



## Right-Sizing NIST IT Assessments: Better Scoping, Focused Effort

### 2025 Cybersecurity Virtual Symposium



# Meet Your Presenters



**Ben Sady**

Principal



**Mareena Bowen**

Manager



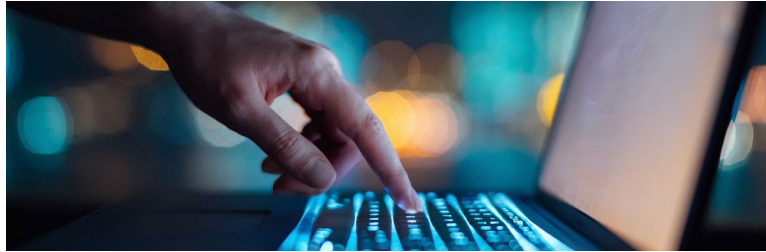
# Purpose & Learning Objectives

Discover how to make NIST IT assessments smarter, faster, and more focused. This session will show you how to use a risk-based approach to streamline NIST assessment scope, reduce audit fatigue, and zero in on what really matters, without sacrificing compliance

## Learning Objectives



Understand how to apply a risk-based methodology to scope NIST-based IT assessments, beginning with data and system inventories and CIA impact assessments.



Learn how to identify and justify the exclusion of non-risk-aligned controls or non-system-specific controls from audit scope without compromising compliance or security.



Learn practical strategies for aligning assessment scope with system risk profiles and improving collaboration between auditors and internal technology teams.



# Overview of Common NIST Assessments



## NIST 800-53

**Purpose**

Baseline framework for security controls for federal information systems and organizations.

**Scope**

20 control families

**Total Requirements / Controls**

1,000+ controls (including enhancements)



## NIST CSF

**Purpose**

Risk-based framework for managing cybersecurity risk.

**Scope**

6 core functions (Govern, Identify, Protect, Detect, Respond, Recover), 23 categories

**Total Requirements / Controls**

100+ controls



## NIST 800-171

**Purpose**

Safeguards for CUI in non-federal systems (e.g., defense contractors).

**Scope**

17 control families

**Total Requirements / Controls**

100+ controls



## NIST 800-161

**Purpose**

Guidance for managing cybersecurity risks in the supply chain.

**Scope**

20 control families

**Total Requirements / Controls**

150+ controls

**NIST 800-37 Risk Management Framework:** overarching risk management process and framework



# Adoption of NIST 800-53 Frameworks



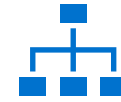
## NIST 800-53

The primary standard for federal information system security controls, but its influence extends far beyond federal agencies.



## Many U.S. States

Adopted NIST 800-53 as the foundation for their own cybersecurity standards for agencies, service providers, and critical infrastructure.



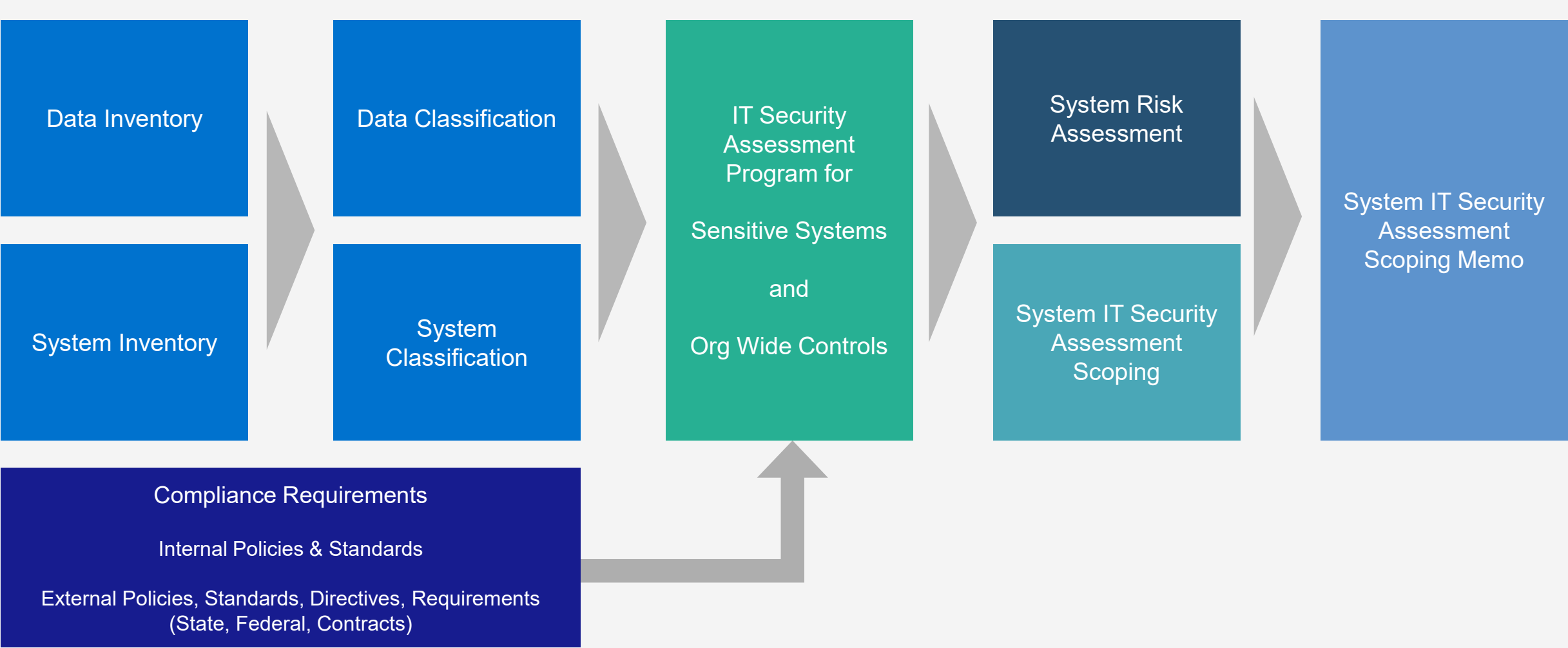
## Customization

States often tailor the baseline controls to fit state-specific laws, risk profiles, and operational needs.



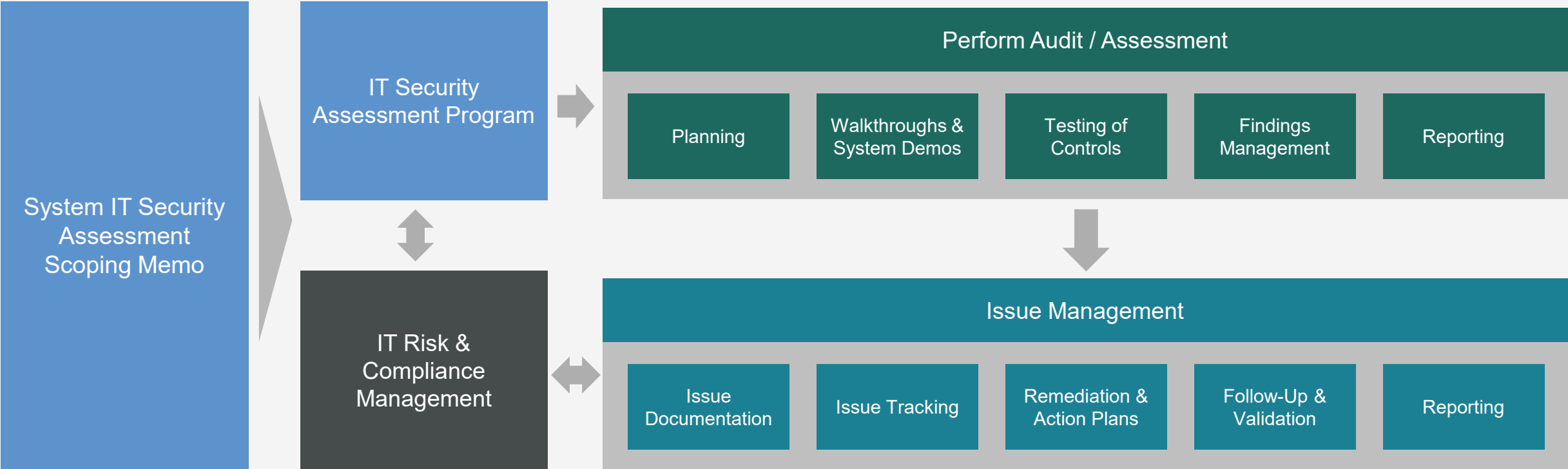


# The Big Picture – How This Fits





# The Big Picture – How This Fits (continued)



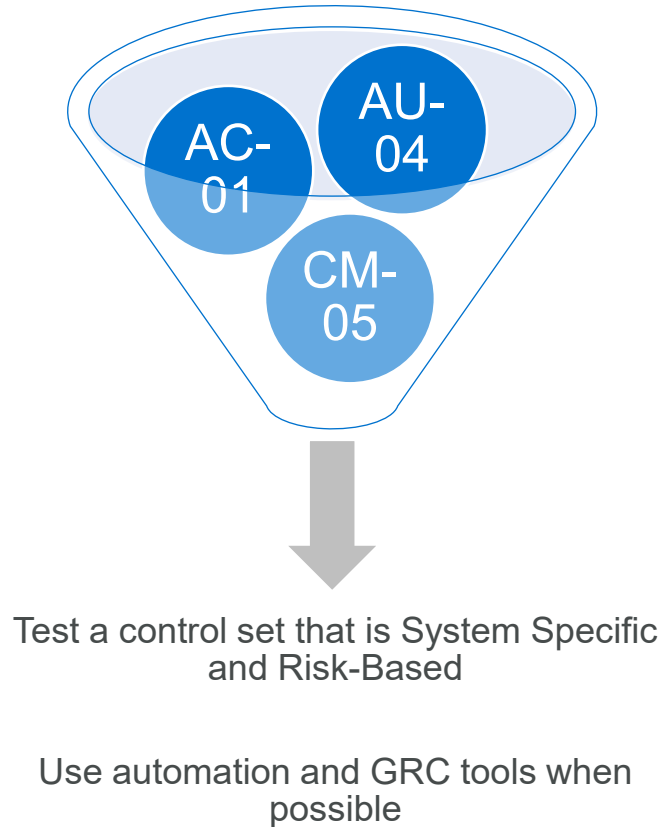


# Challenges With NIST Assessments

## Challenges

1. Too many controls
2. Takes too long
3. Workforce constraints
4. Funding constraints
5. Spend same amount of time on low-risk controls as the high-risk controls
6. Not tailored to each individual system's business function and risk
7. Not producing enough value or focusing on the right risks
8. Reduces time available to spend on other IT risk and compliance needs

## Total Controls




## Desired Outcomes


1. Right-sized control set
2. Improved audit and time management
3. Less strain on workforce
4. Funding is better utilized
5. Focus energy on high-risk controls
6. Tailored to each individual system's business function and risk
7. Produce better value and risk management
8. Free up time to spend on other IT risk and compliance needs




# Right-Sizing

## What Does “Right-Sizing” Mean?


- 


Tailoring the scope and depth of NIST assessments to match the actual risk and business function of each system.
- 


Focuses effort where it matters most: on high-risk areas and critical controls.
- 


Avoids “one-size-fits-all” audits that waste time and resources on out of scope and low-risk controls.

## What Does Success Look Like?

- 

**Improved Value**  
Assessments deliver actionable insights and meaningful risk reduction.
- 

**Greater Focus**  
Audit teams concentrate on the most important controls and threats.
- 

**Efficiency**  
Less audit fatigue, better use of resources, and faster completion.
- 

**Compliance Maintained**  
No sacrifice in meeting regulatory or contractual requirements.



Is a Risk-Based Approach Allowed?

An abstract background featuring a dense field of thin, curved lines in shades of purple, teal, and blue, creating a sense of depth and movement. Scattered throughout are small, out-of-focus light spots (bokeh) in similar colors.

YES!



# NIST Citations

## NIST 800-37 (citations)

### **Section 2.2 (Risk Management Framework Steps and Structure):**

“Flexibility of implementation can also be applied to control selection, control tailoring to meet organizational security and privacy needs.”

“The implementation of control tailoring helps to ensure that security and privacy solutions are customized for the specific missions, business functions, risks, and operating environments of the organization.”

## NIST CSF (citations)

### **Preface:**

“The CSF describes desired outcomes that are intended to be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise. Because these outcomes are sector-, country-, and technology-neutral, they provide an organization with the flexibility needed to address their unique risks, technologies, and mission considerations.”

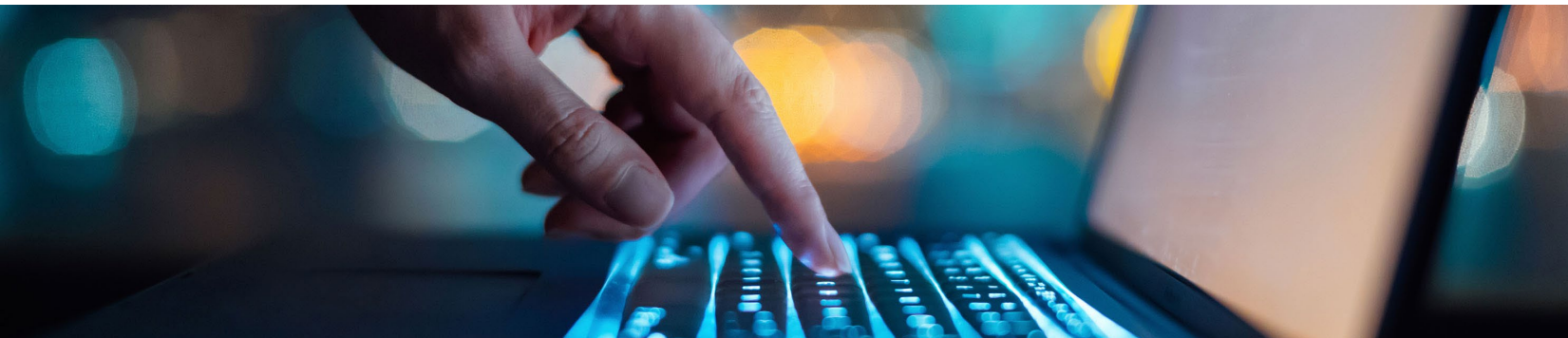
## NIST 800-53 (citations)

### **Section 1.1 (Purpose and Applicability):**

“The control selection criteria can be guided and informed by many factors, including mission and business needs, stakeholder protection needs, threats, vulnerabilities, and requirements to comply with federal laws, executive orders, directives, regulations, policies, standards, and guidelines.”

### **Section 2.4 (Security and Privacy Controls):**

“The selection and implementation of security and privacy controls reflect the objectives of information security and privacy programs and how those programs manage their respective risks.”





# NIST Citations (Continued)

## NIST 800-171 (citations)

### **Section 2.2 (Security Requirement Development Methodology):**

“Organization-defined parameters (ODPs) are included in certain security requirements. ODPs provide flexibility through the use of assignment and selection operations to allow federal agencies and nonfederal organizations to specify values for the designated parameters in the requirements. Assignment and selection operations provide the capability to customize the security requirements based on specific protection needs. The determination of ODP values can be guided and informed by laws, Executive Orders, directives, regulations, policies, standards, guidance, or mission and business needs.”

### **Section 3 (The Security Requirements):**

“Some systems, including specialized systems (e.g., industrial/process control systems, medical devices, computer numerical control machines), may have limitations on the application of certain security requirements.”

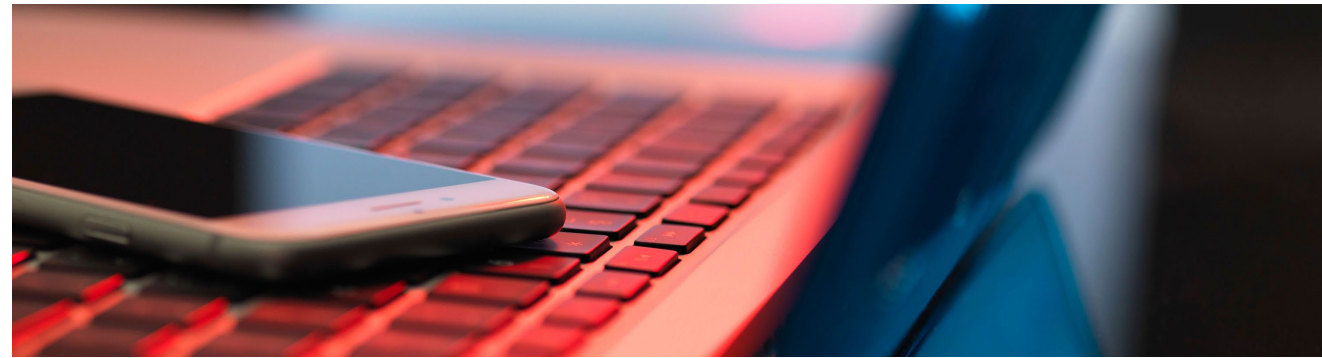
## NIST 800-161 (citations)

### **Section 1.1 (Purpose and Applicability):**

“The control selection criteria can be guided and informed by many factors, including mission and business needs, stakeholder protection needs, threats, vulnerabilities, and requirements to comply with federal laws, executive orders, directives, regulations, policies, standards, and guidelines.”

### **Section 2.4 (Security and Privacy Controls):**

“The selection and implementation of security and privacy controls reflect the objectives of information security and privacy programs and how those programs manage their respective risks.”



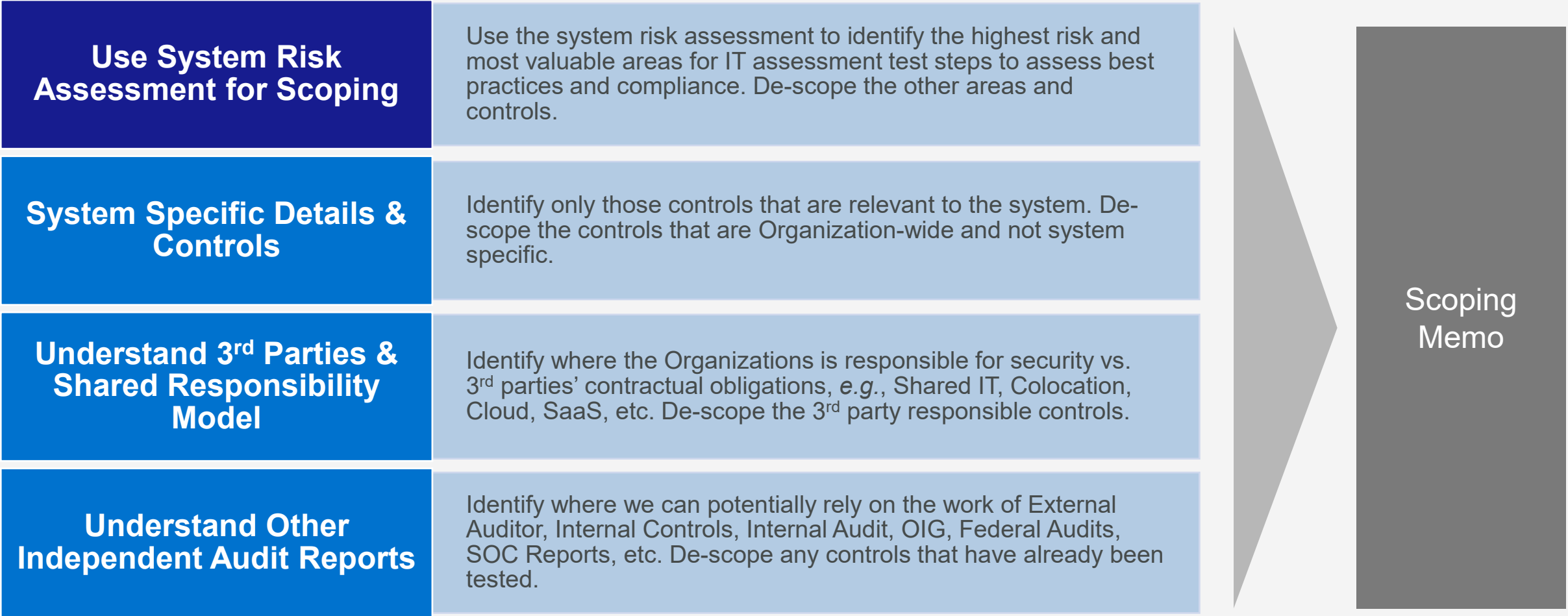


# How to Right-Size Control Scoping





# How to Right-Size Control Scoping (continued)





# Example Scoping Memo

**System Name:** XYZ System

## SCOPING DETAILS

**System Purpose:** Managed inventory of XYZ cases. Users (internal and external) can log in and make updates.

**Implementation Date:** XXXX

**Planned Retirement Date:** XXXX

**System Technical Details:** Web-based system. Custom developed by 3<sup>rd</sup> party. Hosted by XX. Microsoft SQL Server DB.

**System Risk Assessment Summary:** Confidential data should be secured from tampering at DB and by application access rights. Concerns with user access management. Concerns with audit logging. System availability has not been 100% due to aging custom developed code. No external Federal regulations were found to be applicable. Would like to make sure system security plan has been updated recently. Concerned with failover and recoverability controls if custom code issues arise.

**Third Party Responsibilities:** XX is responsible for hosting servers, patching servers, and physical security of servers. 3<sup>rd</sup> party development company is responsible for making custom code updates when needed.

**Independent Audit Reports Available:** External Financial Auditor audited the password controls and internal user access approval/removal process in past 12 months.

## SCOPING DECISIONS

**High Risk Focus Areas:** Web-based application security testing. Secure coding techniques. IAM periodic reviews and architecture. Customer IAM – access management. DB security and performance management. Audit logging. Change management.

**Moderate Risk Focus Areas:** Incident management & recovery. Vendor management. System security plan.



# Example Scoping Memo (continued)

## FINAL SCOPING

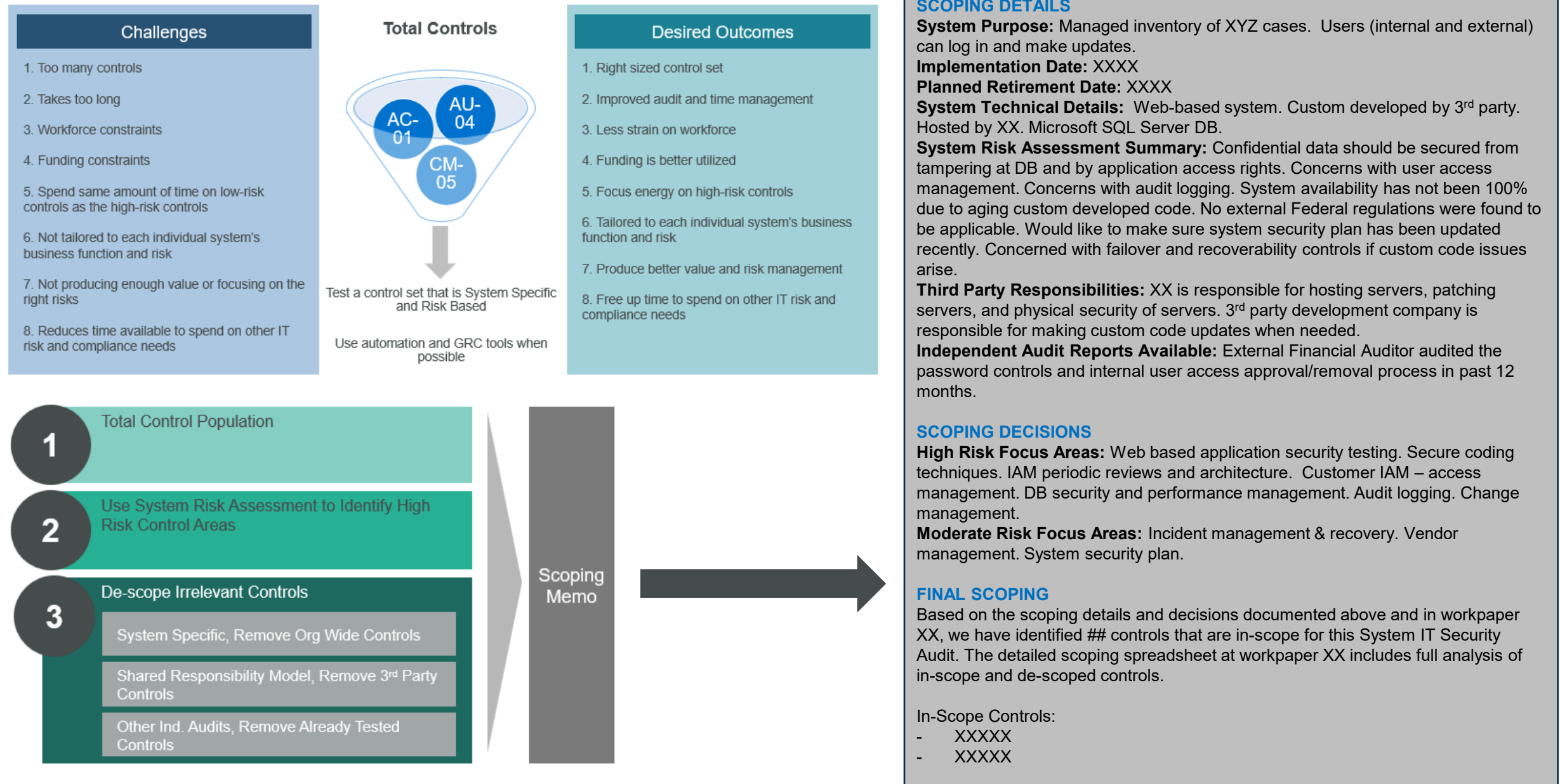
Based on the scoping details and decisions documented above and in workpaper XX, we have identified ## controls that are in-scope for this System IT Security Audit. The detailed scoping spreadsheet at workpaper XX includes full analysis of in-scope and de-scoped controls.

### In-Scope Controls:

- XXXXX
- XXXXX
- XXXXX
- XXXXX
- XXXXX
- XXXXX
- XXXXX
- XXXXX
- XXXXX
- XXXXX
- XXXXX
- XXXXX



# Scoping – Results





# Example Impact of Right-Sizing Assessments

	Traditional Approach	Right-Sized Approach
Controls Tested	500	90
Audit Duration	4 months	2 months
Audit Fatigue	High	Low
Risk Coverage	Broad, unfocused	Targeted, high-value





# Documenting Scoping Decisions

## How to Justify Exclusions & Focus Areas

### Criteria for Exclusion:

- Control is not system-specific (applies only at organization level)
- Control is managed by a third party (e.g., cloud provider, shared IT)
- Control already tested in recent independent audit (e.g., SOC 2, financial audit)
- Control is not applicable to the system's function or risk profile

### Documentation Best Practices:

- Use a scoping memo or spreadsheet to record all inclusions and exclusions
- Reference supporting evidence (contracts, audit reports, risk assessments)
- Clearly state rationale for each exclusion or focus area

### Sample Documentation Language:

- “Excluded: Managed by AWS under shared responsibility model (see contract XYZ).”
- “Excluded: Previously tested in SOC 2 audit, report dated MM/YYYY.”
- “Excluded: Not applicable—system does not process sensitive data.”



# Collaboration Tips

## How to Work With Auditors, IT, & Business Teams for Buy-In



### Engage Stakeholders Early

- Involve IT, business owners, and auditors in scoping discussions
- Share draft scope and rationale for feedback



### Joint Activities

- Conduct walkthroughs and system demos together
- Review documentation and evidence collaboratively



### Build Trust

- Be transparent about exclusions and focus areas
- Document decisions and share with all stakeholders



### Leverage Tools

- Use shared tracking tools (GRC platforms, spreadsheets)
- Schedule regular check-ins and updates





# Key Benefits

## Why Right-Sizing Matters



More efficient use of  
time and resources



Less audit fatigue for  
IT and business teams



Improved compliance  
and risk management  
(and more time for it)



Better coverage of  
high-risk areas



Stronger stakeholder  
buy-in and  
collaboration



# Contact

## Forvis Mazars

### Ben Sady

Principal, Consulting Services

**Tel: 804.474.1267**

**Mobile: 571.334.7431**

**[ben.sady@us.forvismazars.com](mailto:ben.sady@us.forvismazars.com)**

### Mareena Bowen

Manager, Consulting Services

**Tel: 804.474.1314**

**Mobile: 804.938.3628**

**[mareena.bowen@us.forvismazars.com](mailto:mareena.bowen@us.forvismazars.com)**

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.

© 2025 Forvis Mazars, LLP. All rights reserved.