments at least monthly via automated scanning tools for all information systems and assets. Vulnerability assessment reports for the information systems and assets involved in the services offered to ABN AMRO must be shared with ABN AMRO upon request.

4.11.2. The vendor must perform industry-recognized third-party penetration testing at least annually for all critical systems and applications, covering both internal and external facing components. Penetration testing reports for the information systems and assets involved in the services offered to ABN AMRO must be shared with ABN AMRO.

4.11.3. The vendor must define and implement appropriate timelines to fix or mitigate vulnerabilities, addressing systems at high risk first, depending on severity and how urgently a technical vulnerability needs to be addressed, following industry best practices and contractual requirements.

4.12. Physical Security

4.12.1. The vendor must define and implement a Joiners, Movers and Leavers (JML) process for physical access rights to only allow people with authorised access to information processing facilities on a need-to-know basis. These access rights must be reviewed and revalidated at least annually.

4.12.2. The vendor must define and implement appropriate physical security controls to protect secure areas including rooms, offices and facilities from unauthorized physical access, damage and interference and detect such attempts e.g., CCTV, access cards, visitor cards, security guards etc.

4.12.3. The vendor must define, implement, and monitor appropriate controls to protect important infrastructure and equipment against environmental threats.

4.13. Third-Party Security Risks

4.13.1. The vendor must have a Third-Party Security Risk Management program in place to identify, continuously monitor, and minimize security risks stemming from its third parties.

4.13.2. The vendor must include its own right to audit within its third-party contracts and periodically exercise this right following a risk-based approach.

4.13.3. The vendor must establish, agree, document, monitor and assess compliance against relevant information security requirements within its third-party contracts in accordance with industry best practices and international standards.

4.13.4. In case the vendor subcontracts any part of the services/products offered to ABN AMRO, the vendor must ensure that information security requirements are formally agreed and implemented with all involved subcontractors and that the subcontractors offer at least the same level of protection to ABN AMRO data and assets as agreed and contracted with the vendor.

4.14. Business Continuity

4.14.1. The vendor must have defined, implemented, and annually tested business continuity and disaster recovery plans for all services/products offered to ABN AMRO. These plans must address timely recovery of products/services offered to ABN AMRO in accordance with agreed contractual requirements. Testing results of these plans must be communicated to ABN AMRO, when requested.

4.14.2. The vendor must implement redundancies for critical information systems, software, and facilities to meet agreed availability requirements.

4.14.3. The vendor must have controls in place to identify, monitor and report on capacity requirements for infrastructure, facilities, and human resources to ensure timely allocation of related resources and continuity of operations.

4.14.4. The vendor must maintain backups of information, systems, and software to enable data and system recovery. Backup and restore tests must be regularly performed in accordance with industry best practices and availability requirements.

4.14.5. The vendor must store backup data in a separate location from where the original data is processed and stored. Both locations must offer the same adequate level of protection.

4.15. Compliance

4.15.1. The vendor must identify, document, and maintain up-to-date relevant legal, regulatory, and contractual security requirements that affect its operation, including the services/products offered to ABN AMRO.

4.15.2. The vendor must identify and comply with relevant data privacy legislation and adequately protect the privacy of personal data.

4.15.3. The vendor must perform at least annually a gap analysis to assess compliance with its information security policies, legal, regulatory and contractual requirements. In case non-compliances impacting ABN AMRO are detected, the vendor must develop and implement appropriate remediation plans, and share those with ABN AMRO.

4.15.4. The vendor must allow ABN AMRO the right to verify adherence to this standard at least annually, upon prior notification from ABN AMRO. Due care will be taken from ABN AMRO to ensure minimum disruption for the vendor.

4.16. Security Assurance

4.16.1. The vendor must provide security assurance via relevant security certifications, assurance reports, or external audit reports covering at least the control objectives mentioned in this standard. Such assurance must cover at least the services/products offered to ABN AMRO on an ongoing basis and be shared with ABN AMRO at least annually.