SECURE BASELINE CONFIGURATIONS (SBC)

ACME Business Consulting, LLC
# Table of Contents

## Executive Summary

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intended Audience</td>
<td>6</td>
</tr>
<tr>
<td>Scope &amp; Applicability</td>
<td>6</td>
</tr>
</tbody>
</table>

## Determining Secure Baselines & Approved Deviations

### Defining Industry-Recognized Practices

- Center for Internet Security (CIS) Benchmarks
- Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)
- Original Equipment Manufacturer (OEM) Recommendations
- Open Web Application Security Project (OWASP)

### Defining Reasonable Expectations for Secure Baseline Configurations

- Data Sensitivity Considerations
- Safety & Criticality Considerations

### Assurance Levels

- Basic Assurance Requirements
- Enhanced Assurance Requirements

### Determining Mandatory and Discretionary Technology Controls

- Technology Controls By Assurance Level
- Zone-Based Approach To Discretionary Controls

## Shared Configuration Settings

### Centralized Authentication Services

- Active Directory (AD)
- Lightweight Directory Access Protocol (LDAP)
- Radius - Authentication, Authorization & Accounting (AAA)

### Centralized Log Collection

- Security Incident Event Manager (SIEM)

### Networking Services

- Network Time Protocol (NTP)
- Domain Naming Service (DNS)
- Corporate Wireless Network
- Guest Wireless Network

### Email Settings

- SMTP Authenticated Submission
- SMTP Relay

## Server-Class Systems

### Microsoft Server Operating Systems

- Active Directory
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

### Linux Server Operating Systems

- Red Hat 7
- Red Hat 6

### Unix Server Operating Systems

- Solaris 11
- ZOS

### Other Server Operating Systems

- IBM AIX 7.1
- IBM AIX 6.1

## Workstation-Class Systems

### Microsoft Workstations Operating Systems

- Windows 10
- Windows 8.1
Windows 8
Windows 7

Apple Workstation Operating Systems
Mac OS X

Linux Workstation Operating Systems
CentOS 7
Debian 8
SUSE Enterprise 12
Ubuntu 18

Network Devices

Firewalls
Cisco
Palo Alto
F5

Routers
Cisco
Juniper

Wireless Access Controllers (WACs) & Wireless Access Points (WAPs)
Cisco Wireless LAN Control (WLC)

Multi-Function Devices (MFDs) & Printers
[Insert Printer Manufacturer Name]

Voice & Video over Internet Protocol (VVOIP)
[Insert VVOIP Manufacturer Name]

Mobile Devices

Apple iOS Devices
iOS 12

Google Android Devices
Android

Windows Phone Devices
Windows 10 Mobile

Databases

Microsoft
Microsoft SQL Server 2016
Microsoft SQL Server 2014

MySQL
MySQL 5.7

Oracle
Oracle Database 12

PostgreSQL
PostgreSQL 9

IBM
DB2 10

MongoDB
MongoDB 3.4

Major Applications

Microsoft Active Directory
Active Directory

Microsoft Exchange
Exchange Server 2016

Microsoft SharePoint
SharePoint 2016

Microsoft Internet Information Services (IIS)
IIS 10
IIS 8.36

Domain Naming Service (DNS)
BIND 9

Apache Tomcat

Windows 21
Windows 7 21

Apple Workstation Operating Systems 21
Mac OS X 21

Linux Workstation Operating Systems 22
CentOS 7 22
Debian 8 22
SUSE Enterprise 12 22
Ubuntu 18 23

Network Devices 24

Firewalls 24
Cisco 24
Palo Alto 25
F5 25

Routers 25
Cisco 25
Juniper 26

Wireless Access Controllers (WACs) & Wireless Access Points (WAPs) 26
Cisco Wireless LAN Control (WLC) 26

Multi-Function Devices (MFDs) & Printers 26
[Insert Printer Manufacturer Name] 26

Voice & Video over Internet Protocol (VVOIP) 27
[Insert VVOIP Manufacturer Name] 27

Mobile Devices 28

Apple iOS Devices 28
iOS 12 28

Google Android Devices 28
Android 29

Windows Phone Devices 29
Windows 10 Mobile 29

Databases 30

Microsoft 30
Microsoft SQL Server 2016 30
Microsoft SQL Server 2014 30

MySQL 31
MySQL 5.7 31

Oracle 31
Oracle Database 12 31

PostgreSQL 32
PostgreSQL 9 32

IBM 32
DB2 10 32

MongoDB 32
MongoDB 3.4 32

Major Applications 34

Microsoft Active Directory 34
Active Directory 34

Microsoft Exchange 35
Exchange Server 2016 35

Microsoft SharePoint 35
SharePoint 2016 35

Microsoft Internet Information Services (IIS) 35
IIS 10 35
IIS 8.36 35

Domain Naming Service (DNS) 36
BIND 9 36

Apache Tomcat 37
APACHE TOMCAT 7
APACHE HTTP SERVER
    APACHE 2.4
    APACHE 2.2
VMWARE
    vSPHERE
    ESXi 5
    NSX 38
CENTRALIZED LOG MANAGEMENT
    SPLUNK
INTRUSION DETECTION / PREVENTION SYSTEMS (IDS / IPS)
    [INSERT IDS / IPS MANUFACTURER NAME]

MINOR APPLICATIONS
MIXCROSOFT OFFICE
    MICROSOFT OFFICE 2016
    ONEDRIVE FOR BUSINESS
MICROSOFT INTERNET EXPLORER (IE)
    IE 11 BROWSER
GOOGLE CHROME
    CHROME BROWSER
MOZILLA FIREFOX
    FIREFOX BROWSER
APPLE SAFARI
    SAFARI BROWSER
ADOBE
    ACROBAT READER
AJAX
JAVA
    JAVA
.NET
    .NET
WORDPRESS
    WORDPRESS

CLOUD-BASED APPLICATIONS
MICROSOFT
    OFFICE 365
MICROSOFT AZURE
    AZURE
AMAZON WEB SERVICES (AWS)
    AWS
GOOGLE CLOUD COMPUTING PLATFORM
    GOOGLE CLOUD
DOCKER
    DOCKER
KUBERNETES
    KUBERNETES

EMBEDDED TECHNOLOGY
MICROSOFT WINDOWS-BASED DEVICES
HEATING, VENTILATIONS & AIR CONDITIONING (HVAC)
PHYSICAL ACCESS CONTROL
VIDEO SURVEILLANCE
BURGLAR / FIRE ALARM SYSTEMS

APPENDICES
APPENDIX A: DATA CLASSIFICATION
APPENDIX B: SAFETY & CRITICALITY (SC) RATINGS
**EXECUTIVE SUMMARY**

ACME’s asset owners and asset custodians are responsible for implementing and maintaining secure systems, applications and services that are utilize industry-recognized practices and in compliance with applicable statutory, regulatory and contractual obligations.

**PURPOSE**

This document exists to serve as a reference so secure configurations can be implemented consistently across the company. This focus on secure configurations reduces technology-related risk to ACME. As the graphic below depicts, everything revolves around risk where (1) bad actors wish to harm ACME assets and (2) ACME wants to protect its assets. This is where the implementation of cybersecurity and privacy controls comes into play, since that is what reduces risk.

![Diagram](image)

*Figure 1: Focus of risk management for Secure Baseline Configurations*

**INTENDED AUDIENCE**

This Secure Baseline Configurations (SBC) document contains technical guidance that is specifically focused on the following functions internal to ACME or outsourced to a trusted service provider:

- Solutions architects (e.g., IT and cybersecurity architects)
- Systems integrators
- Asset owners
- Asset custodians (e.g., system admins)

**SCOPE & APPLICABILITY**

These secure configurations apply to all ACME systems, applications and services that are owned, leased, controlled or used by ACME, its agents, contractors or other business partners on behalf of ACME.
ACME recognizes that “out of the box” secure baseline configuration recommendations will not always be applicable to meet ACME’s business requirements. Given that reality, it is a necessity for ACME cybersecurity staff to document acceptable deviations from industry-recognized security practices and publish “ACME-approved” secure baseline configurations.

It is the responsibility of asset owners and asset custodians to submit a request for exception for any deviations from a ACME-approved secure baseline configuration. This request must include an assessment of risk posed from the deviation.

**DEFINING INDUSTRY-RECOGNIZED PRACTICES**

ACME’s approved sources for defining appropriate configurations to secure systems, applications and services are:

- Center for Internet Security (CIS) Benchmarks
- Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)
- Original Equipment Manufacturer (OEM) Recommendations
- Open Web Application Security Project (OWASP)

**CENTER FOR INTERNET SECURITY (CIS) BENCHMARKS**

CIS provides free versions of the CIS Benchmarks in PDF format. It is possible to purchase pre-hardened images for certain operating systems for participating cloud environments.

*Note - To stay current on the latest updates to STIGs, asset custodians are encouraged to subscribe to the CIS Workbench newsletter.*

**DEFENSE INFORMATION SYSTEMS AGENCY (DISA) SECURITY TECHNICAL IMPLEMENTATION GUIDES (STIGS)**

DISA provides free hardening guidance, in the form of STIGs. To view a STIG, it is necessary to download the STIG Viewer from DISA’s Information Assurance Support Environment (IASE) website, which is a Java-based application.

*Note - To stay current on the latest updates to STIGs, asset custodians are encouraged to subscribe to the STIG mailing list.*

**ORIGINAL EQUIPMENT MANUFACTURER (OEM) RECOMMENDATIONS**

It is common practice for hardware or software OEMs to provide configuration recommendations to secure their products or services, since default settings rarely come with security functionality enabled by default. Most OEM security recommendations match up with CIS Benchmarks and DISA STIGs (see above), but analysis is required for settings where other security recommendations either conflict with OEM recommendations or if no other guidance exists:

- For new products or services, asset custodians are expected to review OEM security recommendations and assess the risk associated with making or not making OEM recommended configurations.
- For legacy products or services, asset custodians are expected to visit the OEM’s website and search for OEM security recommendations and assess the risk associated with making or not making OEM recommended configurations.

---

1. CIS Benchmarks - [https://www.cisecurity.org/cis-benchmarks/](https://www.cisecurity.org/cis-benchmarks/)
2. DISA Information Assurance Support Environment (IASE) - [https://iase.disa.mil/stigs/Pages/index.aspx](https://iase.disa.mil/stigs/Pages/index.aspx)
3. OWASP - [https://www.owasp.org](https://www.owasp.org)
4. CIS Hardened Images - [https://www.cisecurity.org/hardened-images/](https://www.cisecurity.org/hardened-images/)
5. CIS Workbench - [https://workbench.cisecurity.org/](https://workbench.cisecurity.org/)
<table>
<thead>
<tr>
<th>Assurance Level</th>
<th>BASIC</th>
<th>ENHANCED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level of Effort</td>
<td>Meets industry-recognized secure practices</td>
<td>Greater than basic industry-recognized secure practices</td>
</tr>
</tbody>
</table>
| MANDATORY Technology Controls | • Antimalware (host-based)  
• Encryption in transit (e.g., SSL/TLS, SFTP, SSH, etc.)  
• Log collection (forwarded to centralized log collector)  
• Patch management  
• Vulnerability scanning  
• Identity & Access Management (IAM) | • Antimalware (host-based)  
• Configuration management (automated)  
• Encryption at rest (e.g., file, folder, table or whole drive)  
• Encryption in transit (e.g., SSL/TLS, SFTP, SSH, etc.)  
• File Integrity Monitoring (FIM)  
• Host Intrusion Prevention System (HIPS)  
• Log collection (forwarded to SIEM)  
• Mobile Device Management (MDM)  
• Multi-Factor Authentication (MFA)  
• Network Intrusion Detection / Protection (NIDS / NIPS)  
• Next Generation Firewall (NGF)  
• Patch management |
| DISCRETIONARY Technology Controls | • Configuration management (automated)  
• Encryption at rest (e.g., file, folder, table or whole drive)  
• Host Intrusion Prevention System (HIPS)  
• Mobile Device Management (MDM)  
• Multi-Factor Authentication (MFA)  
• Network Intrusion Detection / Protection (NIDS / NIPS)  
• Next Generation Firewall (NGF)  
• Privileged Identity & Account Management (PIAM)  
• Security Incident Event Manager (SIEM) | • Database encryption  
• Database Access Management (DAM)  
• Data Loss Prevention (DLP)  
• Dynamic / Static Application Security Testing (DAST / SAST)  
• Network Access Control (NAC)  
• Penetration test  
• Privileged Identity & Account Management (PIAM)  
• Session recording  
• Web Application Firewall (WAF) |

*Figure 3: Mandatory vs Discretionary technology control expectations*
ZONE-BASED APPROACH TO DISCRETIONARY CONTROLS

An additional way to help determine the applicability of Discretionary controls is through a zone-based approach to evaluating if Discretionary controls would be prudent, based on possible risks that are unique to the networking environment.

<table>
<thead>
<tr>
<th>Zone</th>
<th>Definition of Cybersecurity Risk Zones</th>
<th>Risk Considerations</th>
</tr>
</thead>
</table>
| 1    | Systems that are exposed to the Internet:  
- Assets in an external-facing Demilitarized Zone (DMZs)  
- Servers with a direct connection to the Internet | Discretionary controls are reasonably-expected, due to the direct Internet exposure. |
| 2    | Network segments that are dedicated to workstations and end-user equipment:  
- Internal workstations & mobile / remote users  
- End-user equipment (e.g., desktop printers, scanners, etc.) | Mandatory controls are expected in this desktop / laptop / mobile device environment. |
| 3    | Network segments that are dedicated to internal servers and infrastructure equipment:  
- Servers  
- Networking equipment (e.g. networked printers, switches, internal servers) | A mixture of Mandatory and Discretionary controls are expected in this environment, since it is the internal server and network infrastructure environment. |
| 4    | Internal DMZs are segmented for statutory, regulatory or special business requirements:  
- PCI DSS cardholder data environment  
- HVAC / facility control systems  
- Test / development / staging environments | A mixture of Mandatory and Discretionary controls are expected in this environment, since some segments will require Enhanced controls (e.g., in scope for PCI DSS or NIST 800-171) while others should have Basic controls (e.g., Test, Dev and Stage). |
| 5    | Encompasses all Bring Your Own Devices (BYOD) categories of equipment:  
- User-owned laptops  
- User-owned smart phones | Based on the "hands off" approach to BYOD, there is generally little-to-no ability to install endpoint controls, so Discretionary controls should be used at the network-level to control BYOD risks. |

Figure 4: Zone-based risk zones
SHARED CONFIGURATION SETTINGS

The following organization-wide configuration settings are intended to be used on all applicable ACME assets, unless an approved deviation from these settings is authorized.

CENTRALIZED AUTHENTICATION SERVICES

ACTIVE DIRECTORY (AD)
- Domain Controller(s) (DC)
  - [insert hostname & IP address of primary DC server(s)]
  - [insert hostname & IP address of backup DC server(s)]
- Domain Name: [insert domain name]

LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)
- LDAP servers:
  - [insert hostname & IP address of primary LDAP server]
  - [insert hostname & IP address of backup LDAP server]
- Distinguished username: [insert distinguished name of the LDAP server account]
- Security: Use LDAP over TLS (LDAP-S), where possible
- LDAP Ports:
  - LDAP: 389/TCP & 389/UDP
  - LDAP-S: 636/TCP

RADIUS - AUTHENTICATION, AUTHORIZATION & ACCOUNTING (AAA)
- RADIUS servers:
  - [insert hostname & IP address of primary RADIUS server]
  - [insert hostname & IP address of backup RADIUS server]
- Radius Ports:
  - Authentication Ports: 1812/UDP & 1645/UDP
  - Accounting Ports: 1813/UDP & 1645/UDP
- Timeout: 5 seconds
- Retry Count: 3

CENTRALIZED LOG COLLECTION

SECURITY INCIDENT EVENT MANAGER (SIEM)
- Name: [insert hostname of SIEM server]
- Log collectors:
  - [insert hostname & IP address of primary log collector]
  - [insert hostname & IP address of backup log collector]
- Port: 514/UDP

NETWORKING SERVICES

NETWORK TIME PROTOCOL (NTP)
- External NTP Servers
  - Primary: tick.usnogps.navy.mil [204.34.198.40]
  - Alternate: tock.usnogps.navy.mil [204.34.198.41]
- Internal NTP Servers
  - [insert hostname & IP address of primary NTP server]
**Server-Class Systems**

Server-class systems include, but are not limited to:

- Microsoft Server
- Linux
- Unix

Server-class considerations for assigning Basic vs Enhanced controls are covered in the following chart to establish expectations for technology-based controls to protect servers:

<table>
<thead>
<tr>
<th>Assurance Level</th>
<th>BASIC</th>
<th>ENHANCED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level of Effort</td>
<td>Meets industry-recognized secure practices</td>
<td>Greater than basic industry-recognized secure practices</td>
</tr>
</tbody>
</table>
| **MANDATORY** Technology Controls for Servers | • Antimalware (host-based)  
• Encryption in transit (e.g., SSL/TLS, SFTP, SSH, etc.)  
• Log collection (forwarded to centralized log collector)  
• Patch management  
• Identity & Access Management (IAM) | • Antimalware (host-based)  
• Configuration management (automated)  
• Encryption at rest (e.g., file, folder, table or whole drive)  
• Encryption in transit (e.g., SSL/TLS, SFTP, SSH, etc.)  
• File Integrity Monitoring (FIM)  
• Host Intrusion Prevention System (HIPS)  
• Log collection (forwarded to SIEM)  
• Multi-Factor Authentication (MFA)  
• Patch management |
| **DISCRETIONARY** Technology Controls for Servers | • Configuration management (automated)  
• Encryption at rest (e.g., file, folder, table or whole drive)  
• Host Intrusion Prevention System (HIPS)  
• Multi-Factor Authentication (MFA)  
• Privileged Identity & Account Management (PIAM)  
• Security Incident Event Manager (SIEM) | • Data Loss Prevention (DLP)  
• Privileged Identity & Account Management (PIAM) |

*Figure 6: Mandatory vs Discretionary technology control expectations for server operating systems*

**Microsoft Server Operating Systems**

**Active Directory**

**Secure Baseline Configuration**

For this technology, the following secure baseline configuration is considered the ACME-approved standard to use:

[choose one (or more) and delete others that are not applicable]

- DISA STIG – Active Directory Forest STIG v2.8
- DISA STIG – Active Directory Domain STIG v2.11

**Approved Deviations**

- [list any requirements not met and the justification for the deviation]

**Discretionary Controls**

- [list any Discretionary controls that are required to be deployed with this OS build]

---

11 DISA STIG - [https://iase.disa.mil/stigs/Pages/a-z.aspx](https://iase.disa.mil/stigs/Pages/a-z.aspx)
12 DISA STIG - [https://iase.disa.mil/stigs/Pages/a-z.aspx](https://iase.disa.mil/stigs/Pages/a-z.aspx)