VENDOR CYBERSECURITY COMPLIANCE PROGRAM

[NIST SP 800-53 REV4 CYBERSECURITY REQUIREMENTS]

ACME Business Consulting, LLC

Table of Contents

INSTRUCTIONS TO VENDORS

ACME's data protection strategy includes the requirement to ensure the security of data protection controls, regardless of the location or the party responsible for those controls. As a vendor, you serve a crucial role to achieve this goal and your cooperation is greatly appreciated.

All vendors are expected to meet the minimum controls identified in this document. In some cases, ACME may require a written response that may be an attestation of compliance, a submission of supporting documentation, or both.

If ACME requests a written response from your organization, you are required to submit an electronic copy of the document(s) confirming compliance. If there are any requirements that are out of scope or that cannot be complied with, those requirements must be fully explained with a business justification and if there are any compensating controls that may exist to reduce risk associated with one of ACME's vendor requirements not being met.

Please note that if your organization processes, stores or transmits ACME data that is considered “sensitive,” additional data protection controls may be required.

VENDOR COMPLIANCE POLICY

Vendors must protect the confidentiality, integrity, and availability of ACME Business Consulting, LLC (ACME) data and systems, regardless of how the data is created, distributed or stored. Vendors' security controls must be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system, in accordance with all legal obligations.

Management Intent: The successful implementation of ACME's program depends on the successful implementation of each vendor's security controls.

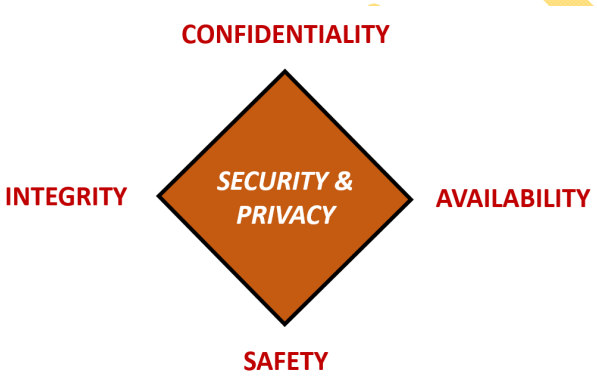
MANAGEMENT DIRECTION FOR VENDOR CYBERSECURITY

The objective of this Vendor Compliance Program (VCP) to provide direction to vendors for cybersecurity requirements that are in accordance with ACME's business requirements, as well as relevant laws and other legal obligations for data security and privacy. [1]

ACME is committed to protecting its employees, partners, clients and ACME from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every vendor that interacts with ACME data and/or systems. Therefore, it is the responsibility of VENDOR to be aware of and adhere to ACME's cybersecurity requirements.

Protecting ACME data and the systems that collect, process and maintain this data is of critical importance. Therefore, the security of systems must include controls and safeguards to offset possible threats, as well as controls to ensure the confidentiality, availability and integrity of the data:

Commensurate with risk, cybersecurity and privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes protection against accidental loss or destruction. The security of systems must include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety:



- **CONFIDENTIALITY** – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.
- **INTEGRITY** – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- **AVAILABILITY** – Availability addresses ensuring timely and reliable access to and use of information.
- **SAFETY** – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated by nefarious actors.

Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes against accidental loss or destruction.

SCOPE

The requirements of the VCP applies to all vendors, contractors, consultants, interns or other third-parties that support ACME operations. This includes all stakeholders involved in transmitting, processing and storing ACME data.

[1] ISO/IEC 27002:2013 – 5.1

Intent

ACME's **Minimum Security Requirements (MSR)** for cybersecurity are comprehensive in nature. Therefore, ACME expects VENDOR to also have a comprehensive set of cybersecurity policies, standards, procedures and controls to protect ACME's data and systems.

VENDOR's cybersecurity program must be reasonably designed to achieve the following objectives:

- Ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of ACME systems, applications, services and data;
- Perform ongoing risk management practices to maintain situational awareness of risk;
- Reasonably protect against any anticipated threats or hazards.

Cybersecurity Practices Alignment

The National Institute of Technology & Standards (NIST) Special Publication 800-53 revision 4 (rev 4) represents leading industry-accepted best practices for cybersecurity. Therefore, ACME's minimum security requirements for its vendors are consistent with NIST 800-53 rev 4 moderate baseline requirements to ensure due care and due diligence in maintaining its cybersecurity program.

Cybersecurity Documentation

In order to reduce possible confusion, VENDOR must be aware of and abide by ACME's use of terminology for cybersecurity documentation:

(1) Core policy that establishes management's intent;
(2) Control objective that identifies leading practices;
(3) Standards that provides quantifiable requirements;
(4) Controls identify desired conditions that are expected to be met;
(5) Procedures / Control Activities establish how tasks are performed to meet the requirements established in standards and to meet controls; and
(6) Guidelines are recommended, but not mandatory.

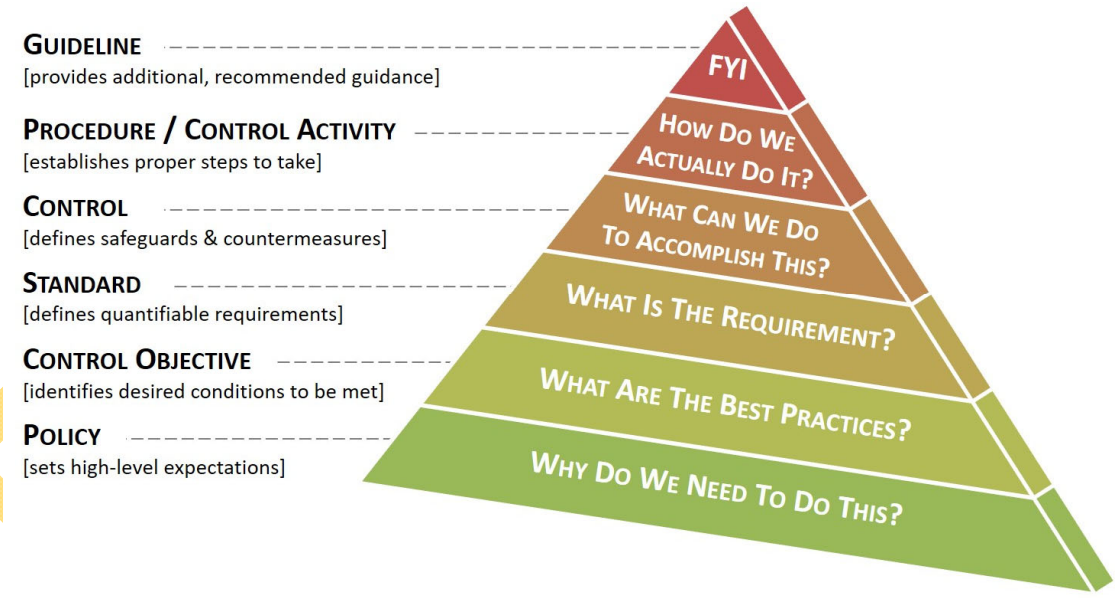


Figure 1: cybersecurity Documentation Framework

CYBERSECURITY PROGRAM MANAGEMENT (PM)

VENDOR is expected to implement IT security program management controls to provide a foundation for VENDOR's Information Security Management System (ISMS).

CYBERSECURITY PROGRAM

1. Cybersecurity Policy: VENDOR must have a documented cybersecurity policy in place which meets applicable industry standards and which is subject to review by ACME under a Non-Disclosure Agreement (NDA). This policy must be reviewed on a regular basis by VENDOR.

2. Cybersecurity Management: VENDOR must develop a data security program that documents the policies, standards, and controls in use that relate to the provisions outlined below. This security plan must include organizational, administrative, technical, and physical safeguards and standards appropriate to the size and complexity, the scope of the activities and the sensitivity of the information at issue.

3. Management Commitment: VENDOR must have executive-level direction on cybersecurity and be able to demonstrate management commitment.

CYBERSECURITY GOVERNANCE

1. Contract: Before VENDOR can collect, use, transfer or store ACME business information or systems, VENDOR must have a valid contract, statement of work, or purchase order with the privacy and security language in place.

2. Cybersecurity Function: VENDOR must have an established cybersecurity function that has VENDOR's enterprise-wide responsibility for promoting cybersecurity.

3. ACME-Specific Security Coordination: VENDOR must appoint an individual to coordinate the cybersecurity arrangements specific to ACME.

4. Cybersecurity Audit / Review: The VENDOR's cybersecurity program must be subject to thorough, independent and regular security audits/reviews.

5. Cybersecurity Architecture: VENDOR must establish a cybersecurity architecture that provides a framework for the application of standard security controls throughout the VENDOR's enterprise.

COMPLIANCE

1. Statutory / Regulatory / Contractual Compliance. VENDOR must maintain a process to be aware of and be compliant with all applicable statutory, regulatory and contractual compliance requirements. Examples include but are not limited to PCI DSS, HIPAA, SOX, and GLBA.

2. Compliance Status: VENDOR must have a process to document non-compliance of any statutory, regulatory or contractual requirement:
    a. VENDOR must identify and quantify the risks and mitigation plans and document the business decision for alternate controls or risk acceptance; and
    b. The mitigation plan and business decision must be signed off by the Chief Information Officer (CIO) or an authorized individual who can accept responsibility and accountability on behalf of the VENDOR.

3. Breach Notification: VENDOR must maintain a documented breach notification process that meets all applicable legal and contractual requirements. The ACME business owner of the solution must:
    a. Approve VENDOR breach notification process; and
    b. Own the ACME response process.

4. Payment Card Industry Data Security Standard (PCI DSS): If VENDOR's solution processes, stores or transmits ACME customers' cardholder data, VENDOR falls within scope of ACME's PCI DSS compliance and therefore must:

a. Maintain documented compliance with the most current version of the PCI DSS;
b. Conduct quarterly network scans by an Approved Scanning Vendor (ASV); and
c. Obtain a Report of Compliance (ROC) from an annual on-site PCI Data Security Assessment with a Qualified Security Assessor (QSA).
    i. VENDOR may provide an annual Self-Assessment Questionnaire (SAQ) in lieu of an annual ROC that is issued by a QSA.

HUMAN RESOURCES SECURITY

1. Requirements for Employment: VENDOR must maintain contractual agreements with employees, contractors, consultants and/or other third-party staff that formally documents their responsibilities for cybersecurity.

2. Roles and Responsibilities: VENDOR must define and document security roles and responsibilities of employees, contractors and third party users to incorporate ACME's data protection control requirements, to the extent permitted by applicable law:
    a. All employees, contractors, and third-party users must be notified of the consequences for not following your security policy in handling ACME data.
    b. All assets used to manage or store ACME data must be protected against unauthorized access, disclosure, modification, destruction or interference.
    c. All employees, contractors and third party users must be provided with education and training in privacy and security procedures and the correct information processing requirements.
    d. All personnel with access to sensitive Personally Identifiable Information (sPII) must complete a privacy training class and be knowledgeable of any specific privacy requirements for the data being handled. Refresher training is required at least on an annual basis.

3. Assigned Ownership: VENDOR must assign ownership of critical and sensitive information, business applications, computer systems and networks to individuals (e.g., business managers) and document the responsibilities of these assigned owners.
    a. Responsibilities for protecting critical and sensitive information, business applications, computer systems and networks must be communicated to and accepted by owners.

4. Personnel Screening: VENDOR must ensure a secure workforce. Background verification checks on all VENDOR's candidates for employment should be carried out in accordance with relevant laws, regulations, and ethics and should be proportional to the business requirements and the classification of the information that may be accessed.

5. Staff Agreements: VENDOR must establish agreements with VENDOR's employees and/or VENDOR's employee representative that specify cybersecurity responsibilities. This agreement must be incorporated into the contracts of VENDOR's employees, contractors, consultants and/or other third party staff and be taken into account when screening applicants for employment.

ACCESS CONTROL (AC)

VENDOR is expected to implement logical access controls to limit access to systems and processes to authorized users.

LOGICAL ACCESS CONTROL

1. Access Control: VENDOR must restrict access to the application and associated information to authorized individuals. This must be enforced accordingly to ensure that only authorized individuals to gain access to business applications, systems, networks and computing devices, that individual accountability is assured and to provide authorized users with access privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

2. User Authorization: VENDOR must ensure that all users have authorization before they are granted access privileges.
    a. User access privileges must be reviewed at least every six (6) months; and
    b. Access must be revoked within forty-eight (48) hours of a user's change in role or employment status.

System & Communications Protection (SC)

VENDOR is expected to employ industry-recognized leading practice principles that promote effective IT security within systems and the network.

Communications & Operations Management

1. Communications Security: VENDOR must support standards and procedures that ensure confidentiality, integrity, and availability of information and services with continuous oversight on new threats and vulnerabilities by a documented risk assessment process driving risk mitigation implementation on a timely basis.

2. Operations Management: VENDOR must maintain sufficient overall operational control and visibility into all security aspects of how data is processed, stored and transmitted:
    a. System administrators must have adequate training and experience to securely administer the infrastructure within their responsibility;
    b. Vendor must have a separation of duties process to prevent one individual from controlling all key aspects of a critical transaction or business process; and
    c. Vendors are responsible for data protection, privacy compliance, and security control validation/ certification of their sub-contractors.

Cryptography

1. Cryptography: VENDOR's cryptographic solutions must:
    a. Meet or exceed ACME's minimum encryption requirement of 128-bit AES; and
    b. Protect the confidentiality of sensitive information that is subject to legal and regulatory-related encryption requirements.

2. Cryptographic Key Management: VENDOR must manage cryptographic keys, in accordance with industry-recognized leading practices for key management:
    a. Documented standards and procedures must exist; and
    b. Cryptographic keys must be protected against unauthorized access or destruction to ensure that these keys are not compromised (e.g., through loss, corruption or disclosure).

Network Security

1. Defense In Depth (DiD): VENDOR must secure its computer networks using multiple layers of access controls to protect against unauthorized access. In particular, VENDOR shall:
    a. Group network servers, applications, data, and users into security domains;
    b. Establish appropriate access requirements within and between each security domain; and
    c. Implement appropriate technological controls to meet those access requirements consistently, including (for example) firewalls.

2. Network Controls: VENDOR must ensure that all data and communications networks are secured to ensure the transmission of data is kept confidential.
    a. Applications, ports, services, and similar access points installed on a computer or network facility, which are not specifically required for business functionality, must be disabled or removed;
    b. Network segments connected to the Internet must be protected by a firewall which is configured to secure all devices behind it;
    c. Network segments where ACME data resides should be isolated from non-ACME data, logically or physically unless approved by ACME Security;
    d. User connection capability must be documented with regard to messaging, electronic mail, file transfer, interactive access, and application access;
    e. All production servers must be located in a secure, access controlled location;
    f. Firewalls must be configured properly to address all reasonably-known security concerns;
    g. Infrastructure diagrams, documentation, and configurations must be up to date, controlled and available to assist in issue resolution; and
    h. Systems must have the ability to detect a potential hostile attack. (e.g., IDS/IPS)
        i. All systems must be updated to the current release and actively monitored.

3. Wireless Access: Wireless access must be authorized, authenticated, encrypted and permitted only from approved locations.