Your Logo
Will Be
Placed Here

NIST 800-53 v4
INFORMATION SECURITY ASSESSMENT TEMPLATE

ACME Consulting Services, Inc.

Table of Contents

TECHNOLOGY AUDIT OVERVIEW

PURPOSE

The purpose of this audit is to review the ACME's due care and due diligence documentation and procedures, in an effort to identify areas of technology management that do not meet industry-recognized best practices and develop a plan to correct those deficiencies. This template is based on the NIST 800-53 revision 4 control set.

SCOPE

The scope of this audit is intended to cover all business-supported technologies at all geographic locations, including outsourcing arrangements.

AUDIT CONTROLS

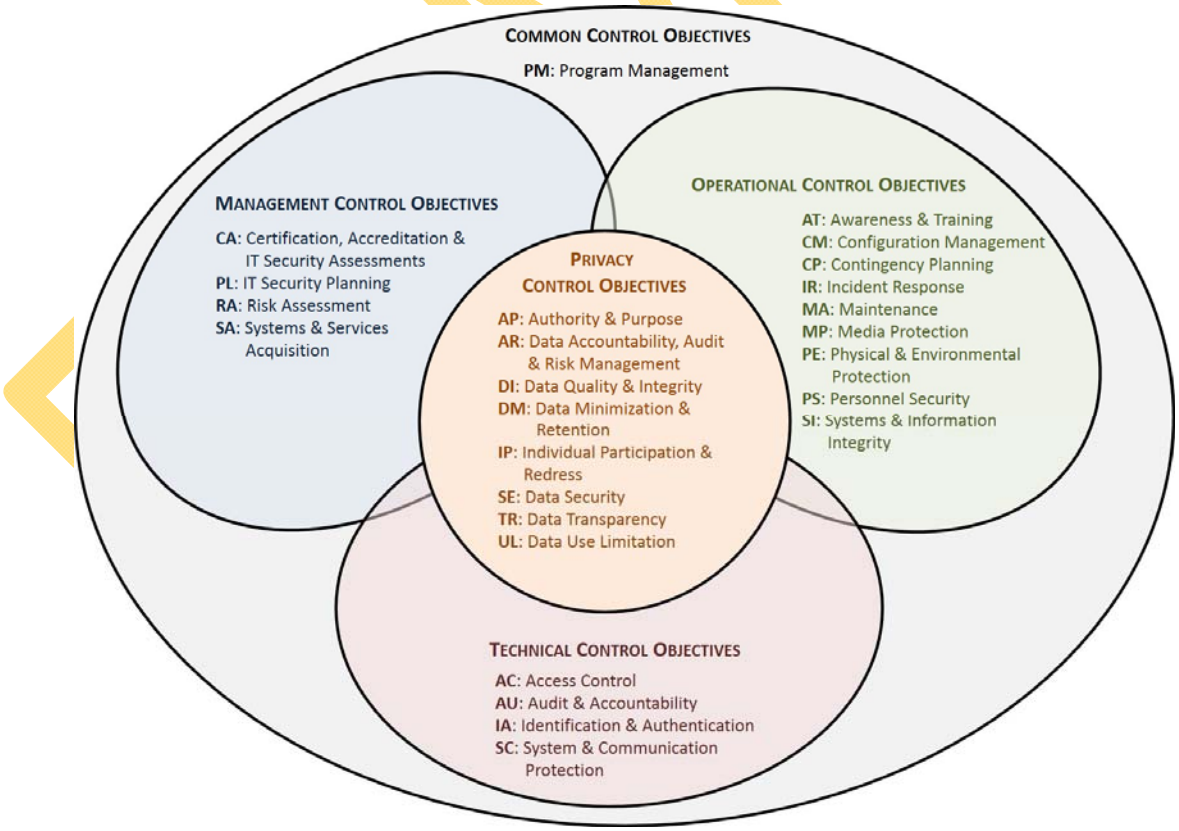
There are five (5) general classes of security control objectives and these classes are further broken down into twenty-six (26) families of security control objective.

- **Common**
  - Common control objectives address information security program-level security topics.
  - These common control objectives establish the overall framework for management, operational and technical controls.
- **Management**
  - Management control objectives address techniques and concerns that are normally addressed by management in ACME's information security program.
  - In general, Management control objectives focus on the management of the information security program and the management of risk within ACME.
- **Operational**
  - Operational control objectives address techniques and concerns that are generally implemented and executed by people, as opposed to systems, that are put in place to improve the security of a particular system or group of systems.
  - Operational control objectives often require technical or specialized expertise; often relying upon management activities as well as technical controls.
- **Technical**
  - Technical control objectives address processes and concerns that a computer system executes.
  - Technical control objectives are dependent upon the proper functioning of the system for their effectiveness and therefore require significant operational considerations.
- **Privacy**
  - Privacy control objectives address Personally Identifiable Information (PII).
  - Privacy control objectives are dependent upon the proper functioning of the other classes of controls for their effectiveness and therefore require significant operational considerations.

Each family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each control family. The table below summarizes the classes and families in the security control catalog and the associated family identifiers.

Class	Family	Identifier
Common	Security Program Management	PM
Management	Certification, Accreditation & Security Assessments	CA
Management	Planning	PL
Management	Risk Assessment	RA
Management	System & Services Acquisition	SA
Operational	Awareness & Training	AT
Operational	Configuration Management	CM
Operational	Contingency Planning	CP
Operational	Incident Response	IR
Operational	Maintenance	MA
Operational	Media Protection	MP
Operational	Personnel Security	PS
Operational	Physical & Environmental Protection	PE
Operational	System & Information Integrity	SI
Technical	Access Control	AC
Technical	Audit & Accountability	AU
Technical	Identification & Authentication	IA
Technical	System & Communications Protection	SC
Privacy	Authority & Purpose	AP
Privacy	Data Accountability, Audit & Risk Management	AR
Privacy	Data Quality & Integrity	DI
Privacy	Data Minimization & Retention	DM
Privacy	Individual Participation & Redress	IP
Privacy	Data Security	SE
Privacy	Data Transparency	TR
Privacy	Data Use Limitation	UL

NIST SP 800-53 Control Objectives Families & Classes



NIST SP 800-53 Control Objectives Families & Classes

COMMON CONTROLS

PROGRAM MANAGEMENT (PM)

PM-01: Information Security Program Plan
Control Requirement: The organization:

- Develops and disseminates an organization-wide Information Security program plan that:
  - Provides an overview of the requirements for the Information Security program and a description of the PM controls in place, or planned, for meeting those requirements;
  - Provides sufficient information about the PM controls to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;
  - Includes roles, responsibilities, management commitment, and compliance;
  - Is approved by a senior management with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;
- Reviews the Information Security program for applicability; and
- Revises the Information Security program to address organizational changes and problems identified during program implementation or security assessments.

Helpful hints for filling out this section: The objective of this control is that the organization maintains a documented and executed Information Security program.

Findings: (provide details below)
Is this control met? **YES** ☐ **NO** ☐ **N/A** ☐ **UNKNOWN** ☐

Details:

PM-02: Assigned Information Security Responsibilities
Control Requirement: The organization appoints an individual assigned with the mission and resources to coordinate, develop, implement, and maintain an organization-wide Information Security program.
Helpful hints for filling out this section: The objective of this control is that the organization formally assigns Information Security responsibilities.

Findings: (provide details below)
Is this control met? **YES** ☐ **NO** ☐ **N/A** ☐ **UNKNOWN** ☐

Details:
Who is the individual?

PM-03: Information Security Resources
Control Requirement: The organization addresses all capital planning and investment requests, include the resources needed to implement the Information Security program, and documents all exceptions to this requirement.
Helpful hints for filling out this section: The objective of this control is that the organization properly supports its Information Security program.

Findings: (provide details below)
Is this control met? **YES** ☐ **NO** ☐ **N/A** ☐ **UNKNOWN** ☐

Details:

PL-02: System Security Plan (SSP)

Control Requirement: The organization develops a functional architecture for identifying and maintaining key architectural information on each critical information system that, at a minimum, includes:

- External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface;
- User roles and the access privileges assigned to each role;
- Unique security requirements;
- Types of information processed, stored, or transmitted by the information system and any specific protection needs in accordance with applicable local, state and Federal laws; and
- Restoration priority of information or information system services.

Helpful hints for filling out this section: The objective of this control is that the organization develops a security plan for information systems that describe both the security requirements for the information system and the security controls that are planned or in place for meeting those security requirements.

Findings: (provide details below)

Is this control met?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN** ☐

Details:

How are systems documented? This includes from projects down to individual systems.

PL-03: System Security Plan (SSP) Update

Control Requirement: The organization updates the architecture for information systems.

Helpful hints for filling out this section: The objective of this control is that the organization reviews the security plan in accordance with the organization-defined frequency (e.g. annually), and updates the plan as a result of system or organizational changes or problems identified during plan implementation or as a result of security assessments.

Findings: (provide details below)

Is this control met?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN** ☐
Once a system goes into production, is it ever reviewed again for its documentation & configuration?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN** ☐

Details:

PL-04: Rules of Behavior

Control Requirement: The organization:

- Develops usage policies for critical technologies (for example, remote access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies; and
- Develops acceptable use policies, as well as what is prohibited behavior.

Helpful hints for filling out this section: The objective of this control is that the organization establishes user responsibilities and expected behavior regarding their use of the information system and the information contained therein, and authorizes a user access to the information system only after receiving signed acknowledgement by that user of his/her acceptance of the rules of behavior.

Findings: (provide details below)

Is this control met?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN** ☐
Are users required to sign off that they understand and will abide by the rules of behavior?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN** ☐
Are there roles & responsibilities assigned to job functions?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN** ☐

Do the rules of behavior cover all the types of technology in use by the company?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN** ☐
Are there restrictions on the use of social networking sites or posting company-related information on website without authorization?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN** ☐

Details:

PL-05: Privacy Impact Assessment (PIA)

Control Requirement: The organization conducts a privacy impact assessment on the information system to evaluate privacy in information systems.

Helpful hints for filling out this section: The objective of this control is that the organization conducts a privacy impact assessment on information system.

Findings: (provide details below)

Is this control met? **YES** ☐ **NO** ☐ **N/A** ☐ **UNKNOWN** ☐

Details:

What privacy concerns does the company have?

PL-06: Security-Related Activity Planning

Control Requirement: The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (e.g., mission, functions, image, and reputation), organizational assets, and individuals.

Helpful hints for filling out this section: The objective of this control is that the organization conducts planning and coordination of security-related activities that could affect the information system (e.g., system hardware/software maintenance, contingency or incident response plan exercises) before conducting the exercise to reduce the impact on organizational operations.

Findings: (provide details below)

Is this control met? **YES** ☐ **NO** ☐ **N/A** ☐ **UNKNOWN** ☐

Details:

PL-07: Security Concept Of Operations

Control Objective: The organization:

- Develops a security Concept of Operations (CONOPS) for information systems containing at a minimum, how the organization intends to operate the systems from the perspective of information security; and
- Reviews and updates the CONOPS at least annually.

Helpful hints for filling out this section: The objective of this control is that there is an operational plan for how information security is handled within the organization.

Findings: (provide details below)

Is this control met? **YES** ☐ **NO** ☐ **N/A** ☐ **UNKNOWN** ☐

Details:

MP-02: Media Access

Control Requirement: The organization restricts access to types of digital and non-digital media authorized individuals using organization-defined security measures.

Helpful hints for filling out this section: The objective of this control is that the organization restricts access to information system media, and not whether the media is allowed to be used, which is covered under AC-19. This control addresses both digital and non-digital media.

Findings: (provide details below)

Is this control met?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN**	☐

Details:
Who has access to installation media?
Who has access to backup media?
How is the media stored?

MP-03: Media Marking

Control Requirement: The organization marks media in accordance with organizational policies and procedures, indicating the distribution limitations, handling caveats, and applicable security markings required, if any.

Helpful hints for filling out this section: The objective of this control is that the organization clearly identifies media security classifications. MP-3 and AC-15 are both concerned with external information applied to media; while AC-16 is concerned with internal information inserted into the data.

Findings: (provide details below)

Is this control met?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN**	☐
Is there a standardized media marking format?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN**	☐
Are limitations published on media handing?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN**	☐

Details:
How are media labeled? (e.g. sensitive, public, confidential, etc.)

MP-04: Media Storage

Control Requirement: The organization:

- Physically controls and securely stores digital and non-digital media within controlled areas using organization-defined security measures;
- Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Helpful hints for filling out this section: The objective of this control is that the organization protects external media storage, particularly portable media, and safekeeping this media in controlled areas. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient. Removable media includes diskettes, magnetic tapes, external/removable hard drives, USB drives, flash drives, compact disks, digital video disks, and non-digital media (e.g., paper, microfilm). This control also includes portable and mobile computing and communications devices with information storage capability (laptop/notebook computers, personal digital assistants, cell phones), and telephone systems that have the capability to store information on internal media (voice mail).

Findings: (provide details below)

Is this control met?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN**	☐
Is the media encrypted?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN**	☐

Details:
What method of encryption is used?
Where are the encryption keys stored and who has access to them?

MP-05: Media Transportation

Control Requirement: The organization:

- Protects and controls digital and non-digital media during transport outside of controlled areas using organization-defined security measures;
- Maintains accountability for information system media during transport outside of controlled areas; and
- Restricts the activities associated with transport of such media to authorized personnel.

Helpful hints for filling out this section: The objective of this control is that the organization takes steps to protect digital (e.g. tape backups) and non-digital (e.g. paper records) during transportation. This also includes how users transport laptops and other media as they travel for business.

Findings: (provide details below)

Is this control met?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN**	☐
Is the transport of media documented?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN**	☐
Is media being transported encrypted?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN**	☐
Are users required to lock laptops in the trunk of their vehicles if the vehicle is left unattended?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN**	☐

Details:
What precautions are currently in place for transporting media?
What procedures must employees follow about traveling with laptops or other company-owned electronics?

MP-06: Media Sanitization

Control Requirement: The organization:

- Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and
- Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

Helpful hints for filling out this section: The objective of this control is that the organization takes steps to effectively destroy all forms of media when it is no longer necessary to be maintained.

Findings: (provide details below)

Is this control met?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN**	☐
Is this media destroyed by shredding or incinerating?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN**	☐
Is the media destruction outsourced?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN**	☐
Is media destruction documented?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN**	☐

Details:
What company does the outsourced destruction?
Does that contract have liability and non-disclosure provisions?
Where is media kept before it is picked up for destruction?

MP-07: Media & Asset Use

Control Objective: The organization restricts the use of organization-defined types of digital and/or non-digital media on information systems or system components using security safeguards.

Helpful hints for filling out this section: The objective of this control is that restrictions are in place for what is acceptable, such as users being able to use USB drives to store/transfer data.

Findings: (provide details below)

Is this control met?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN**	☐

Details:

TECHNICAL CONTROLS

ACCESS CONTROL (AC)

AC-01: Access Control Policy & Procedures

Control Requirement: The organization develops, disseminates, and reviews/updates:

- A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Helpful hints for filling out this section: The policies and procedures may be issued at an organizational level for all systems within the organization as a common control or uniquely developed and issued as supplemental or stand-alone control procedures for specific systems. The expectation for this control action is that the organization has determined the appropriate elements with the approval of senior management official. An effective capability would not be possible if the policy and procedures were not disseminated to the appropriate elements.

Findings: (provide details below)

Is this control met? **YES** ☐ **NO** ☐ **N/A** ☐ **UNKNOWN** ☐

Details:

AC-02: Account Management

Control Requirement: The organization manages information system accounts, including:

- Identifying account types (e.g., individual, group, system, application, guest/anonymous, and temporary);
- Establishing conditions for group membership;
- Identifying authorized users of the information system and specifying access privileges;
- Requiring appropriate approvals for requests to establish accounts;
- Establishing, activating, modifying, disabling, and removing accounts;
- Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
- Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;
- Deactivating:
  - Temporary accounts that are no longer required; and
  - Accounts of terminated or transferred users;
- Granting access to the system based on:
  - A valid access authorization;
  - Intended system usage; and
  - Other attributes as required by the organization or associated missions/business functions; and
- Reviewing accounts on a regular basis.

Helpful hints for filling out this section: The objective of this control is that the organization has a formal process for handling its user, computer and service accounts.

Findings: (provide details below)

Is this control met? **YES** ☐ **NO** ☐ **N/A** ☐ **UNKNOWN** ☐

Details:

How are temporary & emergency accounts disabled or terminated?

How are inactive accounts disabled or terminated?

How are privileged user accounts managed?

AC-03: Access Enforcement

Control Requirement: The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.

Helpful hints for filling out this section: The objective of this control is that the organization has mechanisms with the capability to enforce access restrictions that are configured in compliance with the intended user authorizations.

Findings: (provide details below)

Is this control met? **YES** ☐ **NO** ☐ **N/A** ☐ **UNKNOWN** ☐

Details:

Describe how Role Based Access Control (RBAC) is implemented?

AC-04: Information Flow Enforcement – Access Control Lists (ACLs)

Control Requirement: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Helpful hints for filling out this section: The objective of this control is that the organization manages the flow of information through Access Control Lists (ACLs).

Findings: (provide details below)

Is this control met? **YES** ☐ **NO** ☐ **N/A** ☐ **UNKNOWN** ☐

Details:

How often are ACLs reviewed?

Content checking for encrypted data?

How are embedded data types handled?

How is metadata handled?

AC-05: Separation of Duties

Control Requirement: The organization:

- Separates duties of individuals as necessary, to prevent malevolent activity without collusion;
- Documents separation of duties; and
- Implements separation of duties through assigned information system access authorizations.

Helpful hints for filling out this section: The objective of this control is that the organization enforces a separation of duties to aide in the prevention of both fraud and errors from a lack of quality control. The person requesting a change should not be the person who plans and then implements the change.

Findings: (provide details below)

Is this control met? **YES** ☐ **NO** ☐ **N/A** ☐ **UNKNOWN** ☐

Details:

AC-06: Least Privilege

Control Requirement: The organization employs the concept of least privilege, allowing only authorized accesses for users and processes which are necessary to accomplish assigned tasks in accordance with organizational business functions.

Helpful hints for filling out this section: The objective of this control is that the organization implements least privilege by limiting the rights/privileges or accesses assigned to users to enable performance of specified tasks while adequately mitigating risk to the organization, individuals, and other organizations.

Findings: (provide details below)

Is this control met?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN** ☐

Details:

AC-07: Unsuccessful Login Attempts

Control Requirement: The information system:

- Enforces a limit for consecutive invalid login attempts by a user during an organization-defined time period;
- Automatically locks the account until released by an administrator when the maximum number of unsuccessful attempts is exceeded; and
- The control applies regardless of whether the login occurs via a local or network connection.

Helpful hints for filling out this section: The objective of this control is that the organization defines the maximum number of consecutive invalid user login attempts, a time-period in which the consecutive invalid access attempts occur, and a defined response to be taken should this maximum number of invalid login attempts occur during the defined time-period.

Findings: (provide details below)

Is this control met?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN** ☐
Are mobile devices configured to perform a remote purge after a set number of failed logon attempts?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN** ☐

Details:
How many logon attempts does it take to lock out an account?
Who must reset the account after it is locked out?

AC-08: System Use Notification

Control Requirement: The information system:

- Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices; and
- Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system.

Helpful hints for filling out this section: The objective of this control is that the organization enforces "logon banners" that users must acknowledge before they are allowed to use the system.

Findings: (provide details below)

Is this control met?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN** ☐
Are logon banners standardized across the company?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN** ☐
Are logon banners configured on all firewalls, routers, switches, and other applicable networking gear?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN** ☐
Are logon banners configured on all workstations?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN** ☐
Are logon banners configured on all servers?	**YES**	☐	**NO**	☐	**N/A**	☐	**UNKNOWN** ☐

Details: