

NIST SPECIAL PUBLICATION 1800-22 Supplement

Mobile Device Security: Bring Your Own Device (BYOD)

Supplement:

Example Scenario: Putting Guidance into Practice

Kaitlin Boeckl
Nakia Grayson
Gema Howell
Naomi Lefkovitz

Applied Cybersecurity Division
Information Technology Laboratory

Jason G. Ajmo
Milissa McGinnis*
Kenneth F. Sandlin
Oksana Slivina
Julie Snyder
Paul Ward

The MITRE Corporation
McLean, VA

**Former employee; all work for this publication done while at employer.*

March 2021

DRAFT

This publication is available free of charge from
<https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device>



1 Applying This Build: Example Scenario

2 An example scenario about a fictional company named Great Seneca Accounting illustrates how
3 organizations can use this practice guide's example solution. The example shows how Bring Your Own
4 Device (BYOD) objectives can align with a fictional organization's security and privacy priorities through
5 the use of risk management standards, guidance, and tools.

6 To demonstrate how an organization may use this National Institute of Standards and Technology (NIST)
7 Special Publication (SP) and other NIST tools to implement a BYOD use case, the National Cybersecurity
8 Center of Excellence created an example scenario that centers around a fictional, small-to-mid-size
9 organization called Great Seneca Accounting. This scenario exemplifies the issues that an organization
10 may face when addressing common enterprise BYOD security challenges.

11 1.1 Standards and Guidance Used in this Example Scenario

12 In addition to the Executive Summary contained in Volume A, and the architecture description in
13 Volume B, this practice guide also includes a series of how-to instructions in Volume C. The how-to
14 instructions in Volume C provide step-by-step instructions covering the initial setup (installation or
15 provisioning) and configuration for each component of the architecture. These step-by-step instructions
16 can help security engineers rapidly deploy and evaluate the example solution in their test environment.

17 The example solution uses standards-based, commercially available products that can be used by an
18 organization interested in deploying a BYOD solution. The example solution provides recommendations
19 for enhancing the security and privacy infrastructure by integrating on-premises and cloud-hosted
20 mobile security technologies. This practice guide provides an example solution that an organization may
21 use in whole or in part as the basis for creating a custom solution that best supports their unique needs.

22 The fictional Great Seneca Accounting organization illustrates how this guide may be applied by an
23 organization, starting with a mobile device infrastructure that lacked mobile device security architecture
24 concepts. Great Seneca employed multiple NIST cybersecurity and privacy risk management tools to
25 understand the gaps in its architecture and methods to enhance security of its systems and privacy for
26 its employees.

27 This example scenario provides useful context for using the following NIST Frameworks and other
28 relevant tools to help mitigate some of the security and privacy challenges that organizations may
29 encounter when deploying BYOD capabilities:

- 30 • NIST *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Cybersecurity
31 Framework) [1]
- 32 • the NIST *Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management*,
33 Version 1.0 (Privacy Framework) [2]
- 34 • NIST Special Publication (SP) 800-181 *National Initiative for Cybersecurity Education (NICE)*
35 *Cybersecurity Workforce Framework* [3]
- 36 • NIST Risk Management Framework [4]

- NIST Mobile Threat Catalogue [5]

For additional information, see Volume B's Appendix D.

2 About Great Seneca Accounting

In the example scenario, Great Seneca Accounting is a fictional accounting firm that grew from a single office location into a larger firm with a regional presence. Great Seneca Accounting performs accounting functions related to capturing, communicating, processing, transmitting, and analyzing financial data and accounting services for its customers.

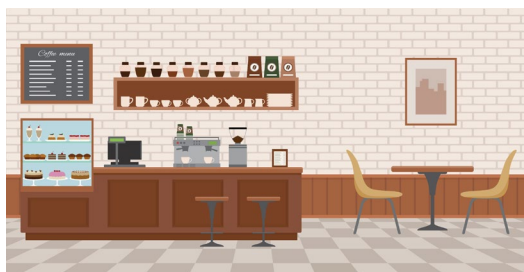
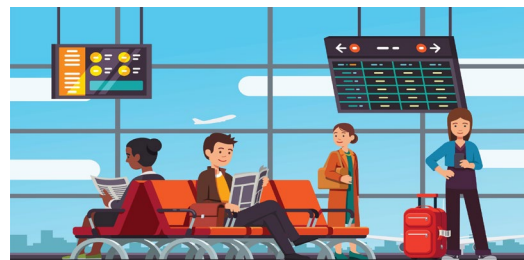
When the firm was first created, most of its employees worked from the Great Seneca Accounting office, with minimal use of mobile devices. They were able to do this without actively embracing mobile device usage because most of the employees worked at their desks at the company's single location.

Over the years, the Great Seneca Accounting company grew from a local company, where all of its employees performed work at their desks by using desktop computers provided by the organization, into a regional firm with employees who work remotely and who support regional customers.

Now, many of the employees spend part of their week traveling and working from customer or other remote locations. This has prompted the organization to specify, as a strategic priority, the need to support employees to work remotely, while both traveling and working from a customer location. As such, the company wants to embrace BYOD solutions to support its remote work.

Figure 1-1 shows an overview of the typical work environments for a Great Seneca Accounting employee. Many employees work remotely while using their own mobile phones and tablets to perform both work and personal activities throughout the day.

Figure 1-1 Great Seneca Accounting's Work Environments



Great Seneca Accounting’s corporate management initiated a complete review of all policies, procedures, and technology relating to its mobile deployment to ensure that the company is well protected against attacks involving personal mobile devices. This includes mitigating risks against its devices, custom applications, and corporate infrastructure supporting mobile services. Management identified NIST’s Risk Management Framework (RMF) [4] and Privacy Risk Assessment Methodology (PRAM) [6] as useful tools for supporting this analysis. The company developed Cybersecurity Framework and Privacy Framework Target Profiles to guide Great Seneca Accounting’s decision-making because the Target Profiles link Great Seneca Accounting’s mission and business priorities with supporting cybersecurity and privacy activities.

Great Seneca Accounting identified the scope of their mobile solution to be both Android and Apple personally owned mobile phones and tablets. While this example scenario intends to provide an exemplar of organization guidance with a description of BYOD concepts and how to apply those concepts, this example scenario should not suggest a limit on BYOD uses.

Great Seneca Accounting plans to use NIST SP 1800-22 (this practice guide) to inform its updated BYOD architecture as well as NIST’s Mobile Threat Catalogue to identify threats to mobile deployment. These NIST frameworks and tools used are described further in [Appendix E](#).

As shown in [Figure 2-1](#), this example solution applied multiple mobile device security technologies. These included a cloud-based Enterprise Mobility Management solution integrated with cloud- and agent-based mobile security technologies to help deploy a set of security and privacy capabilities that support the example solution.

Figure 2-2 Example Solution Architecture

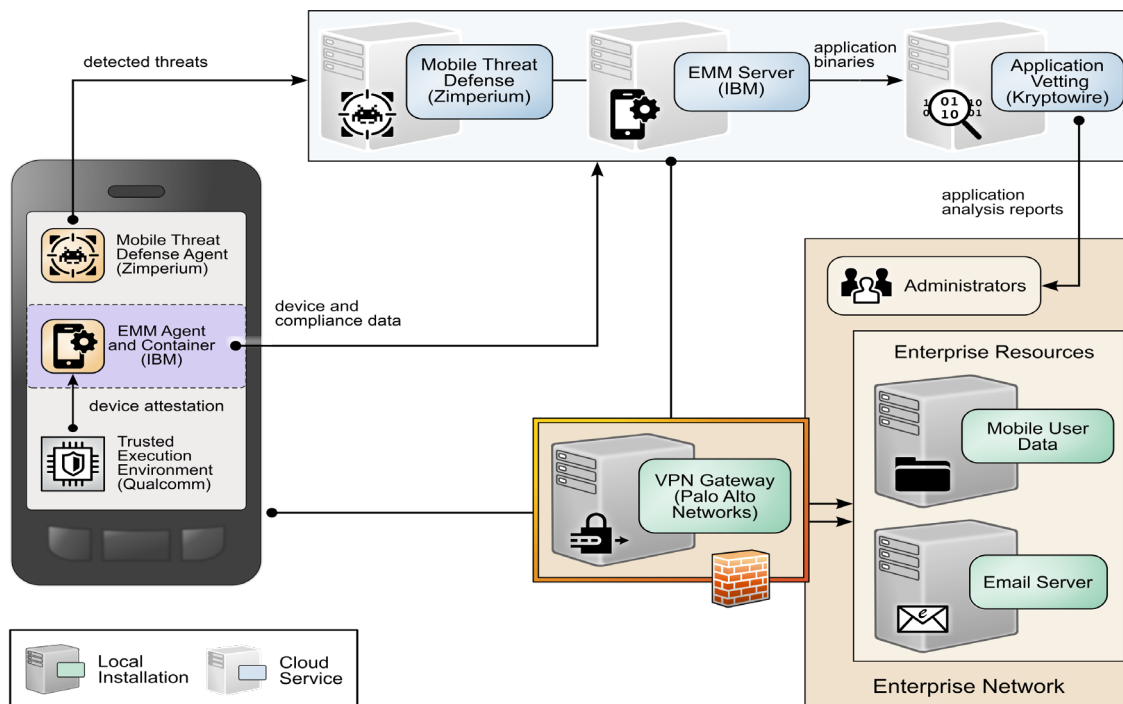
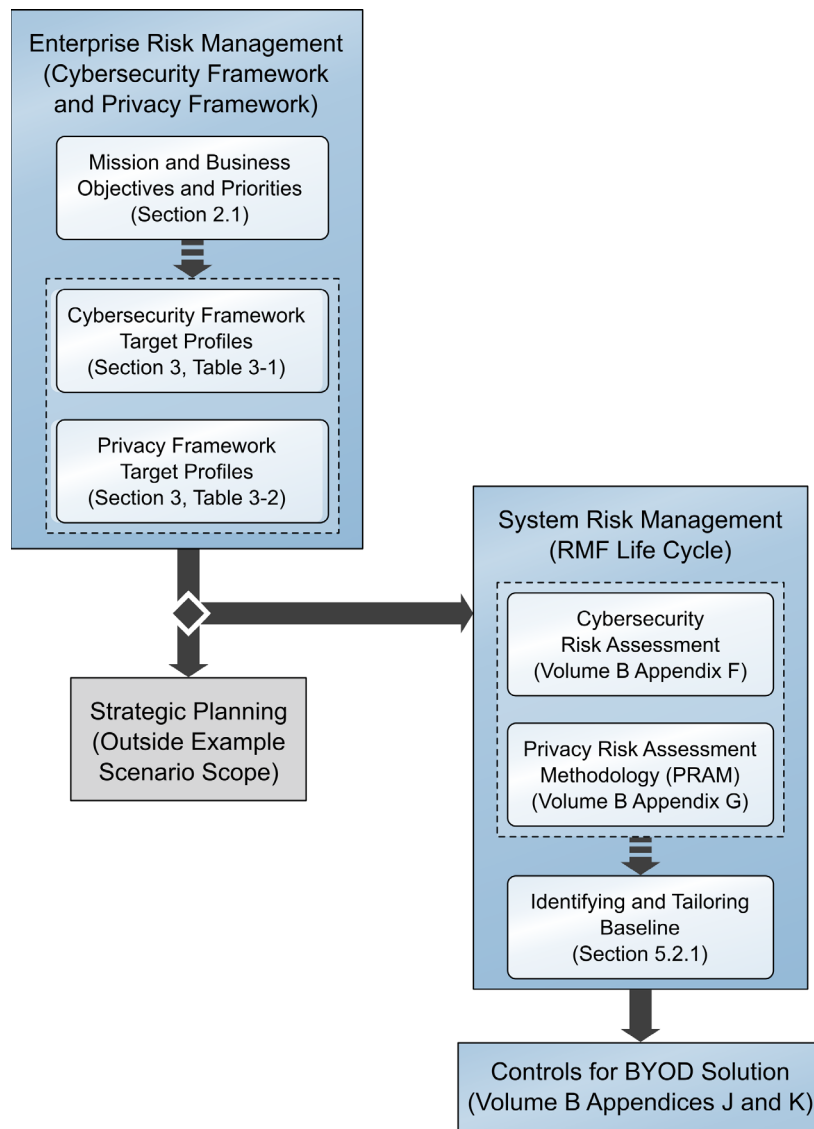


Figure 2-2 shows the overall process that Great Seneca Accounting plans to follow. It highlights key activities from various NIST guidance documents related to security and privacy risk management, each of which is discussed in the sections identified in Figure 2-2. Please note that this process is an abbreviated version of steps provided in NIST SP 800-37 Revision 2 [7], which shows how some available resources may be used by any organization.

Figure 2-3 Great Seneca Accounting's Security and Privacy Risk Management Steps



2.1 Great Seneca Accounting's Business/Mission Objectives

Great Seneca Accounting developed a mission statement and a set of supporting business/mission objectives to ensure that its activities align with its core purpose. The company has had the same mission since it was founded:

Mission Statement

Provide financial services with integrity and responsiveness

While Great Seneca Accounting has a number of business/mission objectives, those below relate to its interest in BYOD, listed in priority order:

1. Provide good data stewardship.
2. Enable timely communication with clients.
3. Provide innovative financial services.
4. Enable workforce flexibility.

3 Great Seneca Accounting's Target Profiles

Great Seneca Accounting used the NIST Cybersecurity Framework and *NIST Privacy Framework* as key strategic planning tools to improve its security and privacy programs. It followed the processes outlined in the frameworks, and as part of that effort, created two Target Profiles—one for cybersecurity and one for privacy.

These Target Profiles describe the desired or aspirational state of Great Seneca Accounting by identifying and prioritizing the cybersecurity and privacy activities and outcomes needed to support its enterprise business/mission objectives. The Subcategories in each Framework Core articulate those cybersecurity and privacy activities and outcomes.

Note: See [Appendix E](#) for a high-level description of the Cybersecurity Framework and Privacy Framework.

To understand what Subcategories to prioritize implementing in each framework, Great Seneca Accounting considered the importance of the Subcategories for accomplishing each business/mission objective. The Target Profiles reflect that discussion by designating prioritized Subcategories as low, moderate, or high.

Subcategory improvements important for BYOD deployment also became part of its Target Profiles because Great Seneca Accounting was upgrading its existing information technology infrastructure as part of its BYOD implementation.

The Cybersecurity Framework Target Profile in [Table 3-1](#) and the Privacy Framework Target Profile in [Table 3-2](#) are included as examples of Great Seneca Accounting's identification of the business/mission objectives that are relevant to their BYOD deployment.

Great Seneca Accounting chose to address the Subcategories that are prioritized as moderate and high for multiple business/mission objectives in its Target Profiles for this year's BYOD deployment with plans to address the low Subcategories in the future.

121 [Table 3-1](#) and [Table 3-2](#) include only those Subcategories that are prioritized as moderate or high for the
122 business/mission Objectives. Any Subcategory designated as low is included in [Table 3-1](#) and [Table 3-2](#)
123 only because it is high or moderate for another business/mission objective.

124 Great Seneca Accounting used the Target Profiles to help guide risk management decisions throughout
125 the organization's activities, including making decisions regarding budget allocation, technology design,
126 and staffing for its programs and technology deployments. Discussions for developing and using the
127 Target Profiles include stakeholders in various parts of the organization, such as business/mission
128 program owners, data stewards, cybersecurity practitioners, privacy practitioners, legal and compliance
129 experts, and technology experts.

130 **Note:** Low, moderate, and high designations indicate the level of relative importance among
131 Subcategories for Great Seneca to accomplish a business/mission objective.

132 Table 3-1 Great Seneca Accounting's Cybersecurity Framework Target Profile

Cybersecurity Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable timely communication with clients	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
IDENTIFY	Asset Management	ID.AM-1: Physical devices and systems within the organization are inventoried.	moderate	moderate	moderate	low
		ID.AM-2: Software platforms and applications within the organization are inventoried.	moderate	moderate	moderate	low
	Risk Assessment	ID.RA-1: Asset vulnerabilities are identified and documented.	moderate	moderate	moderate	moderate
		ID.RA-3: Threats, both internal and external, are identified and documented.	moderate	moderate	moderate	moderate
PROTECT	Identity Management and Access Control	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	moderate	high	moderate	high
		PR.AC-3: Remote access is managed.	moderate	high	high	high
		PR.AC-5: Network integrity is protected (e.g., network	high	high	high	high

Cybersecurity Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable timely communication with clients	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
		segregation, network segmentation).				
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	moderate	high	high	high
	Data Security	PR.DS-1: Data-at-rest is protected.	high	moderate	moderate	high
		PR.DS-2: Data-in-transit is protected.	moderate	high	moderate	high
		PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	high	moderate	moderate	high
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.	moderate	moderate	moderate	low
	Information Protection Processes and Procedures	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles.	moderate	moderate	moderate	low

Cybersecurity Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable timely communication with clients	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
	Protective Technology	PR.PT-4: Communications and control networks are protected.	low	moderate	moderate	low
DETECT	Anomalies and Events	DE.AE-5: Incident alert thresholds are established.	high	high	high	high
	Security Continuous Monitoring	DE.CM-4: Malicious code is detected.	high	high	high	high
		DE.CM-5: Unauthorized mobile code is detected.	moderate	moderate	moderate	low
		DE.CM-8: Vulnerability scans are performed.	high	high	high	high

133 Table 3-2 Great Seneca Accounting's Privacy Target Profile

Privacy Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable timely communication with clients	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
IDENTIFY-P	Inventory and Mapping	ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	high	high	high	high
GOVERN-P	Governance Policies, Processes, and Procedures	GV.PO-P1: Organizational privacy values and policies (e.g., conditions on data processing, individuals' prerogatives with respect to data processing) are established and communicated.	high	high	high	high
		GV.PO-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	high	high	high	high
	Monitoring and Review	GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.	high	high	high	high

Privacy Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable timely communication with clients	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
		GV.MT-P5: Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers, professional events).	high	high	high	high
CONTROL-P	Data Management	CT.DM-P1: Data elements can be accessed for review.	high	moderate	high	moderate
		CT.DM-P3: Data elements can be accessed for alteration.	high	moderate	high	moderate
		CT.DM-P4: Data elements can be accessed for deletion.	high	moderate	high	moderate
		CT.DM-P5: Data are destroyed according to policy.	high	moderate	high	moderate
	Disassociated Processing	CT.DP-P4: System or device configurations permit	high	high	high	high

Privacy Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable timely communication with clients	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
		selective collection or disclosure of data elements.				
COMMUNICATE-P	Data Processing Awareness	CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.	high	moderate	moderate	moderate
PROTECT-P	Data Protection Policies, Processes, and Procedures	PR.PO-P3: Backups of information are conducted, maintained, and tested.	high	moderate	high	moderate
		PR.AC-P1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	moderate	high	moderate	high
	Identity Management, Authentication, and Access Control	PR.AC-P2: Physical access to data and devices is managed.	high	moderate	high	moderate
		PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	high	moderate	high	moderate

Privacy Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable timely communication with clients	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	high	high	high	high
		PR.DS-P1: Data-at-rest are protected.	high	moderate	moderate	high
	Data Security	PR.DS-P2: Data-in-transit are protected.	moderate	high	moderate	high
		PR.DS-P5: Protections against data leaks are implemented.	high	moderate	high	moderate
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	high	moderate	moderate	high
		PR.PT-P3: Communications and control networks are protected.	moderate	high	moderate	high

4 Great Seneca Accounting Embraces BYOD

Great Seneca Accounting now allows its staff to use their personal mobile devices to perform their daily work duties on an as-needed basis. Accountants use the devices for various tasks including communicating with client organizations and other employees, collecting confidential client information, analyzing financial transactions, generating reports, accessing tax and payroll information, and creating and reviewing comprehensive financial statements.

Great Seneca accountants work from many locations including their corporate office building, their homes, their customers' offices, and other locations. And to be able to work in all of these locations, they require the use of mobile devices to perform their job functions.

Great Seneca Accounting's current mobile infrastructure enables accountants to perform their job duties by using their personally owned devices, despite minimal security installed and enforced on these devices. Examples of security concerns with the use of personally owned devices are:

- Employees can connect to any Wi-Fi network to perform work-related activities when they are working on the road, including at a client's site.
- Custom mobile applications being sideloaded onto devices that employees use.
- The personally owned devices allow users to install applications on an as-needed basis without separation of enterprise and personal data.

While not affecting Great Seneca Accounting, a string of well-publicized cybersecurity attacks have recently been reported in the news, and this prompted Great Seneca to review its mobile device security and privacy deployment strategy. When making BYOD deployment decisions, Great Seneca Accounting plans to prioritize implementing cybersecurity and privacy capabilities that would enable it to accomplish its business/mission objectives (i.e., its reasons for deploying BYOD capabilities).

To do this, Great Seneca Accounting conducted a technical assessment of its current BYOD architecture to help it understand ways to improve the confidentiality, integrity, availability, and privacy of data and devices associated with its BYOD deployment. The company identified several vulnerabilities based on its current mobile device deployment. [Figure 4-1](#) below presents a subset of those vulnerabilities.

Figure 4-1 Great Seneca Accounting's Current Mobile Deployment Architecture (Before Security and Privacy Enhancements)

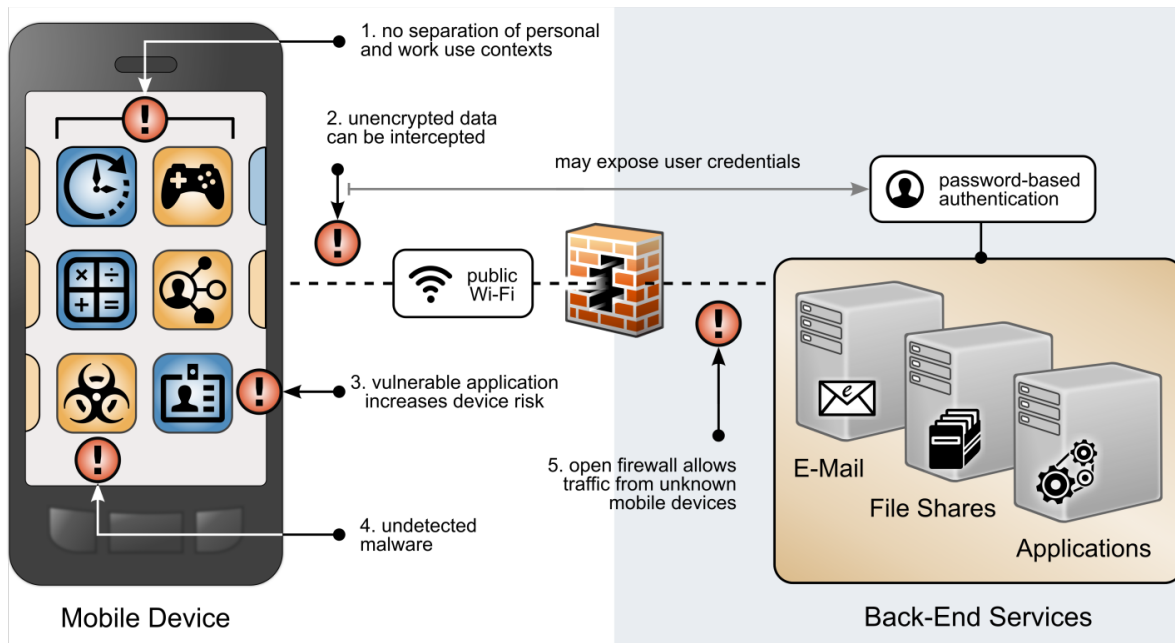


Figure 4-1 highlights the following vulnerabilities with a red exclamation mark:

1. BYOD deployments can place organizational and personal data, as well as employees' privacy, at risk. Organizational and personal data can become commingled if either the same application is used in both contexts or if multiple applications access shared device resources (e.g., contacts or calendar) as applications for both personal and work usage are installed. This also puts employees' privacy at risk, as the organization can have visibility into their personal life outside work.
2. BYOD deployments can leverage nonsecure networks. As employees use nonsecure Wi-Fi hotspots, mobile devices that are connecting to Great Seneca Accounting from those unencrypted networks place data transmitted prior to a secure connection at risk of discovery and eavesdropping, including passwords.
3. As employees install applications on their personally owned devices, the applications can have unidentified vulnerabilities or weaknesses that increase the risk of device compromise (e.g., applications that access contacts may now have access to the organization's client contact information). Further, legitimate, privacy-intrusive applications can legally collect data through terms and conditions and requested permissions.
4. On personally owned devices without restriction policies in place, employees may inadvertently download applications outside official application stores, which are malware in disguise.

5. Because personally owned mobile devices can connect from unknown locations, firewall rules must allow inbound connections from unrecognized, potentially malicious Internet Protocol addresses.

In addition to identifying the technical assets and the vulnerabilities, Great Seneca Accounting identified the scope of the mobile solution (i.e., both Android and Apple personally owned mobile phones and tablets) and the regulatory requirements or guidance that will apply to their deployment and solution (e.g., encryption will be Federal Information Processing Standards [FIPS]-validated to protect sensitive accounting information).

5 Applying NIST Risk Management Methodologies to Great Seneca Accounting's BYOD Architecture

Sections 2 and 3 described Great Seneca Accounting, their business mission, and what security and privacy areas they consider most important. Great Seneca created Target Profiles that mapped their BYOD-related mission/business objectives and priorities with the Functions, Categories, and Subcategories of both the Cybersecurity Framework and the Privacy Framework. Those Cybersecurity Framework and Privacy Framework Target Profiles are provided in [Table 3-1](#) and [Table 3-2](#) in Section 3 of this document.

Now, the Target Profiles provided in Section 3 will demonstrate the role they play in identifying and prioritizing the implementation of the security and privacy controls, as well as the capabilities that Great Seneca would like to include in its new BYOD security and privacy-enhanced architecture.

5.1 Using Great Seneca Accounting's Target Profiles

The Cybersecurity Framework maps its Subcategories to Informative References. The Informative References contained in the Framework Core provide examples of methods that Great Seneca can use to achieve its desired outcomes. The Cybersecurity Framework's Subcategory and Informative References mappings include NIST SP 800-53 controls.

An illustrative segment of the Cybersecurity Framework's Framework Core is shown in [Figure 5-1](#). Highlighted in the green box is an example of how the Cybersecurity Framework provides a mapping of Subcategories to Informative References.

207 **Figure 5-1 Cybersecurity Framework Subcategory to Informative Reference Mapping**

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9

208 To provide a starting point for Great Seneca's mapping of their Cybersecurity Framework and Privacy
 209 Framework Target Profiles to the NIST SP 800-53 security and privacy controls and capabilities, Great
 210 Seneca leveraged the mapping provided in the Cybersecurity Framework. An example of the
 211 Cybersecurity Framework's mapping is provided in [Figure 5-1](#).

212 See Volume B's Appendixes G and H for additional information on the security and privacy outcomes
 213 that this document's example solution supports. Appendixes G and H provide a mapping of this
 214 document's example solution capabilities with the related Subcategories in the Cybersecurity
 215 Framework and Privacy Framework.

216 Volume B's Appendix G provides the Cybersecurity Framework Subcategory mappings, and Volume B's
 217 Appendix H provides the Privacy Framework Subcategory mappings. An excerpt of Volume B's Appendix
 218 G is shown below in [Figure 5-2](#).

219 **Figure 5-2 Volume B Appendix G Example Solution Cybersecurity Framework Mapping Excerpt**

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles
Mobile Threat Defense						
Kryptowire Cloud Service	Application Vetting	ID.RA-1: Asset vulnerabilities are identified and documented.	CA-2, CA-7, CA-8: Security Assessment and Authorization RA-3, RA-5: Risk Assessment SA-4: Acquisition Process SI-7: Software, Firmware, and Information Integrity	A.12.6.1: Control of technical vulnerabilities A.18.2.3: Technical Compliance Review	CSC 4: Continuous Vulnerability Assessment and Remediation	SP-RSK-002: Security Control Assessor SP-ARC-002: Security Architect OM-ANA-001: Systems Security Analyst

221 5.2 Great Seneca Uses the Target Profiles to Help Prioritize Security and

222 Privacy Control Deployment

223 Due to budget constraints, Great Seneca Accounting will focus on implementing the higher priority
 224 security and privacy controls that were identified in the organization's two Target Profiles first. The
 225 company will then focus on implementing lower priority controls when more funding becomes available.
 226 This is accomplished by Great Seneca Accounting comparing the prioritized Subcategories contained in
 227 Section 3's [Table 3-1](#) and [Table 3-2](#) with the outcomes that the example solution supports.

228 By comparing its Cybersecurity Framework Target Profile ([Table 3-1](#)) with the Subcategories supported
 229 by the example solution that are shown in Volume B's Appendix G, Great Seneca Accounting determines
 230 that the example solution will help it achieve its desired Cybersecurity Framework Target Profile
 231 outcomes.

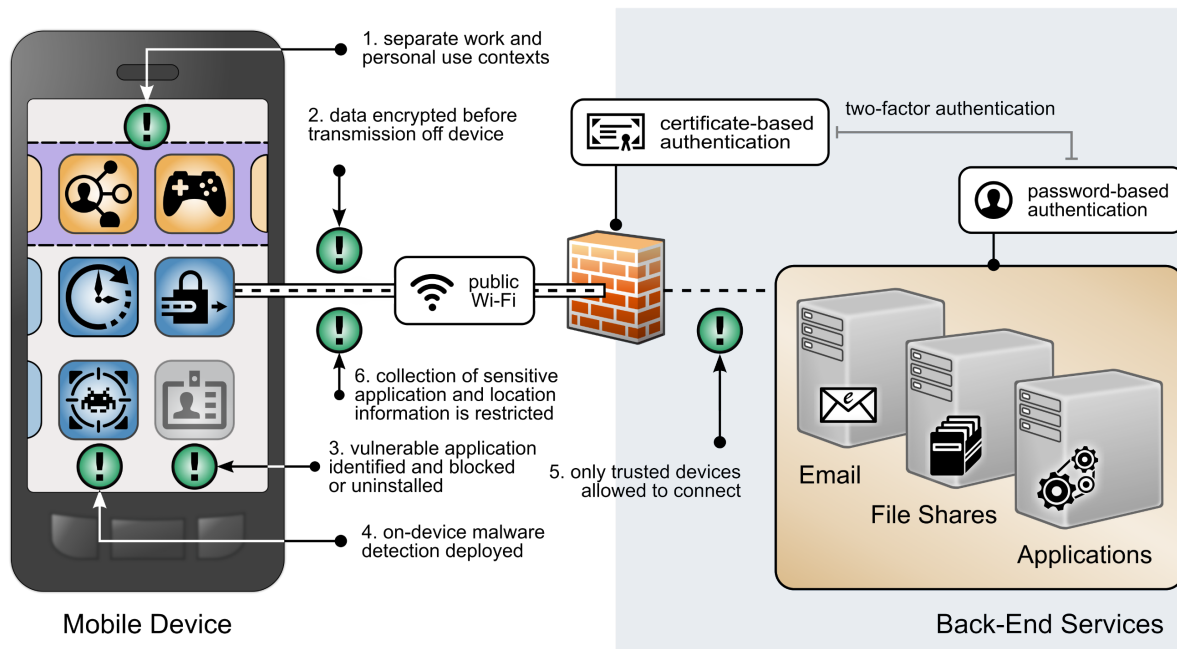
232 Great Seneca performs a similar comparison of the Privacy Framework Target Profile in [Table 3-2](#) with
 233 the Subcategories supported by the example solution that are shown in Volume B's Appendix H. From
 234 that comparison of the example solution's capabilities and Great Seneca's privacy-related architecture
 235 goals, Great Seneca determines that the example solution provided in this practice guide will help it to
 236 achieve the privacy-related outcomes that were identified in [Table 3-2's](#) Privacy Framework Target
 237 Profile.

238 5.2.1 Identifying and Tailoring the Baseline Controls

239 Now that Great Seneca Accounting understands how the Target Profiles will help prioritize the
 240 implementation of the high-level security and privacy goals shown in [Figure 5-3](#), it would like to look

more closely at the NIST SP 800-53 controls it will initially implement in its new BYOD architecture. This will help Great Seneca identify the capabilities it will deploy first to meet its architecture needs.

Figure 5-3 Security and Privacy Goals



Volume B's Appendix G and H provide a list of the controls that the example solution implements, including how the controls in the example solution align to the Subcategories in both the Cybersecurity Framework and Privacy Framework. Because these controls only focus on the example solution, Great Seneca will need to implement additional controls that address the unique risks associated with its environment.

To help identify the specific controls Great Seneca Accounting will be implementing to support the new BYOD architecture, it uses the NIST RMF process to manage security and privacy risk for its systems. The organization decides to follow the RMF guidance in NIST SP 800-37 [7] to conduct security and privacy risk assessments as it continues preparing to design its new solution.

5.3 Great Seneca Accounting Performs a Risk Assessment

Great Seneca Accounting completes a security risk assessment by using the guidance in NIST SP 800-30 [8] and the Mobile Threat Catalogue [5] to identify cybersecurity threats to the organization. The company then uses the NIST PRAM [6] to perform a privacy risk assessment. Appendix F and G describe these risk assessments in more detail. These risk assessments produce two significant conclusions:

1. Great Seneca Accounting finds similar cybersecurity threats in its environment and problematic data actions for employee privacy as those discussed in NIST SP 1800-22, validating that the controls discussed in the example solution are relevant to their environment.
2. The organization determines that it has a high-impact system, based on the impact guidance in NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* [9], and needs to implement more controls beyond those identified in NIST SP 1800-22 and its Target Profiles to support the additional system components in its own solution (e.g., underlying OS, the data center where the equipment will reside).

5.4 Great Seneca Accounting Tailors Their Security and Privacy Control Baselines

As part of their review of NIST FIPS 200 [9], Great Seneca Accounting selects the high controls baseline in NIST SP 800-53 [10] for their BYOD architecture implementation. They then tailor the control baselines based on the needs identified through the priority Subcategories in its cybersecurity and privacy Target Profiles.

Control baselines are tailored to meet their organization's needs. NIST SP 800-53 [10] defines tailoring as "The process by which security control baselines are modified by: (i) identifying and designating common controls; (ii) applying scoping considerations on the applicability and implementation of baseline controls; (iii) selecting compensating security controls; (iv) assigning specific values to organization-defined security control parameters; (v) supplementing baselines with additional security controls or control enhancements; and (vi) providing additional specification information for control implementation."

While not discussed in this example scenario, Great Seneca also plans to make tailoring decisions based on other unique needs in its environment (e.g., legal and regulatory requirements).

5.4.1 An Example Tailoring of the System and Communications Protection Security Control Family

As Great Seneca Accounting reviews the System and Communications Protection (SC) control family in NIST SP 800-53 [10], it notes there are opportunities for tailoring.

For example, the NIST SP 800-53 baseline includes control enhancements, whereas the Cybersecurity Framework Informative References contain only base controls. Great Seneca Accounting decides to implement the enhancements that are applicable to a high-impact system for the SC controls they have selected.

Using this decision as a guide, Great Seneca Accounting also makes the following tailoring decisions related to the NIST SP 800-53 SC control family:

- NIST SP 800-53 provides recommendations regarding implementation priorities for controls. The implementation priorities of controls related to some Cybersecurity Framework Subcategories

were adjusted to be higher or lower based on their alignment with Subcategory prioritization in the Target Profile.

- For example, the implementation priority for Cybersecurity Framework Subcategory DE.CM-5 was identified as having low or moderate importance for accomplishing all four BYOD-Related Business/Mission Objectives. NIST SP 800-53 designates control SC-18, which supports the implementation of Cybersecurity Framework Subcategory DE.CM-5, as high priority. However, since Cybersecurity Framework Subcategory DE.CM-5 is moderate or low priority in this context, Great Seneca makes a tailoring decision to lower the implementation priority for the SC-18 NIST SP 800-53 control to moderate.
 - DE.CM-5's importance designations for accomplishing the BYOD-Related Business/Mission Objectives are highlighted in green in [Figure 5-4](#).

Figure 5-4 Subcategory DE.CM-5 Mapping to BYOD-Related Business/Mission Objectives

Cybersecurity Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable Workforce Flexibility	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
DETECT	Security Continuous Monitoring	DE.CM-5: Unauthorized mobile code is detected.	moderate	moderate	moderate	low

- Conversely, just as the implementation priority for the NIST SP 800-53 control that supports implementation of Subcategory DC-CM-5 was lowered based on the Target Profile, the implementation priority for the NIST SP 800-53 controls that supports implementation of Cybersecurity Framework Subcategory PR.AC-5 was raised. This is because Subcategory PR.AC-5 was identified as having high importance for accomplishing all four BYOD-Related Business/Mission Objectives.
 - The NIST SP 800-53 SC Family security control related to the Cybersecurity Framework Subcategory PR.AC-5 is SC-7. NIST SP 800-53 prioritizes control SC-7 as low. Since control SC-7 supports the implementation of a Cybersecurity Framework Subcategory that is designated as high priority in Great Seneca's Target Profile (Cybersecurity Framework Subcategory PR.AC-5), Great Seneca makes a tailoring decision to increase the priority of NIST SP 800-53 control SC-7 to high.
 - PR.AC-5's high importance designation for accomplishing the BYOD-Related Business/Mission Objectives are highlighted in green in [Figure 5-5](#). All Subcategory prioritizations (including PR.AC-5's shown below) can be found in [Table 3-1](#).

322 **Figure 5-5 Subcategory PR.AC-5 Mapping to BYOD-Related Business/Mission Objectives**

Cybersecurity Framework Core			BYOD-Related Business/Mission Objectives			
Function	Category	Subcategory	(1) Provide Good Data Stewardship	(2) Enable Workforce Flexibility	(3) Provide Innovative Financial Services	(4) Enable Workforce Flexibility
PROTECT	Identity Management and Access Control	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	high	high	high	high

323

324 Great Seneca Accounting follows the same approach for the privacy controls in NIST SP 800-53, using
 325 the Privacy Framework Target Profile and controls identified through its PRAM analysis (for more
 326 information reference [Appendix G](#)).

327 Great Seneca Accounting will evaluate the security controls as they come up for review under its
 328 continuous monitoring program to determine whether there are enhancements to the implemented
 329 security controls that can be made over time.

330 In addition to identifying controls to select, the priorities articulated in Target Profiles will also help
 331 Great Seneca Accounting decide how to align financial resources for controls implementation (e.g.,
 332 buying a tool to automate a control as opposed to relying on policy and procedures alone). The Target
 333 Profiles will help Great Seneca identify how robustly to re-assess the efficacy of implemented controls
 334 before new system components or capabilities are enabled in a production environment. Great Seneca
 335 will also be able to use the Target Profiles to help evaluate the residual risks of the architecture in the
 336 context of Great Seneca Accounting's business/mission objectives, and the frequency and depth of
 337 continued monitoring requirements over time.

338 **Note:** All of the tailoring decisions discussed above are for example purposes only. An organization's
 339 actual tailoring decision will be based upon their own unique business/mission objectives, risk
 340 assessment results, and organizational needs that may significantly vary from these examples.

341 **Appendix A List of Acronyms**

BYOD	Bring Your Own Device
FIPS	Federal Information Processing Standards
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
PRAM	Privacy Risk Assessment Methodology
RMF	Risk Management Framework
SP	Special Publication

342 **Appendix B** **Glossary**

Access Management	Access Management is the set of practices that enables only those permitted the ability to perform an action on a particular resource. The three most common Access Management services you encounter every day perhaps without realizing it are: Policy Administration, Authentication, and Authorization [11].
Availability	Ensure that users can access resources through remote access whenever needed [12].
Bring Your Own Device (BYOD)	A non-organization-controlled telework client device [12].
Confidentiality	Ensure that remote access communications and stored user data cannot be read by unauthorized parties [12].
Data Actions	System operations that process PII [13].
Disassociability	Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system [13].
Eavesdropping	An attack in which an Attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the Claimant [14] (definition located under eavesdropping attack).
Firewall	Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures [15].
Integrity	Detect any intentional or unintentional changes to remote access communications that occur in transit [12].
Manageability	Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure [13].
Mobile Device	A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for

synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers [10].

**Personally
Identifiable
Information
(PII)**

Any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information [16] (adapted from Government Accountability Office Report 08-536).

**Problematic
Data Action**

A data action that could cause an adverse effect for individuals [2].

Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service [8].

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source [8].

Appendix C References

- [1] National Institute of Standards and Technology (NIST). *NIST Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Cybersecurity Framework). Apr. 16, 2018. [Online]. Available: <https://www.nist.gov/cyberframework>.
- [2] NIST. *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*, Version 1.0 (Privacy Framework). Jan. 16, 2020. [Online]. Available: <https://www.nist.gov/privacy-framework>.
- [3] W. Newhouse et al., *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, NIST Special Publication (SP) 800-181, NIST, Gaithersburg, Md., Aug. 2017. Available: <https://csrc.nist.gov/publications/detail/sp/800-181/final>.
- [4] NIST. Risk Management Framework (RMF) Overview. [Online]. Available: [https://csrc.nist.gov/projects/risk-management/risk-management-framework-\(rmf\)-overview](https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview).
- [5] NIST. Mobile Threat Catalogue. [Online]. Available: <https://pages.nist.gov/mobile-threat-catalogue/>.
- [6] NIST. NIST Privacy Risk Assessment Methodology. Jan. 16, 2020. [Online]. Available: <https://www.nist.gov/privacy-framework/nist-pram>.
- [7] Joint Task Force, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST SP 800-37 Revision 2, NIST, Gaithersburg, Md., Dec. 2018. Available: <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>.
- [8] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments*, NIST SP 800-30 Revision 1, NIST, Gaithersburg, Md., Sept. 2012. Available: <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>.
- [9] NIST. *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards Publication (FIPS) 200, Mar. 2006. Available: <https://csrc.nist.gov/publications/detail/fips/200/final>.
- [10] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53 Revision 5, NIST, Gaithersburg, Md., Sept. 2020. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>.
- [11] IDManagement.gov. "Federal Identity, Credential, and Access Management Architecture." [Online]. Available: <https://arch.idmanagement.gov/services/access/>.

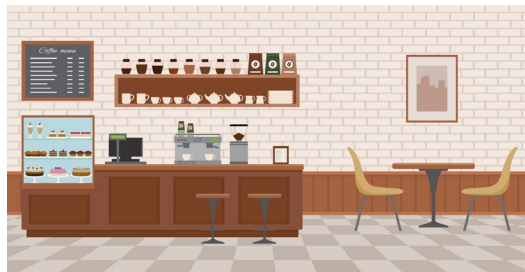
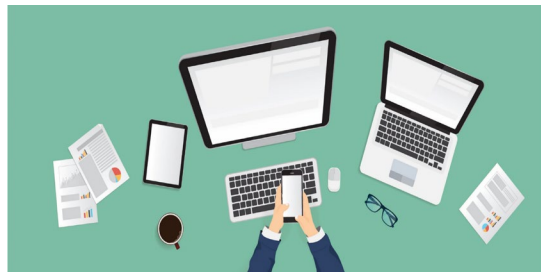
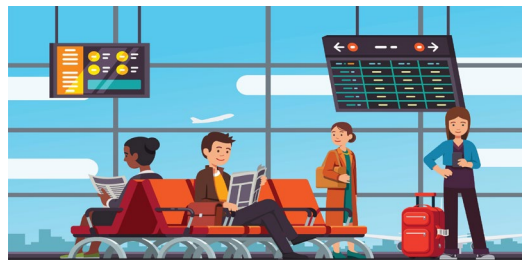
- 374 [12] M. Souppaya and K. Scarfone, *Guide to Enterprise Telework, Remote Access, and Bring Your Own*
375 *Device (BYOD) Security*, NIST SP 800-46 Revision 2, NIST, Gaithersburg, Md., July 2016. Available:
376 <https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final>.
- 377 [13] S. Brooks et al., *An Introduction to Privacy Engineering and Risk Management in Federal*
378 *Systems*, NIST Interagency or Internal Report 8062, Gaithersburg, Md., Jan. 2017. Available:
379 <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf>.
- 380 [14] P. Grassi et al., *Digital Identity Guidelines*, NIST SP 800-63-3, NIST, Gaithersburg, Md., June 2017.
381 Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>.
- 382 [15] K. Stouffer et al., *Guide to Industrial Control Systems (ICS) Security*, NIST SP 800-82 Revision 2,
383 NIST, Gaithersburg, Md., May 2015. Available:
384 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>.
- 385 [16] E. McCallister et al., *Guide to Protecting the Confidentiality of Personally Identifiable Information*
386 *(PII)*, NIST SP 800-122, NIST, Gaithersburg, Md., Apr. 2010. Available:
387 <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>.
- 388 [17] J. Franklin et al., *Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)*, NIST SP
389 1800-21, NIST, Gaithersburg, Md., July 22, 2019. Available:
390 <https://csrc.nist.gov/News/2019/NIST-Releases-Draft-SP-1800-21-for-Comment>.
- 391 [18] NIST, NIST Interagency Report (NISTIR) 8170, *Approaches for Federal Agencies to Use the*
392 *Cybersecurity Framework*, Mar. 2020. [Online]. Available:
393 <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8170.pdf>.
- 394 [19] NIST. Risk Management Framework (RMF) Overview. [Online]. Available:
395 [https://csrc.nist.gov/projects/risk-management/risk-management-framework-\(rmf\)-overview](https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview).

Appendix D A Note Regarding Great Seneca Accounting

A description of a fictional organization, Great Seneca Accounting, was included in the National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-22 Mobile Device Security: Bring Your Own Device (BYOD) Practice Guide.

This fictional organization demonstrates how a small-to-medium sized, regional organization implemented the example solution in this practice guide to assess and protect their mobile-device-specific security and privacy needs. It illustrates how organizations with office-based, remote-working, and travelling personnel can be supported in their use of personally owned devices that enable their employees to work while on the road, in the office, at customer locations, and at home.

Figure D-1 Great Seneca Accounting's Work Environments



Appendix E How Great Seneca Accounting Applied NIST Risk Management Methodologies

This practice guide contains an example scenario about a fictional organization called Great Seneca Accounting. The example scenario shows how to deploy a Bring Your Own Device (BYOD) solution to be in alignment with an organization's security and privacy capabilities and objectives.

The example scenario uses National Institute of Standards and Technology (NIST) standards, guidance, and tools. It is provided in the *Example Scenario: Putting Guidance into Practice* supplement of this practice guide.

This appendix provides a brief description of some of the key NIST tools referenced in the example scenario supplement of this practice guide.

In this Appendix, Section E.1 provides descriptions of the risk frameworks and tools, along with a high-level discussion of how Great Seneca Accounting applied each framework or tool in the example scenario. Section E.2 describes how the *NIST Cybersecurity Framework* and *NIST Privacy Framework* can be used to establish or improve cybersecurity and privacy programs.

E.1 Overview of Risk Frameworks and Tools That Great Seneca Used

Great Seneca used NIST frameworks and tools to identify common security and privacy risks related to BYOD solutions and to guide approaches to how they were addressed in the architecture described in Section 4. Great Seneca used additional standards and guidance, listed in Appendix D of Volume B, to complement these frameworks and tools when designing their BYOD architecture.

Both the Cybersecurity Framework and Privacy Framework include the concept of Framework Profiles, which identify the organization's existing activities (contained in a Current Profile) and articulate the desired outcomes that support its mission and business objectives within its risk tolerance (that are contained in the Target Profile). When considered together, Current and Target Profiles are useful tools for identifying gaps and for strategic planning.

E.1.1 Overview of the NIST Cybersecurity Framework

Description: The NIST Cybersecurity Framework “is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.” [17]

Application: This guide refers to two of the main components of the Cybersecurity Framework: the Framework Core and the Framework Profiles. As described in Section 2.1 of the Cybersecurity Framework, the Framework Core provides a set of activities to achieve specific cybersecurity outcomes,

and reference examples of guidance to achieve those outcomes (e.g., controls found in NIST Special Publication [SP] 800-53). Section 2.3 of the Cybersecurity Framework identifies Framework Profiles as the alignment of the Functions, Categories, and Subcategories (i.e., the Framework Core) with the business requirements, risk tolerance, and resources of the organization.

The Great Seneca Accounting example scenario assumed that the organization used the Cybersecurity Framework Core and Framework Profiles, specifically the Target Profiles, to align cybersecurity outcomes and activities with its overall business/mission objectives for the organization. In the case of Great Seneca Accounting, its Cybersecurity Framework Target Profile helps program owners and system architects understand business and mission-driven priorities and the types of cybersecurity capabilities needed to achieve them. Great Seneca Accounting also used the NIST Interagency Report (NISTIR) 8170, *The Cybersecurity Framework, Implementation Guidance for Federal Agencies* [18], for guidance in using the NIST Cybersecurity Framework.

E.1.2 Overview of the NIST Privacy Framework

Description: The *NIST Privacy Framework* is a voluntary enterprise risk management tool intended to help organizations identify and manage privacy risk and build beneficial products and services while protecting individuals' privacy. It follows the structure of the Cybersecurity Framework to facilitate using both frameworks together [2].

Application: This guide refers to two of the main components of the Privacy Framework: the Framework Core and Framework Profiles. As described in Section 2.1 of the Privacy Framework, the Framework Core provides an increasingly granular set of activities and outcomes that enable dialog about managing privacy risk as well as resources to achieve those outcomes (e.g., guidance in NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* [13]). Section 2.2 of the Privacy Framework identifies Framework Profiles as the selection of specific Functions, Categories, and Subcategories from the core that an organization has prioritized to help it manage privacy risk.

Great Seneca Accounting used the Privacy Framework as a strategic planning tool for its privacy program as well as its system, product, and service teams. The Great Seneca Accounting example scenario assumed that the organization used the Privacy Framework Core and Framework Profiles, specifically Target Profiles, to align privacy outcomes and activities with its overall business/mission objectives for the organization. Its Privacy Framework Target Profile helped program owners and system architects to understand business and mission-driven priorities and the types of privacy capabilities needed to achieve them.

E.1.3 Overview of the NIST Risk Management Framework

Description: The NIST Risk Management Framework (RMF) “provides a process that integrates security and risk management activities into the system development life cycle. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to

applicable laws, directives, Executive Orders, policies, standards, or regulations” [19]. Two of the key documents that describe the RMF are NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*; and NIST SP 800-30, *Guide for Conducting Risk Assessments*.

Application: The RMF has seven steps: Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor. These steps provide a method for organizations to characterize the risk posture of their information and systems and identify controls that are commensurate with the risks in the system’s environment. They also support organizations with selecting beneficial implementation and assessment approaches, reasoning through the process to understand residual risks, and monitoring the efficacy of implemented controls over time.

The Great Seneca Accounting example solution touches on the risk assessment activities conducted under the *Prepare* step, identifying the overall risk level of the BYOD system architecture in the *Categorize* step, and, consistent with example approach 8 in NISTIR 8170, reasoning through the controls that are necessary in the *Select* step. The influence of the priorities provided in Great Seneca Accounting’s Cybersecurity Framework Target Profile is also briefly mentioned regarding making decisions for how to apply controls during *Implement* (e.g., policy versus tools), how robustly to verify and validate controls during *Assess* (e.g., document review versus “hands on the keyboard” system testing), and the degree of evaluation required over time as part of the *Monitor* step.

E.1.4 Overview of the NIST Privacy Risk Assessment Methodology

Description: The NIST Privacy Risk Assessment Methodology (PRAM) is a tool for analyzing, assessing, and prioritizing privacy risks to help organizations determine how to respond and select appropriate solutions. A blank version of the PRAM is available for download on NIST’s website.

Application: The PRAM uses the privacy risk model and privacy engineering objectives described in NISTIR 8062 to analyze for potential problematic data actions. Data actions are any system operations that process data. Processing can include, collection, retention, logging, analysis, generation, transformation or merging, disclosure, transfer, and disposal of data. A problematic data action is one that could cause an adverse effect, or problem, for individuals. The occurrence or potential occurrence of problematic data actions is a privacy event. While there is a growing body of technical privacy controls, including those found in NIST SP 800-53, applying the PRAM may result in identifying controls that are not yet available in common standards. This makes it an especially useful tool for managing risks that may otherwise go unaddressed.

The Great Seneca Accounting example solution assumed that a PRAM was used to identify problematic data actions and mitigating controls for employees. The controls in this build include some technical controls, such as controls that can be handled by security capabilities, as well as policy and procedure-level controls that need to be implemented outside yet supported by the system.

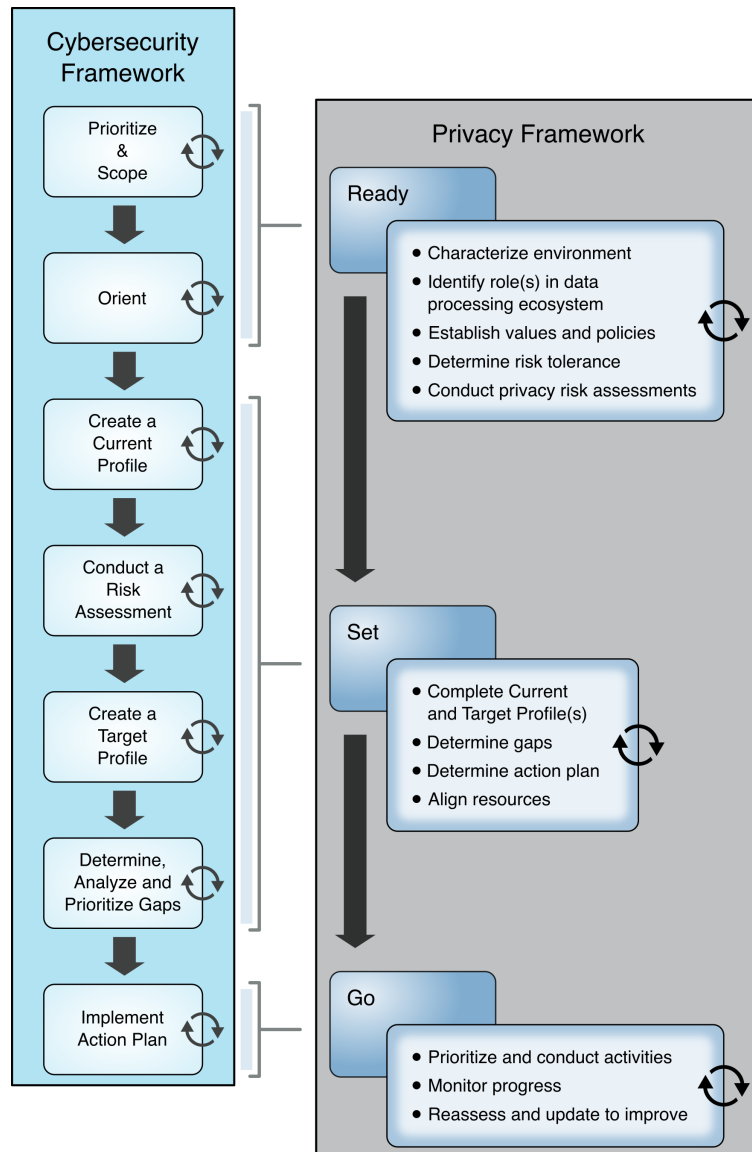
E.2 Using Frameworks to Establish or Improve Cybersecurity and Privacy Programs

While their presentation differs, the NIST Cybersecurity Framework and *NIST Privacy Framework* also both provide complementary guidance for establishing and improving cybersecurity and privacy programs. The NIST Cybersecurity Framework's process for establishing or improving programs provides seven steps that an organization could use iteratively and as necessary throughout the program's life cycle to continually improve its cybersecurity posture:

- Step 1: Prioritize and scope the organization's mission.
- Step 2: Orient its cybersecurity program activities to focus efforts on applicable areas.
- Step 3: Create a current profile of what security areas it currently supports.
- Step 4: Conduct a risk assessment.
- Step 5: Create a Target Profile of the security areas that the organization would like to improve in the future.
- Step 6: Determine, analyze, and prioritize cybersecurity gaps.
- Step 7: Implement an action plan to close those gaps.

The *NIST Privacy Framework* includes the same types of activities for establishing and improving privacy programs, described in a three-stage Ready, Set, Go model. Figure E-1 below shows a comparison of these two approaches, demonstrating their close alignment.

526 **Figure E-1 Comparing Framework Processes to Establish or Improve Programs**



527 Both approaches are equally effective. Regardless of the approach selected, an organization begins with
 528 orienting around its business/mission objectives and high-level organizational priorities and carry out
 529 the remaining activities in a way that makes the most sense for the organization. The organization
 530 repeats these steps as necessary throughout the program's life cycle to continually improve its risk
 531 posture.

Appendix F How Great Seneca Accounting Used the NIST Risk Management Framework

This practice guide contains an example scenario about a fictional organization called Great Seneca Accounting. The example scenario shows how to deploy a Bring Your Own Device (BYOD) solution to be in alignment with an organization's security and privacy capabilities and objectives.

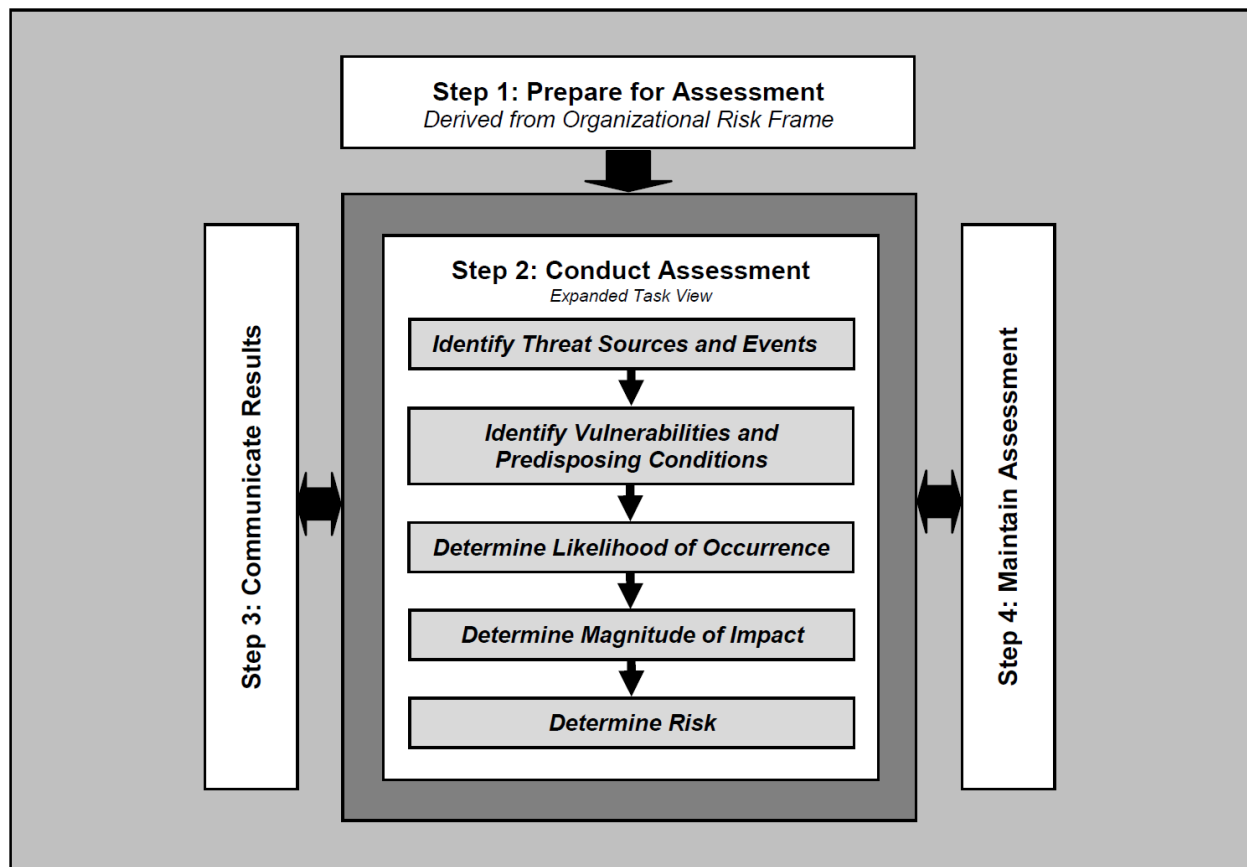
The example scenario uses National Institute of Standards and Technology (NIST) standards, guidance, and tools. It is provided in the *Example Scenario: Putting Guidance into Practice* supplement of this practice guide.

In the example scenario supplement of this practice guide, Great Seneca Accounting decided to use the NIST Cybersecurity Framework, the *NIST Privacy Framework*, and the NIST Risk Management Framework to help improve its mobile device architecture. The following material provides information about how Great Seneca Accounting used the NIST Risk Management Framework to improve its BYOD deployment.

F.1 Understanding the Risk Assessment Process

This section provides information on the risk assessment process employed to improve the mobile security posture of Great Seneca Accounting. Typically, a risk assessment based on NIST SP 800-30 Revision 1 follows a four-step process as shown in [Figure F-1](#): prepare for assessment, conduct assessment, communicate results, and maintain assessment.

549 **Figure F-1 Risk Assessment Process**



550 **F.2 Risk Assessment of Great Seneca Accounting's BYOD Program**

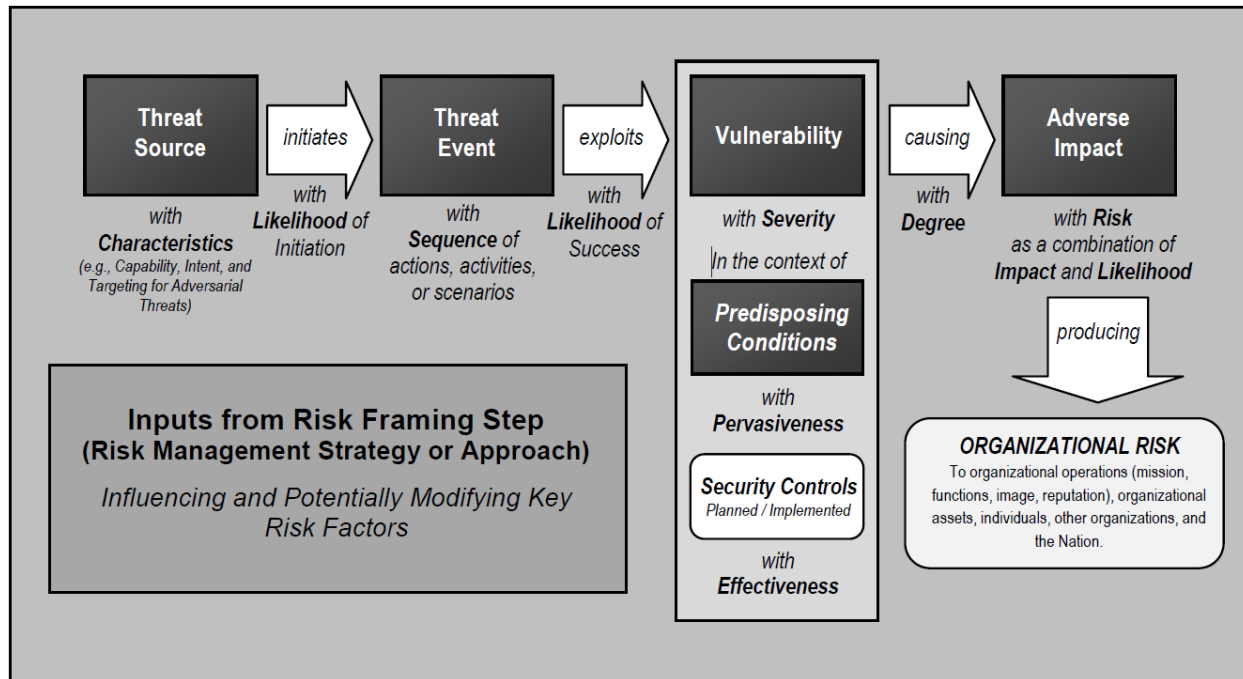
551 This risk assessment is scoped to Great Seneca Accounting's mobile deployment, which includes the
 552 mobile devices used to access Great Seneca Accounting's enterprise resources, along with any
 553 information technology components used to manage or provide services to those mobile devices.

554 Risk assessment assumptions and constraints were developed by using a NIST SP 800-30 Revision 1
 555 generic risk model as shown in [Figure F-2](#) to identify the following components of the risk assessment:

- 556 ▪ threat sources
- 557 ▪ threat events
- 558 ▪ vulnerabilities
- 559 ▪ predisposing conditions
- 560 ▪ security controls

- adverse impacts
- organizational risks

Figure F-2 NIST SP 800-30 Generic Risk Model



F.3 Development of Threat Event Descriptions

Great Seneca Accounting developed threat event tables based on NIST SP 800-30 Revision 1 and used those to help analyze the sources of mobile threats. Using this process, Great Seneca Accounting leadership identified the following potential mobile device threat events that are described in the following subsections.

A note about selection of the threat events:

This practice guide's example solution helps protect organizations from the threat events shown in [Table F-1](#). A mapping of these threat events to the NIST Mobile Threat Catalogue is provided in [Table F-2](#).

572 **Table F-1 Great Seneca Accounting's BYOD Deployment Threats**

Great Seneca Accounting's Threat Event Identification Number	Threat Event Description
TE-1	privacy-intrusive applications
TE-2	account credential theft through phishing
TE-3	malicious applications
TE-4	outdated phones
TE-5	camera and microphone remote access
TE-6	sensitive data transmissions
TE-7	brute-force attacks to unlock a phone
TE-8	protection against weak password practices
TE-9	protection against unmanaged devices
TE-10	protection against lost or stolen data
TE-11	protecting data from being inadvertently backed up to a cloud service
TE-12	protection against sharing personal identification number (PIN) or password

573 Great Seneca Accounting's 12 threat events and their mapping to the NIST Mobile Threat Catalogue [5]
 574 are shown in [Table F-2](#).

575 **Table F-2 Threat Event Mapping to the Mobile Threat Catalogue**

Great Seneca Accounting's Threat Event Identification Number	NIST Mobile Threat Catalogue Threat ID
TE-1	APP-2, APP-12
TE-2	AUT-9
TE-3	APP-2, APP-5, APP-31, APP-40, APP-32, AUT-10
TE-4	APP-4, APP-26, STA-0, STA-9, STA-16
TE-5	APP-32, APP-36

Great Seneca Accounting's Threat Event Identification Number	NIST Mobile Threat Catalogue Threat ID
TE-6	APP-0, CEL-18, LPN-2
TE-7	AUT-2, AUT-4
TE-8	APP-9, AUT-0
TE-9	EMM-5
TE-10	PHY-0
TE-11	EMM-9
TE-12	AUT-0, AUT-2, AUT-4, AUT-5

F.4 Great Seneca Accounting's Leadership and Technical Teams Discuss BYOD's Potential Threats to Their Organization

Great Seneca Accounting's leadership team wanted to understand real-world examples of each threat event and what the risk was for each. Great Seneca Accounting's leadership and technical teams then discussed those possible threats that BYOD could introduce to their organization.

The analysis performed by Great Seneca Accounting's technical team included analyzing the likelihood of each threat, the level of impact, and the threat level that the BYOD deployment would pose. The following are leadership's questions and the technical team's responses regarding BYOD threats during that discussion using real-world examples. A goal of the example solution contained within this practice guide is to mitigate the impact of these threat events. Reference [Table 5-1](#) for a listing of the technology that addresses each of the following threat events.

F.4.1 Threat Event 1

What happens if an employee installs risky applications?

A mobile application can attempt to collect and exfiltrate any information to which it has been granted access. This includes any information generated during use of the application (e.g., user input), user-granted permissions (e.g., contacts, calendar, call logs, photos), and general device data available to any application (e.g., International Mobile Equipment Identity, device make and model, serial number). Further, if a malicious application exploits a vulnerability in other applications, the operating system (OS), or device firmware to achieve privilege escalation, it may gain unauthorized access to any data stored on or otherwise accessible through the device.

Risk assessment analysis:

Overall likelihood: very high

Justification: Employees have access to download any application at any time. If an employee requires an application that provides a desired function, the employee can download that application from any available source (trusted or untrusted) that provides a desired function. If an application performs an employee's desired function, the employee may download an application from an untrusted source and/or disregard granted privacy permissions.

Level of impact: high

Justification: Employees may download an application from an untrusted source and/or disregard granted privacy permissions. This poses a threat for sensitive corporate data, as some applications may include features that could access corporate data, unbeknownst to the user.

BYOD-specific threat: In a BYOD scenario, users are still able to download and install applications at their leisure. This capability allows users to unintentionally side-load or install a malicious application that may harm the device or the enterprise information on the device.

F.4.2 Threat Event 2**Can account information be stolen through phishing?**

Malicious actors may create fraudulent websites that mimic the appearance and behavior of legitimate ones and entice users to authenticate to them by distributing phishing messages over short message service (SMS) or email. Effective social engineering techniques such as impersonating an authority figure or creating a sense of urgency may compel users to forgo scrutinizing the message and proceed to authenticate to the fraudulent website; it then captures and stores the user's credentials before (usually) forwarding them to the legitimate website to allay suspicion.

Risk assessment analysis:

Overall likelihood: very high

Justification: Phishing campaigns are a very common threat that occurs almost every day.

Level of impact: high

Justification: A successful phishing campaign could provide the malicious actor with corporate credentials, allowing access to sensitive corporate data; or personal credentials that could lead to compromise of corporate data or infrastructure via other means.

BYOD-specific threat: The device-level controls applied to personal devices do not inhibit a user's activities. This allows the user to access personal/work messages and emails on their device that could

be susceptible to phishing attempts. If the proper controls are not applied to a user's enterprise messages and email, successful phishing attempts could allow an attacker unauthorized access to enterprise data.

F.4.3 Threat Event 3

How much risk do malicious applications pose to Great Seneca Accounting?

Malicious actors may send users SMS or email messages that contain a uniform resource locator (URL) where a malicious application is hosted. Generally, such messages are crafted using social engineering techniques designed to dissuade recipients from scrutinizing the nature of the message, thereby increasing the likelihood that they access the URL using their mobile device. If they do, it will attempt to download and install the application. Effective use of social engineering by the attacker will further compel an otherwise suspicious user to grant any trust required by the developer and all permissions requested by the application. Granting the former facilitates installation of other malicious applications by the same developer, and granting the latter increases the potential for the application to do direct harm.

Risk assessment analysis:

Overall likelihood: high

Justification: Installation of malicious applications via URLs is less common than other phishing attempts. The process for side-loading applications requires much more user input and consideration (e.g., trusting the developer certificate) than standard phishing, which solely requests a username and password. A user may proceed through sideloading an application to acquire a desired capability from an application.

Level of impact: high

Justification: Once a user installs a malicious side-loaded application, an adversary could gain full access to a mobile device, and therefore access to corporate data and credentials, without the user's knowledge.

BYOD-specific threat: Like Threat Event 1, BYOD deployments may have fewer restrictions to avoid preventing the user from performing desired personal functions. This increases the attack surface for malicious actors to take advantage.

F.4.4 Threat Event 4

What happens when outdated phones access Great Seneca Accounting's network?

When malware successfully exploits a code execution vulnerability in the mobile OS or device drivers, the delivered code generally executes with elevated privileges and issues commands in the context of

the root user or the OS kernel. This may be enough for some malicious actors to accomplish their goal, but those that are advanced will usually attempt to install additional malicious tools and to establish a persistent presence. If successful, the attacker will be able to launch further attacks against the user, the device, or any other systems to which the device connects. As a result, any data stored on, generated by, or accessible to the device at that time – or in the future – may be compromised.

Risk assessment analysis:

Overall likelihood: high

Justification: Many public vulnerabilities specific to mobile devices have been seen over the years. In these, users can jailbreak iOS devices and root Android devices to download third-party applications and apply unique settings/configurations that the device would not typically be able to apply/access.

Level of impact: high

Justification: Exploiting a vulnerability allows circumventing security controls and modifying protected device data that should not be modified. Jailbroken and rooted devices exploit kernel vulnerabilities and allow third-party applications/services root access that can also be used to bypass security controls that are built in or applied to a mobile device.

BYOD-specific threat: As with any device, personal devices are susceptible to device exploitation if not properly used or updated.

F.4.5 Threat Event 5

Can Great Seneca Accounting stop someone from turning on a camera or microphone?

Malicious actors with access (authorized or unauthorized) to device sensors (microphone, camera, gyroscope, Global Positioning System receiver, and radios) can use them to conduct surveillance. It may be directed at the user, as when tracking the device location, or it may be applied more generally, as when recording any nearby sounds. Captured sensor data may be immediately useful to a malicious actor, such as a recording of an executive meeting. Alternatively, the attacker may analyze the data in isolation or in combination with other data to yield sensitive information. For example, a malicious actor can use audio recordings of on-device or proximate activity to probabilistically determine user inputs to touchscreens and keyboards, essentially turning the device into a remote keylogger.

Risk assessment analysis:

Overall likelihood: very high

Justification: This has been seen on public application stores, with applications allegedly being used for data-collection. As mentioned in Threat Event 1, unbeknownst to the user, a downloaded application may be granted privacy intrusive permissions that allow access to device sensors.

691 Level of impact: high

692 *Justification:* When the sensors are being misused, the user is typically not alerted. This allows collection
693 of sensitive enterprise data, such as location, without knowledge of the user.

694 **BYOD-specific threat:** Applications commonly request access to these sensors. In a BYOD deployment,
695 the enterprise does not have control over what personal applications the user installs on their device.
696 These personal applications may access sensors on the device and eavesdrop on a user's enterprise-
697 related activities (e.g., calls and meetings).

698 F.4.6 Threat Event 6

699 **Is sensitive information protected when the data travels between the employee's mobile device and**
700 **Great Seneca Accounting's network?**

701 Malicious actors can readily eavesdrop on communication over unencrypted, wireless networks such as
702 public Wi-Fi access points, which coffee shops and hotels commonly provide. While a device is
703 connected to such a network, a malicious actor could gain unauthorized access to any data sent or
704 received by the device for any session that has not already been protected by encryption at either the
705 transport or application layers. Even if the transmitted data were encrypted, an attacker would be privy
706 to the domains, internet protocol (IP) addresses, and services (as indicated by port numbers) to which
707 the device connects; an attacker could use such information in future watering hole or person-in-the-
708 middle attacks against the device user.

709 Additionally, visibility into network-layer traffic enables a malicious actor to conduct side-channel
710 attacks against the network's encrypted messages, which can still result in a loss of confidentiality.
711 Further, eavesdropping on unencrypted messages during a handshake to establish an encrypted session
712 with another host or endpoint may facilitate attacks that ultimately compromise the security of the
713 session.

714 **Risk assessment analysis:**

715 Overall likelihood: moderate

716 *Justification:* Unlike installation of an application, installations of enterprise mobility management
717 (EMM)/mobile device management (MDM), network, virtual private network (VPN) profiles, and
718 certificates require additional effort and understanding from the user to properly implement.

719 Level of impact: very high

720 *Justification:* If malicious actor can install malicious configuration profiles or certificates, they would be
721 able to perform actions such as decrypting network traffic and possibly even control the device.

BYOD-specific threat: Like Threat Event 2, personal devices may not have the benefit of an always-on device-wide VPN. This leaves application communications at the discretion of the developer.

F.4.7 Threat Event 7

Is Great Seneca Accounting's data protected from brute-force PIN attacks?

A malicious actor may be able to obtain a user's device unlock code by direct observation, side-channel attacks, or brute-force attacks. Both the first and second can be attempted with at least proximity to the device; only the third technique requires physical access. However, applications with access to any peripherals that detect sound or motion (microphone, gyroscope, or accelerometer) can attempt side-channel attacks that infer the unlock code by detecting taps and swipes to the screen. Once the device unlock code has been obtained, a malicious actor with physical access to the device will gain immediate access to any data or functionality not already protected by additional access control mechanisms. Additionally, if the user employs the device unlock code as a credential to any other systems, the malicious actor may further gain unauthorized access to those systems.

Risk assessment analysis:

Overall likelihood: moderate

Justification: Unlike shoulder-surfing to observe a user's passcode, brute-force attacks are not as common or successful due to the built-in deterrent mechanisms. These mechanisms include exponential back-off/lockout period and device wipes after a certain number of failed unlock attempts.

Level of impact: very high

Justification: If a malicious actor can successfully unlock a device without the user's permission, they could have full control over the user's corporate account and thus gain unauthorized access to corporate data.

BYOD-specific threat: Because BYODs are prone to travel (e.g., vacations, restaurants, and other nonwork locations), the risk that the device's passcode is obtained increases due to the heightened exposure to threats in different environments.

F.4.8 Threat Event 8

Can Great Seneca Accounting protect its data from weak password practices?

If a malicious actor gains unauthorized access to a mobile device, they also have access to the data and applications on that mobile device. The mobile device may contain an organization's in-house applications that a malicious actor can subsequently use to gain access to sensitive data or backend services. This could result from weaknesses or vulnerabilities present in the authentication or credential storage mechanisms implemented within an in-house application.

754 **Risk assessment analysis:**

755 Overall likelihood: moderate

756 *Justification:* Often applications include hardcoded credentials for the default password of the admin
 757 account. Default passwords are readily available online. The user might not change these passwords to
 758 allow access and eliminate the need to remember a password.

759 Level of impact: high

760 *Justification:* Successful extraction of the credentials allows an attacker to gain unauthorized access to
 761 enterprise data.

762 **BYOD-specific threat:** The risk of hardcoded credentials residing in an application on the device is the
 763 same for any mobile device deployment scenario.

764 **F.4.9 Threat Event 9**

765 **Can unmanaged devices connect to Great Seneca Accounting?**

766 An employee who accesses enterprise resources from an unmanaged mobile device may expose the
 767 enterprise to vulnerabilities that may compromise enterprise data. Unmanaged devices do not benefit
 768 from any security mechanisms deployed by the organization such as mobile threat defense, mobile
 769 threat intelligence, application vetting services, and mobile security policies. These unmanaged devices
 770 limit an organization's visibility into the state of a mobile device, including if a malicious actor
 771 compromises the device. Therefore, users who violate security policies to gain unauthorized access to
 772 enterprise resources from such devices risk providing malicious actors with access to sensitive
 773 organizational data, services, and systems.

774 **Risk assessment analysis:**

775 Overall likelihood: very high

776 *Justification:* This may occur accidentally when an employee attempts to access their email or other
 777 corporate resources.

778 Level of impact: high

779 *Justification:* Unmanaged devices pose a sizable security risk because the enterprise has no visibility into
 780 their security or risk postures of the mobile devices. Due to this lack of visibility, a compromised device
 781 may allow an attacker to attempt to exfiltrate sensitive enterprise data.

782 **BYOD-specific threat:** The risk of an unmanaged mobile device accessing the enterprise is the same for
 783 any mobile deployment scenario.

F.4.10 Threat Event 10

Can Great Seneca Accounting protect its data when a phone is lost or stolen?

Due to the nature of the small form factor of mobile devices, they can be misplaced or stolen. A malicious actor who gains physical custody of a device with inadequate security controls may be able to gain unauthorized access to sensitive data or resources accessible to the device.

Risk assessment analysis:

Overall likelihood: very high

Justification: Mobile devices are small and can be misplaced. Enterprise devices may be lost or stolen at the same frequency as personally owned devices.

Level of impact: high

Justification: Similar to Threat Event 9, if a malicious actor can gain access to the device, they could access sensitive corporate data.

BYOD-specific threat: Due to the heightened mobility of BYODs, they are more prone to being accidentally lost or stolen.

F.4.11 Threat Event 11

Can data be protected from unauthorized cloud services?

If employees violate data management policies by using unmanaged services to store sensitive organizational data, the data will be placed outside organizational control, where the organization can no longer protect its confidentiality, integrity, or availability. Malicious actors who compromise the unauthorized service account or any system hosting that account may gain unauthorized access to the data.

Further, storage of sensitive data in an unmanaged service may subject the user or the organization to prosecution for violation of any applicable laws (e.g., exportation of encryption) and may complicate efforts by the organization to achieve remediation or recovery from any future losses, such as those resulting from public disclosure of trade secrets.

Risk assessment analysis:

Overall likelihood: high

Justification: This could occur either intentionally or accidentally (e.g., taking a screenshot and having pictures backed up to an unmanaged cloud service).

Level of impact: high

Justification: Storage in unmanaged services presents a risk to the confidentiality and availability of corporate data because the corporation would no longer control it.

BYOD-specific threat: In a BYOD deployment, employees are more likely to have some backup or automated cloud storage solution configured on their device, which may lead to unintentional backup of enterprise data.

F.4.12 Threat Level 12

Can Great Seneca Accounting protect its data from PIN or password sharing?

Many individuals choose to share the PIN or password to unlock their personal device with family members. This creates a scenario where a nonemployee can access the device, the work applications, and therefore the work data.

Risk assessment analysis:

Overall likelihood: moderate

Justification: Even though employees are conditioned almost constantly to protect their work passwords, personal device PINs and passwords are not always protected with that same level of security. Anytime individuals share a password or PIN, there is increased risk that it might be exposed or compromised.

Level of impact: very high

Justification: If a malicious actor can bypass a device lock and gain access to the device, they can potentially access sensitive corporate data.

BYOD-specific threat: The passcode of an individual's personal mobile device is more likely to be shared among family and/or friends to provide access to applications (e.g., games). Although sharing passcodes may be convenient for personal reasons, this increases the risk of an unauthorized individual gaining access to enterprise data through a personal device.

F.5 Identification of Vulnerabilities and Predisposing Conditions

In this section we identify vulnerabilities and predisposing conditions that increase the likelihood that identified threat events will result in adverse impacts for Great Seneca Accounting. We list each vulnerability or predisposing condition in [Table F-3](#), along with the corresponding threat events and ratings of threat pervasiveness. More details on threat event ratings can be found in [Appendix Section F.3](#).

843 **Table F-3 Identify Vulnerabilities and Predisposing Conditions**

Vulnerability ID	Vulnerability or Predisposing Condition	Resulting Threat Events	Pervasiveness
VULN-1	Email and other enterprise resources can be accessed from anywhere, and only username/password authentication is required.	TE-2, TE-9, TE-10	very high
VULN-2	Public Wi-Fi networks are regularly used by employees for remote connectivity from their mobile devices.	TE-6	very high
VULN-3	No EMM/MDM deployment exists to enforce and monitor compliance with security-relevant policies on mobile devices.	TE-1, TE-3, TE-4, TE-5, TE-6, TE-7, TE-8, TE-9, TE-10, TE-11, TE-12	very high

844 **F.6 Summary of Risk Assessment Findings**

845 [Table F-4](#) summarizes the risk assessment findings. More detail about the methodology used to rate
 846 overall likelihood, level of impact, and risk is in the Appendix Section [F.3](#).

847 **Table F-4 Summary of Risk Assessment Findings**

Threat Event	Vulnerabilities, Predisposing Conditions	Overall Likelihood	Level of Impact	Risk
TE-1: unauthorized access to sensitive information via a malicious or privacy-intrusive application	VULN-3	very high	high	high
TE-2: theft of credentials through an SMS or email phishing campaign	VULN-1	very high	high	high
TE-3: malicious applications installed via URLs in SMS or email messages	VULN-3	high	high	high

Threat Event	Vulnerabilities, Predisposing Conditions	Overall Likelihood	Level of Impact	Risk
TE-4: confidentiality and integrity loss due to exploitation of known vulnerability in the OS or firmware	VULN-3	high	high	high
TE-5: violation of privacy via misuse of device sensors	VULN-3	very high	high	high
TE-6: loss of confidentiality of sensitive information via eavesdropping on unencrypted device communications	VULN-2, VULN-3	moderate	very high	high
TE-7: compromise of device integrity via observed, inferred, or brute-forced device unlock code	VULN-3	moderate	very high	high
TE-8: unauthorized access to backend services via authentication or credential storage vulnerabilities in internally developed applications	VULN-3	moderate	high	high
TE-9: unauthorized access of enterprise resources from an unmanaged and potentially compromised device	VULN-1, VULN-3	very high	high	high
TE-10: loss of organizational data due to a lost or stolen device	VULN-1, VULN-3	very high	high	high
TE-11: loss of confidentiality of organizational data due to its unauthorized storage in non-organizationally managed services	VULN-3	high	high	high
TE-12: unauthorized access to work applications via bypassed lock screen	VULN-3	moderate	very high	high

848 **Note 1:** Risk is stated in qualitative terms based on the scale in Table I-2 of Appendix I in NIST SP 800-30
849 Revision 1 [8].

850 **Note 2:** The risk rating is derived from both the overall likelihood and level of impact using Table I-2 of
851 Appendix I in NIST SP 800-30 Revision 1 [8]. Because these are modified interval scales, the combined
852 overall risk ratings from Table I-2 do not always reflect a strict mathematical average of these two
853 variables. The table above demonstrates this where levels of moderate weigh more heavily than other
854 ratings.

855 **Note 3:** Ratings of risk relate to the probability and level of adverse effect on organizational operations,
856 organizational assets, individuals, other organizations, or the nation. Per NIST SP 800-30 Revision 1,
857 adverse effects (and the associated risks) range from negligible (i.e., very low risk), limited (i.e., low),
858 serious (i.e., moderate), severe or catastrophic (i.e., high), to multiple severe or catastrophic (i.e., very
859 high).

Appendix G How Great Seneca Accounting Used the NIST Privacy Risk Assessment Methodology

This practice guide contains an example scenario about a fictional organization called Great Seneca Accounting. The example scenario shows how to deploy a Bring Your Own Device (BYOD) solution to be in alignment with an organization's security and privacy capabilities and objectives.

The example scenario uses National Institute of Standards and Technology (NIST) standards, guidance, and tools. It is provided in the *Example Scenario: Putting Guidance into Practice* supplement of this practice guide.

In the example scenario, Great Seneca Accounting decided to use the NIST Privacy Risk Assessment Methodology (PRAM) to conduct a privacy risk assessment and help improve the company's mobile device architecture. The PRAM helps an organization analyze and communicate about how it conducted its data processing to achieve business/mission objectives.

At Great Seneca Accounting, the PRAM helped elucidate how enabling employees to use their personal devices for work-related functions can present privacy concerns for individuals. The PRAM also supports the risk assessment task in the Prepare step of the NIST Risk Management Framework as discussed in Appendix section E.1. The privacy events that were identified are below, along with potential mitigations.

G.1 Problematic Data Action 1: Unwarranted restriction through blocking access and wiping devices

Data Action: Devices can be wiped and reset to factory settings based on inputs regarding anomalous activity and untrusted applications.

Potential Problem for Individuals: In a BYOD environment, employees are likely to use their devices for both personal and work-related purposes; thus, in a system that features robust security information and event management capable of wiping a device entirely, there could be an issue of employees losing personal data and employees may not even expect that this is a possibility. A hypothetical example is that a Great Seneca Accounting employee stores personal photos on their mobile device, but these photos are lost when their device is wiped after anomalous activity is detected.

Mitigations:

Block access to corporate resources by removing device from mobile device management (MDM) control instead of wiping devices.

As an alternative to wiping data entirely, section F.4.3, Threat Event 3, discusses blocking a device from accessing enterprise resources until an application is removed. Temporarily blocking access ensures that

an individual will not lose personal data through a full wipe of a device. This approach may help bring the system's capabilities into alignment with employees' expectations about what can happen to their devices, especially if they are unaware that devices can be wiped by administrators—providing greater predictability in the system.

Related mitigation: If this mitigation approach is taken, the organization may also wish to consider establishing and communicating these remediation processes to employees. It is important to have a clear remediation process in place to help employees regain access to resources on their devices at the appropriate time. It is also important to clearly convey this remediation process to employees. A remediation process provides greater manageability in the system supporting employees' ability to access resources. If well communicated to employees, this also provides greater predictability as employees will know the steps to regain access.

Enable only selective wiping of corporate resources on the device.

An alternative mitigation option for wiping device data is to limit what can be wiped. International Business Machines' (IBM's) MaaS360 can be configured to selectively wipe instead of performing a full factory reset. When configured this way, a wipe preserves employees' personal configurations, applications, and data while removing only the corporate configurations, applications, and data. However, on Android, a selective wipe will preserve restrictions imposed via policy on the device. To fully remove MDM control, the Remove Work Profile action must be used.

Advise employees to back up the personal data maintained on devices.

If device wiping remains an option for administrators, encourage employees to perform regular backups of their personal data to ensure it remains accessible in case of a wipe.

Restrict staff access to system capabilities that permit removing device access or performing wipes.

Limit staff with the ability to perform a wipe to only those with that responsibility by using role-based access controls. This can help decrease the chances of accidentally removing employee data or blocking access to resources.

G.2 Problematic Data Action 2: Employee surveillance

Data Action: The assessed infrastructure offers Great Seneca Accounting and its employees a number of security capabilities, including reliance on comprehensive monitoring capabilities, as noted in Section 4, Architecture. Multiple parties could collect and analyze a significant amount of data relating to employees, their devices, and their activities.

Potential Problem for Individuals: Employees may not be aware that the organization has the ability to monitor their interactions with the system and may not want this monitoring to occur. Collection and analysis of information might enable Great Seneca Accounting or other parties to craft a narrative about

an employee based on the employee's interactions with the system, which could lead to a power imbalance between Great Seneca Accounting and the employee and loss of trust in the employer if the employee discovers monitoring that they did not anticipate.

Mitigations:

Restrict staff access to system capabilities that permit reviewing data about employees and their devices.

This may be achieved using role-based access controls. Access can be limited to any dashboard in the system containing data about employees and their devices but is most sensitive for the MaaS360 dashboard, which is the hub for data about employees, their devices, and threats. Minimizing access to sensitive information can enhance disassociability for employees using the system.

Limit or disable collection of specific data elements.

Conduct a system-specific privacy risk assessment to determine what elements can be limited. In the configuration of MaaS360, location services and application inventory collection may be disabled. iOS devices can be configured in MaaS360 to collect only an inventory of applications that have been installed through the corporate application store instead of all applications installed on the device.

While these administrative configurations may help provide disassociability in the system, there are also some opportunities for employees to limit the data collected. Employees can choose to disable location services in their device OS to prevent collection of location data. MaaS360 can also be configured to provide employees with the ability to manage their own devices through the IBM User Portal.

Each of these controls contributes to limiting the number of attributes regarding employees and their devices that is collected, which can impede administrators' ability to associate information with specific individuals.

Dispose of personally identifiable information (PII).

Disposing of PII after an appropriate retention period can help reduce the risk of entities building profiles of individuals. Disposal can also help bring the system's data processing into alignment with employees' expectations and reduce the security risk associated with storing a large volume of PII. Disposal may be particularly important for certain parties in the system that collect a larger volume of data or more sensitive data. Disposal may be achieved using a combination of policy and technical controls. Parties in the system may identify what happens to data, when, and how frequently.

G.3 Problematic Data Action 3: Unanticipated revelations through data sharing across parties

Data Action: The infrastructure involves several parties that serve different purposes supporting Great Seneca Accounting’s security objectives. As a result, device usage information could flow across various parties.

Potential Problems for Individuals: This transmission among a variety of different parties could be confusing for employees who might not know who has access to information about them. If administrators and co-workers know which colleagues are conducting activity on their device that triggers security alerts, employees could be embarrassed by its disclosure. Information being revealed and associated with specific employees could also lead to stigmatization and even impact Great Seneca Accounting upper management in its decision-making regarding the employee. Further, clear text transmissions could leave information vulnerable to attackers and therefore to unanticipated release of employee information.

Mitigations:

De-identify personal and device data when such data is not necessary to meet processing objectives.

De-identifying data helps decrease the chances that a third party is aggregating information pertaining to one individual. While de-identification can help reduce privacy risk, there are residual risks of re-identification.

Encrypt data transmitted between parties.

Encryption reduces the risk of compromise of information transmitted between parties. MaaS360 encrypts all communications over the internet with Transport Layer Security.

Limit or disable access to data.

Conduct a system-specific privacy risk assessment to determine how access to data can be limited. Using access controls to limit staff access to compliance information, especially when associated with individuals, can be important in preventing association of specific events with particular employees.

Limit or disable collection of specific data elements.

Conduct a system-specific privacy risk assessment to determine what elements can be limited. MaaS360 can be configured to limit collection of application and location data. Further, instead of collecting a list of all the applications installed on the device, MaaS360 can collect only the list of those applications that were installed through the corporate application store (called “managed applications”). This would prevent insight into the employees’ applications that employees downloaded for personal use. Zimperium provides privacy policies that can be configured to collect or not collect data items when certain events occur.

990 **Use contracts to limit third-party data processing.**

991 Establish contractual policies to limit data processing by third parties to only the processing that
992 facilitates delivery of security services and to no data processing beyond those explicit purposes.

993 **G.4 Mitigations Applicable Across Various Data Actions**

994 Several mitigations benefit employees in all three data actions identified in the privacy risk assessment.
995 The following training and support mitigations can help Great Seneca Accounting appropriately inform
996 employees about the system and its data processing.

997 **Mitigations:**

998 **Train employees about the system, parties involved, data processing, and actions that administrators**
999 **can take.**

1000 Training sessions can also highlight any privacy-preserving techniques used, such as for disclosures to
1001 third parties. Training should include confirmation from employees that they understand the actions
1002 that administrators can take on their devices and their consequences—whether this is blocking access or
1003 wiping data. Employees may also be informed of data retention periods and when their data will be
1004 deleted. This can be more effective than sharing a privacy notice, which research has shown, individuals
1005 are unlikely to read. Still, MaaS360 should also be configured to provide employees with access to a
1006 visual privacy policy, which describes what device information is collected and why, as well as what
1007 actions administrators can take on the device. This enables employees to make better informed
1008 decisions while using their devices, and it enhances predictability.

1009 **Provide ongoing notifications or reminders about system activity.**

1010 This can be achieved using notifications to help directly link administrative actions on devices to relevant
1011 threats and to also help employees understand why an action is being taken. MaaS360 also notifies
1012 employees when changes are made to the privacy policy or MDM profile settings. These notifications
1013 can help increase system predictability by setting employee expectations appropriately regarding the
1014 way the system processes data and the resulting actions.

1015 **Provide a support point of contact.**

1016 By providing employees with a point of contact in the organization who can respond to inquiries and
1017 concerns regarding the system, employees can better understand how the system processes their data,
1018 which enhances predictability.

1019 **G.5 Privacy References for Example Solution Technologies**

1020 Additional privacy information on the example solution's technologies appears below.

1021 Table G-1 Privacy References for the Example Solution Technologies

Commercially Available Product	Mobile Security Technology	Product Privacy Information Location
<p>IBM MaaS360 Mobile Device Management (SaaS) Version 10.73</p> <p>IBM MaaS360 Mobile Device Management Agent Version 3.91.5 (iOS), 6.60 (Android)</p> <p>IBM MaaS360 Cloud Extender / Cloud Extender Modules</p>	mobile device management	<p>https://www.ibm.com/support/pages/node/1093156?mhsrc=ibm-search_a&mhq=maas360%20privacy</p> <p>https://www.ibm.com/support/pages/node/571227</p> <p>https://www.ibm.com/support/knowledge-center/SS8H2S/com.ibm.mc.doc/pag_source/tasks/pag_sec_privacy.htm</p> <p>http://public.dhe.ibm.com/software/security/products/maas360/GDPR/</p>
Kryptowire Cloud Service	application vetting	https://www.kryptowire.com
<p>Palo Alto Networks PA-VM-100 Version 9.0.1</p> <p>Palo Alto Networks GlobalProtect VPN Client Version 5.0.6-14 (iOS), 5.0.2-6 (Android)</p>	virtual private network (VPN) and firewall/filtering	<p>https://docs.paloaltonetworks.com/globalprotect/8-0/globalprotect-admin/host-information/about-host-information/what-data-does-the-globalprotect-agent-collect#</p> <p>https://www.paloaltonetworks.com/resources/datasheets/url-filtering-privacy-datasheet</p>
Qualcomm (Version is mobile device dependent)	trusted execution environment	https://www.qualcomm.com/media/documents/files/guard-your-data-with-the-qualcomm-snapdragon-mobile-platform.pdf
<p>Zimperium Defense Suite</p> <p>Zimperium Console Version vGA-4.23.1</p> <p>Zimperium zIPS Agent Version 4.9.2 (Android and iOS)</p>	mobile threat defense	https://www.zimperium.com/mobile-app-protection