Your Logo
Will Be
Placed Here

SECURE BASELINE CONFIGURATIONS (SBC)

ACME Business Consulting, Inc.

SBC
Secure Baseline Configurations

Table of Contents

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.

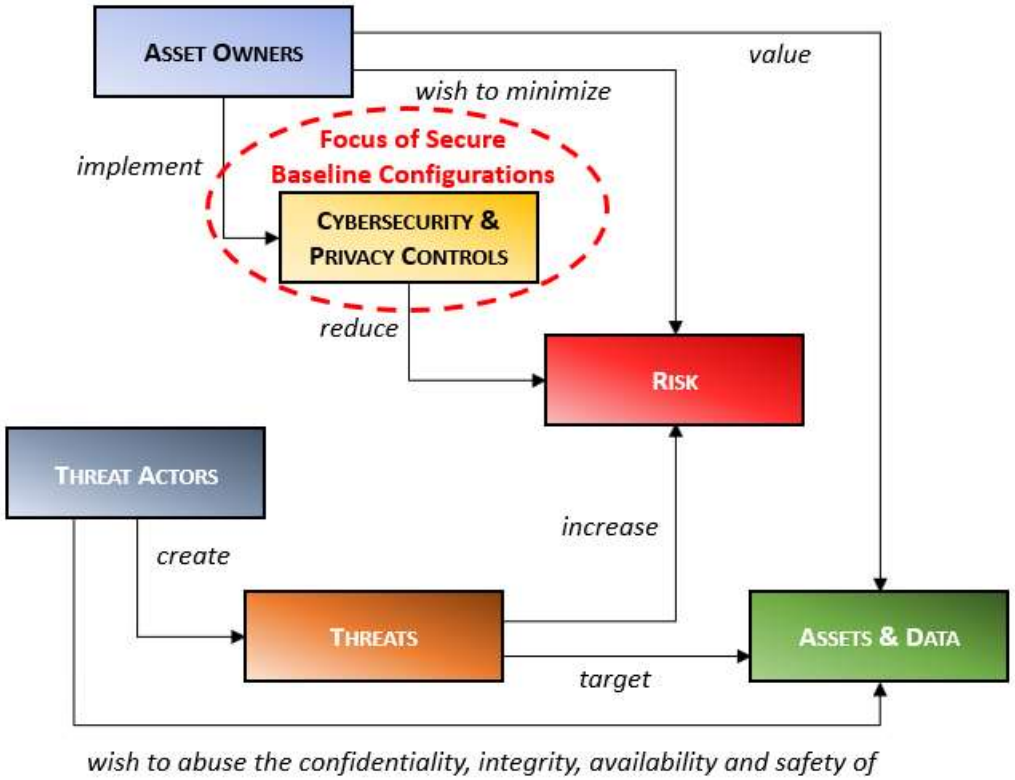

Figure 1: Focus of risk management for Secure Baseline Configurations

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[1]
- Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)[2]
- Original Equipment Manufacturer (OEM) Recommendations
- Open Web Application Security Project (OWASP)[3]

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.[4]

Note - To stay current on the latest updates to STIGs, asset custodians are encouraged to subscribe to the CIS Workbench newsletter.[5]

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.[6]

Note - To stay current on the latest updates to STIGs, asset custodians are encouraged to subscribe to the STIG mailing list.[7]

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/
[2] DISA Information Assurance Support Environment (IASE) - https://iase.disa.mil/stigs/Pages/index.aspx
[3] OWASP - https://www.owasp.org
[4] CIS Hardened Images - https://www.cisecurity.org/hardened-images/
[5] CIS Workbench - https://workbench.cisecurity.org/
[6] STIG Viewer - https://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx
[7] STIG mailing list - https://public.govdelivery.com/accounts/USDISA/subscriber/new?topic id=USDISA 181

Assurance Levels

Where the Data Sensitivity intersects with Safety & Criticality is considered the Assurance Levels (AL). The AL represents the "level of effort" that is needed to properly ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of the asset or process. Each system needs to be categorized by AL:

- Basic; or
- Enhanced

Basic Assurance Requirements

Basic establishes the minimum level of control that would be "reasonably-expected" and is defined as industry-recognized secure practices (e.g., PCI DSS, NIST 800-53, ISO 27002, etc.).

Enhanced Assurance Requirements

Enhanced establishes a more secure level of control that exceed minimum requirements and is defined as exceeding industry-recognized secure practices (e.g., DLP, FIM, DAM, etc.). These requirements are often "situationally required" per a statutory, regulatory or contractual obligation that is specific to a type of data or under a specific circumstance (e.g., personal data, cardholder data, electronic health protected information, etc.

Asset Categorization Matrix		Data Sensitivity			
		RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Safety & Criticality	SC-1 Mission Critical	*Enhanced*	*Enhanced*	*Enhanced*	*Enhanced*
	SC-2 Business Critical	*Enhanced*	*Enhanced*	*Basic*	*Basic*
	SC-3 Non-Critical	*Enhanced*	*Basic*	*Basic*	*Basic*

Figure 2: Asset categorization risk matrix

Determining Mandatory and Discretionary Technology Controls

What sets the Basic and Enhanced requirements apart comes down to the technology controls in place, where Enhanced will have more protection in place than Basic. The expectation is that Basic contains "reasonably-expected protections" that would withstand scrutiny by an outside auditor or regulator, based on following industry-recognized practices to design, build and maintain secure systems, applications and services. In terms of "basic security," this consists of having antimalware protections, protecting sensitive data, maintain systems and reviewing security logs (see the chart below for more details).

When it is necessary to increase security requirements, additional controls are needed. These Discretionary controls go above and beyond Mandatory controls to meet specific data protection needs that would withstand scrutiny by an outside auditor or regulator (see the chart below for specific examples of enhanced controls). The assignment of Enhanced controls is often required to meet a statutory, regulatory or contractual obligation (e.g., PCI DSS, EU GDPR, NIST 800-171, etc.).

Technology Controls By Assurance Level

There will be cases where the Assurance Level may require a set of controls, but cybersecurity, privacy, technology or business teams feel additional controls are needed to address a specific risk. This is where discretionary controls come into play. Discretionary controls are at the discretion of stakeholders to implement that go above and beyond Mandatory controls.

Enhanced controls are "situationally required" and must be selected and implemented based on applicable statutory, regulatory or contractual requirements. These requirements may only apply in specific circumstances, so consult with a Governance, Risk or Compliance (GRC) analyst for specific implementation requirements. In the absence of any such requirements, ACME may treat these controls or enhancements as discretionary technology controls.

The diagram below provides a high-level distinction between cybersecurity-related technology controls that are categorized as Basic or Enhanced. The specifics of technology controls are determined by the technology platform, since certain technologies are not possible to be installed on all technology platforms. The chart below is intended to provide reasonable guidance for expectations to keep systems, applications and services secure.

Assurance Level	BASIC	ENHANCED
Level of Effort	Meets industry-recognized secure practices	Greater than basic industry-recognized secure practices
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

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:

Assurance Level	BASIC	ENHANCED
Level of Effort	**Meets industry-recognized secure practices**	**Greater than basic industry-recognized secure practices**
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[11]
- DISA STIG – Active Directory Domain STIG v2.11[12]
- OEM – Microsoft – Best Practices for Securing Active Directory[13]

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
[12] DISA STIG - https://iase.disa.mil/stigs/Pages/a-z.aspx
[13] Microsoft – Best Practices for Securing Active Directory - https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

Windows Server 2019

Secure Baseline Configuration

For this OS, the following secure baseline configuration is considered the ACME-approved standard to use:
[choose one (or more) and delete others that are not applicable]

- OEM – Microsoft – Security baseline (DRAFT) for Windows 10 v1809 and Windows Server 2019[14]

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]

Windows Server 2016

Secure Baseline Configuration

For this OS, the following secure baseline configuration is considered the ACME-approved standard to use:
[choose one (or more) and delete others that are not applicable]

- CIS Benchmark - Microsoft Windows Server 2016 RTM Release 1607 Benchmark v1.0.0[15]
- DISA STIG – Microsoft Windows Server 2016 STIG Benchmark v1.7[16]
- OEM – Microsoft – Windows Server 2016 Security Guide[17]

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]

Windows Server 2012 R2

Secure Baseline Configuration

For this OS, the following secure baseline configuration is considered the ACME-approved standard to use:
[choose one (or more) and delete others that are not applicable]

- CIS Benchmark - Microsoft Windows Server 2012 R2 Benchmark v2.3.0[18]
- DISA STIG – Microsoft Windows Server 2012 and 2012 R2 DC STIG Benchmark v2.13[19] (domain controller)
- DISA STIG – Microsoft Windows Server 2012 and 2012 R2 MS STIG Benchmark v2.13[20] (member server)

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]

Windows Server 2012

Secure Baseline Configuration

For this OS, the following secure baseline configuration is considered the ACME-approved standard to use:
[choose one (or more) and delete others that are not applicable]

- CIS Benchmark - Microsoft Windows Server 2012 non-R2 Benchmark v2.1.0[21]

---

[14] Microsoft Windows Server 2019 - https://blogs.technet.microsoft.com/secguide/2018/10/01/security-baseline-draft-for-windows-10-v1809-and-windows-server-2019/
[15] CIS Benchmark - https://www.cisecurity.org/cis-benchmarks/
[16] DISA STIG - https://iase.disa.mil/stigs/Pages/a-z.aspx
[17] Microsoft Windows Server 2016 Security Guide - https://cloudblogs.microsoft.com/windowsserver/2017/08/22/now-available-windows-server-2016-security-guide/
[18] CIS Benchmark - https://www.cisecurity.org/cis-benchmarks/
[19] DISA STIG - https://iase.disa.mil/stigs/Pages/a-z.aspx
[20] DISA STIG - https://iase.disa.mil/stigs/Pages/a-z.aspx
[21] CIS Benchmark - https://www.cisecurity.org/cis-benchmarks/

MAJOR APPLICATIONS

Major Application-class applications include, but are not limited to:

- Active Directory
- Exchange
- Enterprise Resource Management (ERM)
- SAP
- DNS

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

Assurance Level	BASIC	ENHANCED
Level of Effort	Meets industry-recognized secure practices	Greater than basic industry-recognized secure practices
MANDATORY Technology Controls for Major Applications	▪ Encryption in transit (e.g., SSL/TLS, SFTP, SSH, etc.) ▪ Log collection (forwarded to centralized log collector) ▪ Patch management ▪ Identity & Access Management (IAM)	▪ Encryption at rest (e.g., file, folder, table or whole drive) ▪ Encryption in transit (e.g., SSL/TLS, SFTP, SSH, etc.) ▪ Log collection (forwarded to **SIEM**) ▪ Multi-Factor Authentication (**MFA**) ▪ Network Intrusion Detection / Protection (**NIDS** / **NIPS**)
DISCRETIONARY Technology Controls for Major Applications	▪ Encryption at rest (e.g., file, folder, table or whole drive) ▪ Multi-Factor Authentication (**MFA**) ▪ Network Intrusion Detection / Protection (**NIDS** / **NIPS**) ▪ Next Generation Firewall (**NGF**) ▪ Privileged Identity & Account Management (**PIAM**) ▪ Security Incident Event Manager (**SIEM**)	▪ Data Loss Prevention (**DLP**) ▪ Dynamic / Static Application Security Testing (**DAST** / **SAST**) ▪ Privileged Identity & Account Management (**PIAM**) ▪ Security Incident Event Manager (**SIEM**) ▪ Web Application Firewall (**WAF**)

Figure 11: Mandatory vs Discretionary technology control expectations for major applications

MICROSOFT ACTIVE DIRECTORY

ACTIVE DIRECTORY

SECURE BASELINE CONFIGURATION

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

- DISA STIG – Active Directory Forest STIG v2.8[107]
- DISA STIG – Active Directory Domain STIG v2.11[108]
- DISA STIG – Group Policy Objects (GPOs) - July 2018[109]
- OEM – Microsoft – Best Practices for Securing Active Directory[110]

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]

[107] DISA STIG - https://iase.disa.mil/stigs/Pages/a-z.aspx
[108] DISA STIG - https://iase.disa.mil/stigs/Pages/a-z.aspx
[109] DISA STIG - https://iase.disa.mil/stigs/Pages/a-z.aspx
[110] Microsoft – Best Practices for Securing Active Directory - https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

Microsoft Exchange

Exchange Sever 2016

Secure Baseline Configuration

For this application, the following secure baseline configuration is considered the ACME-approved standard to use: [choose one (or more) and delete others that are not applicable]

- CIS Benchmark - Microsoft Exchange Server 2016 Benchmark v1.0.0[111]
- DISA STIG – Microsoft Exchange 2016 Mailbox Server STIG v1[112]
- DISA STIG – Microsoft Exchange 2016 Edge Transport Server STIG v1[113]
- OEM – Vendor – x[114]

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]

Microsoft SharePoint

SharePoint 2016

Secure Baseline Configuration

For this application, the following secure baseline configuration is considered the ACME-approved standard to use: [choose one (or more) and delete others that are not applicable]

- CIS Benchmark - x[115]
- DISA STIG – x[116]
- OEM – Vendor – x[117]

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]

Microsoft Internet Information Services (IIS)

IIS 10

Secure Baseline Configuration

For this application, the following secure baseline configuration is considered the ACME-approved standard to use: [choose one (or more) and delete others that are not applicable]

[111] CIS Benchmark - https://www.cisecurity.org/cis-benchmarks/
[112] DISA STIG - https://iase.disa.mil/stigs/Pages/a-z.aspx
[113] DISA STIG - https://iase.disa.mil/stigs/Pages/a-z.aspx
[114] Microsoft Windows Server 2019 - https://blogs.technet.microsoft.com/secguide/2018/10/01/security-baseline-draft-for-windows-10-v1809-and-windows-server-2019/
[115] CIS Benchmark - https://www.cisecurity.org/cis-benchmarks/
[116] DISA STIG - https://iase.disa.mil/stigs/Pages/a-z.aspx
[117] Microsoft Windows Server 2019 - https://blogs.technet.microsoft.com/secguide/2018/10/01/security-baseline-draft-for-windows-10-v1809-and-windows-server-2019/