**Contents**

[1. Introduction 3](#_Toc112330269)

[2. Scope 3](#_Toc112330270)

[3. Project Baselines 3](#_Toc112330271)

[4. Baseline configuration discussion 4](#_Toc112330272)

[5. Configuration Test Approach 5](#_Toc112330273)

[5.1 Testing Stages: 5](#_Toc112330274)

[5.2 Testing Types 6](#_Toc112330275)

[5.3 Configuration Testing: 7](#_Toc112330276)

[6. Equipment manufacturer recommendations 8](#_Toc112330277)

[7. Centralized authentication service 9](#_Toc112330278)

[7.1 Lightweight directory access protocol 9](#_Toc112330279)

[7.2 Centralized log collection 9](#_Toc112330280)

**DOCUMENT REVISION CONTROL**

REVISION HISTORY

| **Date** | **Author** | **Version** | **Change Reference** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

REVIEWERS

| **Name** | **Position** | **Date** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

DISTRIBUTION

| **Date** | **Distributed to** | **Version** | **Distribution Format** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Introduction

This document captures and controls the hardware, network, software, documentation, and people associated with or employed by an IT service. In other words, it is a snapshot of the key elements that make up an IT service at a given point in time.

# Scope

All **<Company Name>** systems, applications, and services that are owned, leased, managed, or used by ACME, its representatives, subcontractors, or any business partners on behalf of **<Company Name>** are subject to these security configurations. The recommendations for a secure baseline configuration that comes "out of the box" may not necessarily be suitable for ACME's particular business needs, as acknowledged by ACME. Given this fact, it is essential for the cybersecurity personnel at ACME to publish "ACME-approved" secure baseline configurations and to document permitted departures from generally accepted security procedures.

# Project Baselines

**Configuration Baseline types**

**System baseline**

**Subsystem baseline**

**Development baseline**

**Product Baseline**

**Operational Baseline**

* System baseline- This baseline could be regarded as the system's whole set of functional needs. The requirements published as part of a system purchase solicitation are frequently this baseline. Additionally, as is common in many acquisitions, these requirements may be slightly altered as a result of requirements research and negotiation after a contractor is hired.
* Subsystem baseline- This is an intermediate baseline that comes between functional and development baseline once the requirements are completed and mapping of high-level functions to system components has been established by preliminary design work.
* Development baseline- It is important to have a carefully designed baseline before beginning system development. System development can be significantly hindered by changes in design caused by various reasons such as new functionality, changes in technology, and roadblocks in development. Controlling these changes to design is necessary to maintain a cohesive system.
* Product baseline- The product baseline is important because it documents the design of the completed system. The product baseline results from the series of changes that have been made to the original developmental baseline during the system development process. If the developmental baseline is subject to configuration control, the product baseline will be the product of the developmental baseline undergoing the various system acceptance and verification tests, as directed by the configuration control board.
* Operational baseline- Transportation management systems are genuinely "active" systems because of the ongoing pressure for change. To put it another way, the product baseline will evolve over time to accommodate the required adjustments. Maintaining the operational baseline during system operations is crucial to reflect modifications that have been accepted through the configuration management process and put into effect.

# Baseline configuration discussion

Baselining the Configuration Activities and Considerations

* Determine what data needs to be recorded and which users require access to system component information.
* Determine the way the information will be presented.
* Decide how frequently the component information has to be updated.
* Specify how the data will be utilized.

| **Data** | **Mode of presentation** | **Frequency** | **Utilization measures** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Configuration Test Approach

Testing will be carried out in various stages with different types.

## 5.1 Testing Stages:

Unit Testing:

|  |  |
| --- | --- |
| Test Objective: |  |
| Technique: |  |
| Completion Criteria: |  |
| Special Considerations: |  |

Integrated Testing:

|  |  |
| --- | --- |
| Test Objective: |  |
| Technique: |  |
| Completion Criteria: |  |
| Special Considerations: |  |

System Testing:

|  |  |
| --- | --- |
| Test Objective: |  |
| Technique: |  |
| Completion Criteria: |  |
| Special Considerations: |  |

Acceptance Testing:

|  |  |
| --- | --- |
| Test Objective: |  |
| Technique: |  |
| Completion Criteria: |  |
| Special Considerations: |  |

## 5.2 Testing Types

GUI Testing

|  |  |
| --- | --- |
| **Test Objective:** |  |
| **Technique:** |  |
| **Completion Criteria:** |  |
| **Special Considerations:** |  |

Functional Testing

|  |  |
| --- | --- |
| Test Objective: |  |
| Technique: |  |
| Completion Criteria: |  |
| Special Considerations: |  |

Performance Profiling:

|  |  |
| --- | --- |
| Test Objective: |  |
| Technique: |  |
| Completion Criteria: |  |
| Special Considerations: |  |

Load Testing:

|  |  |
| --- | --- |
| Test Objective: |  |
| Technique: |  |
| Completion Criteria: |  |
| Special Considerations: |  |

Configuration Testing:

|  |  |
| --- | --- |
| Test Objective: |  |
| Technique: |  |
| Completion Criteria: |  |
| Special Considerations: |  |

Installation Testing:

|  |  |
| --- | --- |
| Test Objective: |  |
| Technique: |  |
| Completion Criteria: |  |
| Special Considerations: |  |

Browser Testing:

|  |  |
| --- | --- |
| Test Objective: |  |
| Technique: |  |
| Completion Criteria: |  |
| Special Considerations: |  |

# Equipment manufacturer recommendations

OEMs of hardware or software frequently offer configuration suggestions to safeguard their goods or services because security functionality is rarely enabled by default in default settings.

Asset custodians are expected to study OEM security recommendations for new goods or services and evaluate the risk involved with implementing or not implementing OEM recommended configurations.

Asset custodians are expected to visit the OEM's website for legacy products or services, seek for OEM security recommendations, and evaluate the risk associated with following or not following OEM suggested configurations.

| **Meets industry practices** | **Greater than industry-recognized practices** |
| --- | --- |
| Identify and access management | Multi-factor authentication |
| Encryption | Encryption at rest |
| Host Intrusion Prevention System | Host Intrusion Prevention System |

# Centralized authentication service

A centralized authentication service is a system that allows you to log in to multiple applications with a single set of credentials. This can be extremely helpful if you have a lot of different passwords to remember, or if you want to make sure that your passwords are more secure. There are a few different centralized authentication services to choose from, but they all work in basically the same way. Once you’ve set up an account with a centralized authentication service, you can link it to all the applications that you use. When you log in to the centralized authentication service, you’ll be able to access all the applications that you’ve linked to it.

## 7.1 Lightweight directory access protocol

An open, vendor-neutral, industry-standard application protocol called the Lightweight Directory Access Protocol is used to access and maintain distributed directory information services over an IP network.

| **LDAP servers** | **Username** | **Security** | **LDAP ports** |
| --- | --- | --- | --- |
| (Insert hostname and IP address) | (Insert the name of the LDAP server account) | Use LDAP wherever possible | (Insert port number) |
|  |  |  |  |
|  |  |  |  |

## Centralized log collection

| **Name** | **Log collectors** | **Port** |
| --- | --- | --- |
| (Insert hostname of SIEM server) | (Insert hostname and IP address of primary log collector) | 514/UDP |
|  |  |  |
|  |  |  |