ABN·AMRO

Chief Architect & Data Management

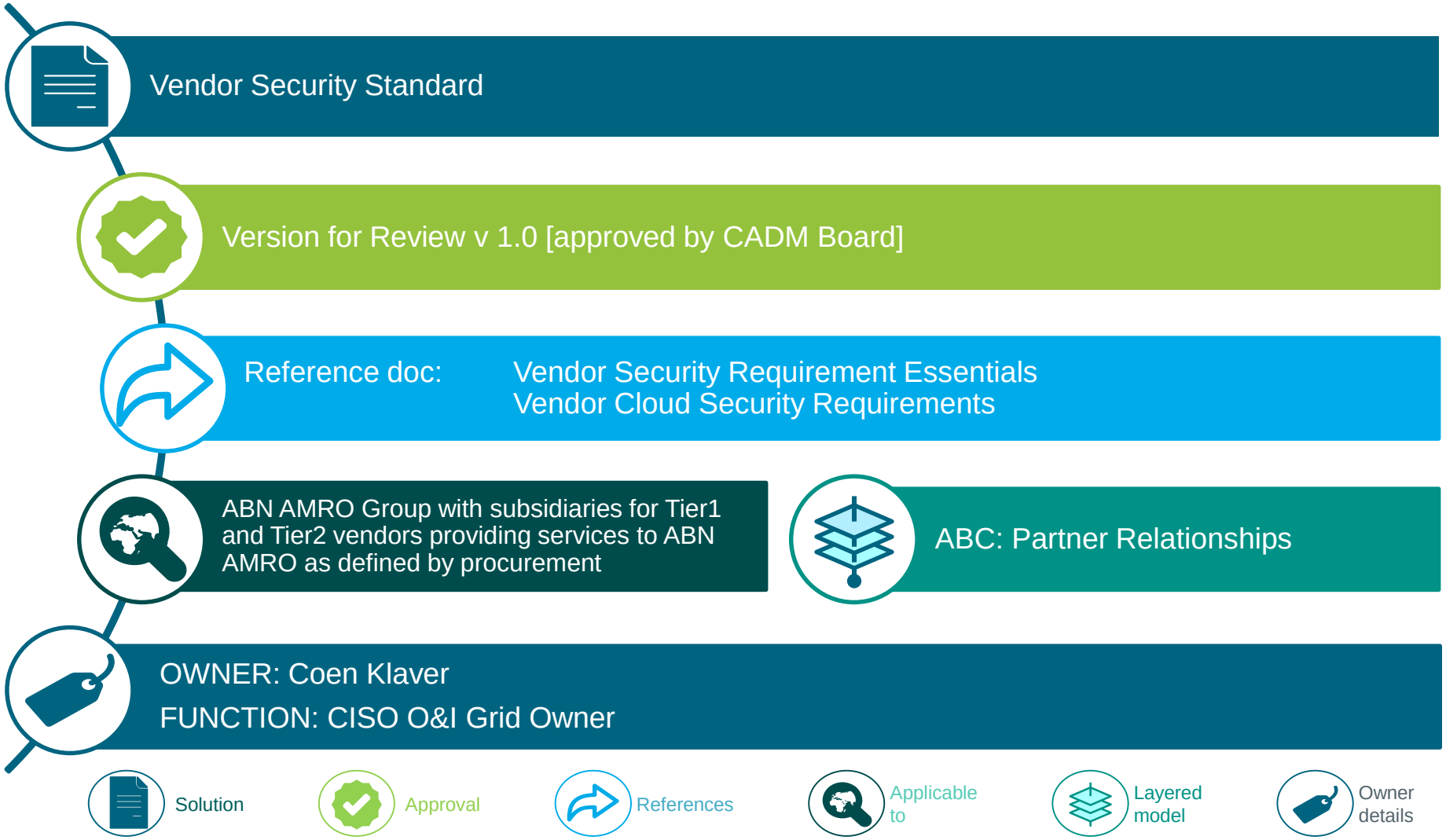
# Vendor Security Standard

18 November 2020

# Version management

| Version | Changes | Author |
|---|---|---|
| 1.0 | Version ready for approval<br>Approved by CADM Board, on 24-11-2020 | Elli Tsiala, VSS/CISO<br>Brenda van het Hul, VSS/CISO |
| | | |
| | | |

# Vendor Security Standard



# Link to Architecture Reference Models

| Impacted Business Capability (ABC) | Impacted Application Functions (ARM) | Impacted Infrastructure Functions (IRM) |
|---|---|---|
| *Partner Relationships*<br>*Vendor & Supplier Management*<br>*Sourcing*<br>*Supplier Onboarding* | *n.a.* | *n.a.* |

Grouping | ABC L1 | ABC L2 | ABC L2

# Vendor Security Standard

*This standard defines which controls need to be implemented at a minimum by vendors* providing services to ABN AMRO**. The focus of these requirements is on the WHAT, and for most of the HOW the service providing vendors are free to choose their solution.*

*Specifically, this standard is applicable for Tier1 and Tier2 vendors as defined by Procurement, including cloud-based services.*

*This document consists of three sections:*

- *First part is the overview and summary of the requirements listed in this Standard.*
- *Second part is the foundational controls which are applicable for all Tier 1 & Tier 2 vendors.*
- *Third part is the controls applicable for cloud-base service provider.*

*Any exception to these requirements should be formally communicated to and approved by ABN AMRO.*

** For the purposes of this standard the terms "Vendor", "Supplier" and "Third Party", are used interchangeably, meaning an organization outside of the ABN AMRO Group offering services or products to ABN AMRO Group.*

*** For the purposes of this standard, "ABN AMRO" refers to all ABN AMRO Group entities, including subsidiaries.*

# Vendor Security Standard – Overview & Summary

## Foundation controls

- A01. Documented security policy and periodic review of policy
- A02. Provide security awareness education and training at a minimum once a year to employees and relevant contractors
- A03. Right to audit
- A04. Agreed exit strategy in place
- A05. WFH (Working from Home) related controls in place
- B01. Documented information security risk management policy and process
- B02. Documented information security risk methodology and implementation of controls for managing and tracking the identified risks including periodic assessment of those risks
- C01. Background verification should be performed
- D01. Access policies and processes should be in place
- D02. JML (Joiner, Mover, Leaver) processes should be documented and implemented
- D03. Segregation of Duties (SOD) should be in place
- D04. Least privilege model should be implemented
- D05. Only one user account is allowed per users and access should be revoked as soon as user don't have business needs
- D06. Periodic review of access rights including timely corrective actions
- D07. Multi factor authentication should be implemented when required
- E01. Documented policy for the acceptable use of information and assets
- E02. Asset disposal policy and related procedures should be in place
- E03. Assets and associated configurations should be registered in the centralized repository
- E04. Return of assets should be integrated with the leaver process
- F01. Monitor and manage critical security incidents including notification to ABN AMRO within 24 hours
- F02. Logging and monitoring should be in place including log file protection
- F03. Adequate process to select or create Test data / Test environment should be in place
- G01. Network segmentation should be in place
- G02. Systems to be separated for test, development, and production
- H01. Vulnerability management process in place including quarterly scanning at minimum
- H02. Patch management process should be in place
- H03. Periodic industry-recognized network penetration testing should be performed
- I01. Anti-malware or anti-virus process and software should be implemented
- I02. Documented and implemented Security configuration standards
- I03. Hardening standards should be in place
- I04. Controls to ensure all adequate configurations and controls are implemented prior to production
- J01. Third party risk management and its monitoring should be in place
- J02. Documented policy to manage and control third party's access to its network
- K01. Documented and implemented change management process
- K02. Controls should in place to track and manage changes to code
- L01. Data encryption policy covering data in transit and data at rest should be in place
- L02. Documented key management policy and procedures
- L03. Documented and implemented Data Disposal Policy
- L04. Documented backup and restore policy including periodic test of backup and restore
- L05. Separate location for backup data from original data and same level of protection on backup and original data
- L06. Controls to prevent usage of unauthorized software, applications or SaaS should be in place
- L07. Comply with ABN AMRO's data retention requirements
- L08. ABN AMRO data should not be transmitted, processed or stored in any end user devices other than ABN AMRO provided devices
- M01. Documented and implemented secure development policy
- M02. Established acceptance testing programs and related criteria
- M03. Testing of security functionality should be integral part of development process
- M04. ABN AMRO data should never be used for test or development
- N01. Defined security perimeters and implemented physical and environmental controls
- N02. Secure areas should be protected by appropriate entry controls
- N03. Equipment should be sited and protected
- O01. BCP/DR should be in place and reviewed periodically. Additionally BCP/DR tests should be performed periodically
- P01. Maintain the list of applicable legal and regulatory requirements and comply with those requirements
- P02. Obtain one of the industry recognized information security certificates at least annually
- P03. Obtain one of the market standard assurance report at least annually
- Q01. Supplier should ensure controls are in place to comply with GDPR and other applicable data privacy legislations
- Q02. Supplier should have sufficient legal ground or EU model clauses in place for data transfers outside the EU/EEA

## Additional Cloud controls

- F04. Collect and review capacity information periodically
- G03. Network segregation from supplier's other clients
- L09. Client-side encryption should be supported
- O02. DoS/DDoS protection in place

## Control areas

- A. Security Governance
- B. Risk Management
- C. Human Resource Security
- D. Access Controls
- E. Asset Management
- F. Operations Security
- G. Network Security
- H. Vulnerability and Patch Management
- I. Secure Configuration
- J. Third Party Risk Management
- K. Change Management
- L. Data Protection / Data Security
- M. SDLC
- N. Physical & Environmental Security
- O. Business Continuity
- P. Compliance, Regulations and Assurance
- Q. Data privacy

# Vendor Security Standard – Foundation Controls

| Foundation Controls – Foundation controls are applicable for all suppliers, irrespective of the service they are offering to ABN AMRO Group | | | |
|---|---|---|---|
| **Nr** | **Status** | **Standard** | **Area** |
| S-A01 | New | Supplier should have a documented information security policy, which should be reviewed and updated periodically. | Security Governance |
| S-A02 | New | Suppliers should provide their employees and relevant contractors with appropriate security awareness education and training at a minimum once a year. | Security Governance |
| S-A03 | New | Supplier should allow ABN AMRO the right to audit. | Security Governance |
| S-A04 | New | Supplier should agree on an exit strategy with ABN AMRO addressing among others, data disposal, knowledge transfer, data migration, etc. | Security Governance |
| S-A05 | New | Supplier should have Working From Home (WFH)-related controls in place to minimize relative information security risks. | Security Governance |
| S-B01 | New | Information security risk management policy and process should be documented and implemented | Risk Management |
| S-B02 | New | Information security risk assessment methodology should be documented and the controls to ensure identified risks are managed and tracked appropriately should be in place. Additionally, controls to ensure identified risks are assessed periodically should be implemented. | Risk Management |
| S-C01 | New | Background verification checks on all employees and contractors should be performed, in accordance with relevant laws and regulations. | Human Resources Security |
| S-D01 | New | Access policies and processes should be documented and implemented across all supplier's organizations. | Access Controls |
| S-D02 | New | JML (Joiner, Mover, Leaver) processes should be documented, implemented. | Access Controls |
| S-D03 | New | Segregation of Duties (SOD) principle should be implemented, where applicable, to ensure preventing fraud, misuse, and errors. | Access Controls |
| S-D04 | New | Suppliers should have controls in place to limit privileges to users based on the need-to-know principle. | Access Controls |

# Vendor Security Standard – Foundation Controls

| Foundation Controls – Foundation controls are applicable for all suppliers, irrespective of the service they are offering to ABN AMRO Group | | | |
|---|---|---|---|
| **Nr** | **Status** | **Standard** | **Area** |
| S-D05 | New | Supplier should have controls in place to ensure each user has only one user account and the access is revoked as soon as the user does not have business needs. | Access Controls |
| S-D06 | New | Controls should be in place to ensure all access rights are reviewed periodically and corrective actions as a result of review should be performed within required time frame. | Access Controls |
| S-D07 | New | Multi factor authentication should be implemented when either of the following is applicable:<br>a.remote access to ABN AMRO information assets is permitted,<br>b.laptops other than ABN AMRO-provided are used, or<br>c.accessed data are classified as 'Critical' by ABN AMRO. | Access Controls |
| S-E01 | New | Supplier should have documented policy for the acceptable use of information and assets associated with information and information processing facilities. | Asset Management |
| S-E02 | New | An asset disposal policy and related procedures should be documented and implemented. | Asset Management |
| S-E03 | New | Controls should be documented and implemented to ensure all assets and associated configurations are registered in the centralized repository. | Asset Management |
| S-E04 | New | Controls to govern the return of assets integrated with the leaver process (or employee off-boarding) should be documented and implemented. | Asset Management |
| S-F01 | New | Supplier should have capabilities to monitor and manage critical security incidents and in case of those incidents, supplier should notify ABN AMRO within 24 hours since the identification of the incidents. | Operations Security |
| S-F02 | New | Logs should be collected and retained for all users and systems and log files should be protected against unauthorized access. Additionally, supplier should have capabilities to monitor and analyze those logs and provide the analysis result upon request. | Operations Security |
| S-F03 | New | Adequate processes to select or create Test data / Test environment should be in place. | Operations Security |
| S-G01 | New | Network segmentation should be in place to separate critical networks from external-facing and other less sensitive networks. | Network Security |
| S-G02 | New | Development, testing and production environments should be separated. | Network Security |

# Vendor Security Standard – Foundation Controls

| Foundation Controls – Foundation controls are applicable for all suppliers, irrespective of the service they are offering to ABN AMRO Group | | | |
|---|---|---|---|
| **Nr** | **Status** | **Standard** | **Area** |
| S-H01 | New | Vulnerability management process should be documented and implemented in the supplier's organization. Additionally, scanning to identify vulnerabilities in the environment should be performed periodically and no longer than quarterly. | Vulnerability and Patch Management |
| S-H02 | New | Supplier should have a documented patch management process, including defined timeframes to implement high or critical security patches. | Vulnerability and Patch Management |
| S-H03 | New | Industry-recognized network penetration testing should be performed periodically, covering both internal and external facing components. | Vulnerability and Patch Management |
| S-I01 | New | Supplier should have a documented policy to detect and handle malware infections and should have controls to ensure malware detection software is installed and the definition files are frequently updated on all required systems. | Secure Configuration |
| S-I02 | New | Security configuration standards for systems should be documented and implemented on all systems. | Secure Configuration |
| S-I03 | New | Supplier should have a defined and implemented hardening standard, which is based on best practices (e.g. Center for Internet Security). | Secure Configuration |
| S-I04 | New | Supplier should have controls in place to ensure all adequate configurations and controls are implemented prior to promoting to production. | Secure Configuration |
| S-J01 | New | Controls to manage third party risk (sub-contractors) should be in place including continuous monitoring of those parties' adherence to supplier's security policies and standards, and contractual agreements. | Third Party Risk Management |
| S-J02 | New | Supplier should have documented policy to manage and control third party's access to its network. | Third Party Risk Management |
| S-K01 | New | Change management process should be documented and implemented, including handling emergency changes. | Change Management |
| S-K02 | New | Supplier should have controls in place to track and manage changes to code. This also applies to software and configuration items | Change Management |

# Vendor Security Standard – Foundation Controls

| Foundation Controls – Foundation controls are applicable for all suppliers, irrespective of the service they are offering to ABN AMRO Group | | | |
|---|---|---|---|
| **Nr** | **Status** | **Standard** | **Area** |
| S-L01 | New | Supplier should have a data encryption policy covering data at rest and data in transit. Additionally, technical controls should be in place to detect and prevent data breaches. | Data Protection / Data Security |
| S-L02 | New | Key management policy/procedures should be documented and implemented across supplier's organization. Additionally, controls to protect private / public keys should be in place in a way to limit physical and logical access to the keys. | Data Protection / Data Security |
| S-L03 | New | Supplier should have a documented and implemented Data Disposal Policy aligned with industry best practice. Related controls, including data to be made unreadable prior to disposal, should be in place. | Data Protection / Data Security |
| S-L04 | New | Supplier should have a documented backup and restore policy, aligned with industry best practice. Backup and restore tests should be performed periodically. | Data Protection / Data Security |
| S-L05 | New | Back-ups of data should be stored in a separate location from where the original data is processed and stored. Both locations should have the same adequate level of protection. | Data Protection / Data Security |
| S-L06 | New | Supplier should have controls in place to prevent usage of unauthorized software, applications or SaaS. | Data Protection / Data Security |
| S-L07 | New | Supplier should comply with ABN AMRO's data retention requirements (1) | Data Protection / Data Security |
| S-L08 | New | ABN AMRO data should not be transmitted, processed or stored in any end user devices (Desktops, Laptops, Tablets, Smartphones) other than the ones provided by ABN AMRO unless otherwise agreed. Any exception to this requirement should be formally approved by ABN AMRO. | Data Protection / Data Security |
| S-M01 | New | Supplier should have a documented and implemented secure development policy, which should include at least the rules for the secure development of software and systems within the organization and relevant requirements when this process is outsourced. | SDLC |
| S-M02 | New | Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions. | SDLC |

*(1) Data retention requirements depend on the type of data involved in the supplied service. If you have any questions, please contact ABN AMRO Procurement for more information.*

# Vendor Security Standard – Foundation Controls

| Foundation Controls – Foundation controls are applicable for all suppliers, irrespective of the service they are offering to ABN AMRO Group | | | |
|---|---|---|---|
| **Nr** | **Status** | **Standard** | **Area** |
| S-M03 | New | Testing of security functionality should be integral part of development process. | SDLC |
| S-M04 | New | The supplier should never make use of ABN AMRO data for testing or development purposes. | SDLC |
| S-N01 | New | Security perimeters should be defined, and appropriate physical and environmental controls should be implemented. | Physical & environmental security |
| S-N02 | New | Supplier should ensure that secure areas are protected by appropriate entry controls to ensure only authorized personnel has access. Additionally, the access should be revalidated periodically. | Physical & environmental security |
| S-N03 | New | Supplier should ensure that equipment is sited and protected, to reduce the risks of environmental threats, hazards and opportunities for unauthorized access | Physical & environmental security |
| S-O01 | New | Supplier should have Business Continuity Plan and Disaster Recovery program (BCP/DR) in place covering the services provided to ABN AMRO, and the BCP/DR plan should be reviewed and updated periodically. Additionally, BCP/DR test should be performed periodically, and the result should be communicated to ABN AMRO when requested. | Business Continuity |
| S-P01 | New | Supplier should maintain the list of applicable legal and regulatory requirements. Controls to ensure compliance to those requirements should be in place. Additionally, these controls should be assessed periodically, and the result reports should be provided to ABN AMRO when requested. | Compliance, Regulations and Assurance |
| S-P02 | New | Supplier should obtain one of the industry recognized information security certificates at least annually and provide the scope of such certificate(s) and the Statement(s) of Applicability, where applicable. (e.g. PCI-DSS, CCSK, ISO27001, or other equivalent certifications) | Compliance, Regulations and Assurance |
| S-P03 | New | Supplier should obtain one of the market standard assurance report at least annually and provide the latest result report to ABN AMRO, such as SOC2 Type 2 or other equivalent assurance reports. | Compliance, Regulations and Assurance |
| S-Q01 | New | In case the supplier handles any ABN AMRO employees' or customers' data, it should be clearly documented what kinds of data are handled, including the classification of those data. Additionally, a data protection contract should be documented and agreed with ABN AMRO, and supplier should ensure controls are in place to comply with GDPR and other applicable data privacy legislations. | Data privacy |
| S-Q02 | New | Supplier should have sufficient legal ground or EU model clauses in place for data transfers outside the EU/EEA. | Data privacy |

# Vendor Security Standard – Additional Cloud (*) Controls

| Additional Cloud Controls – These controls apply to suppliers who offer services on the cloud | | | |
|---|---|---|---|
| **Nr** | **Status** | **Standard** | **Area** |
| S-F04 | New | Supplier should have controls in place to collect and review capacity information periodically. | Operations Security |
| S-G03 | New | Network providing services to ABN AMRO should be segregated from service to supplier's other clients. | Network Security |
| S-L09 | New | Supplier should support client-side encryption, when required. | Data Protection / Data Security |
| S-O02 | New | Supplier should have adequate DoS/DDoS protection in place. | Business Continuity |

* By cloud we mean any IaaS, PaaS, and/or SaaS solutions and services.

# Vendor Security Standard