Example Audit Presentation

REPUBLIC BANK

Presented by: Crystal Burton

OBJECTIVE

- TO VERIFY AND ASSESS ALL SECURITY MEASURES

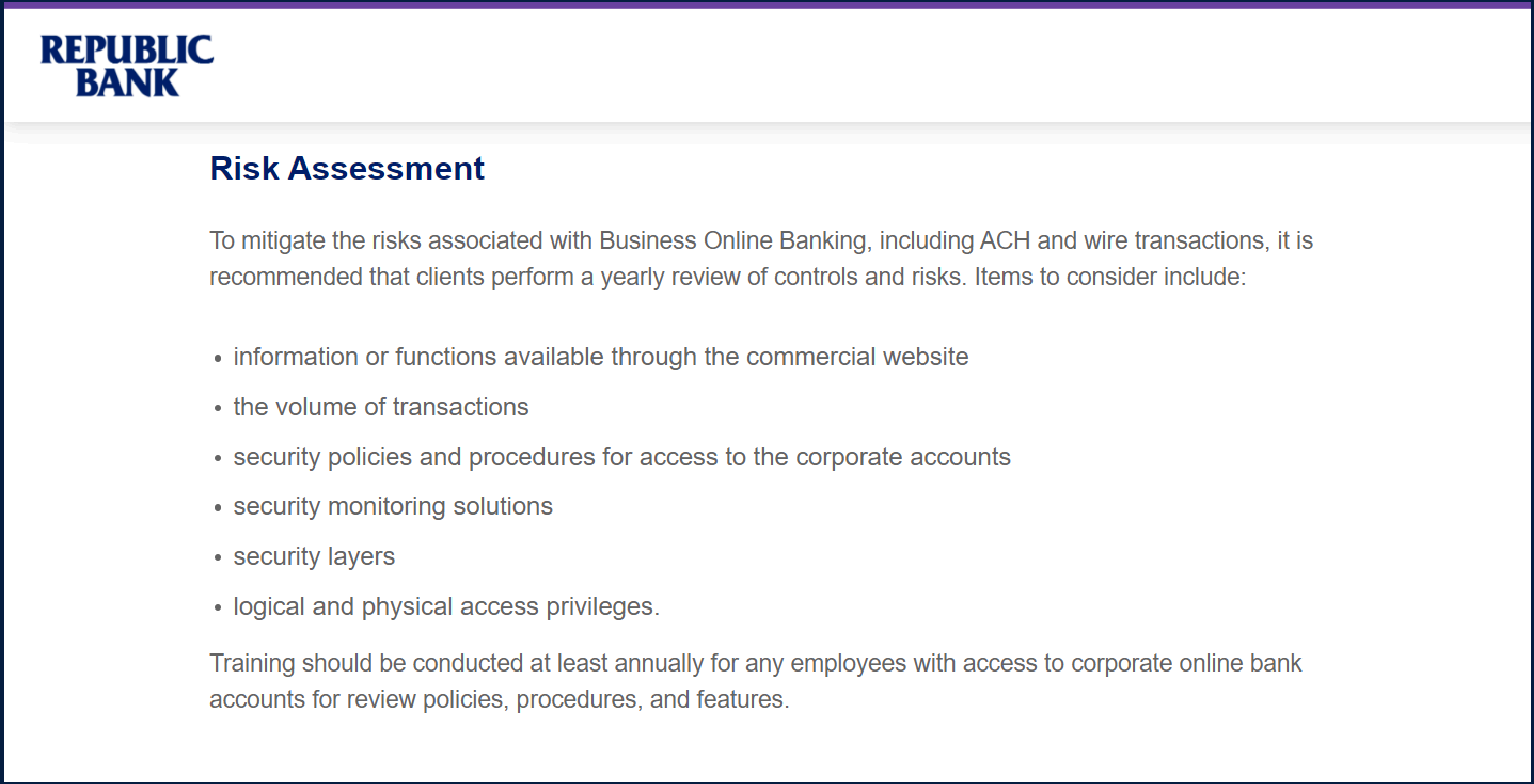
- TO CONFIRM THAT SECURITY MEASURES ARE IN ALIGNMENT WITH THE PCI DSS FRAMEWORK

PCI DSS IS THE PAYMENT CARD INDUSTRY DATA SECURTY STANDARD

THIS FRAMEWORK SHOULD BE IMPLEMENTED BY ANY BUSINESS THAT:

- STORES
- PROCESSES
- TRANSMITS

CARDHOLDER DATA



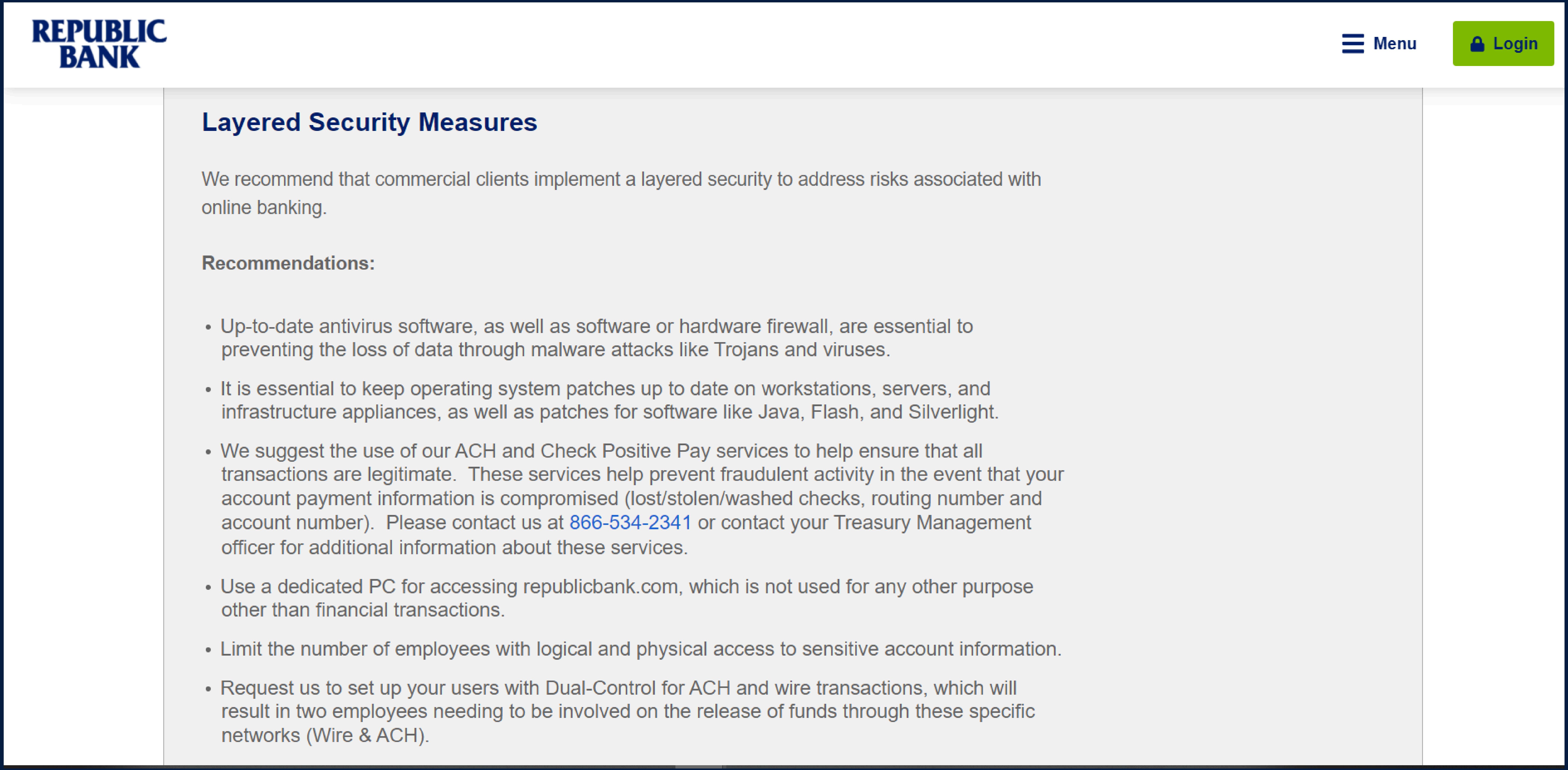
REPUBLIC BANK

Risk Assessment

To mitigate the risks associated with Business Online Banking, including ACH and wire transactions, it is recommended that clients perform a yearly review of controls and risks. Items to consider include:

- information or functions available through the commercial website
- the volume of transactions
- security policies and procedures for access to the corporate accounts
- security monitoring solutions
- security layers
- logical and physical access privileges.

Training should be conducted at least annually for any employees with access to corporate online bank accounts for review policies, procedures, and features.



Layered Security Measures

We recommend that commercial clients implement a layered security to address risks associated with online banking.

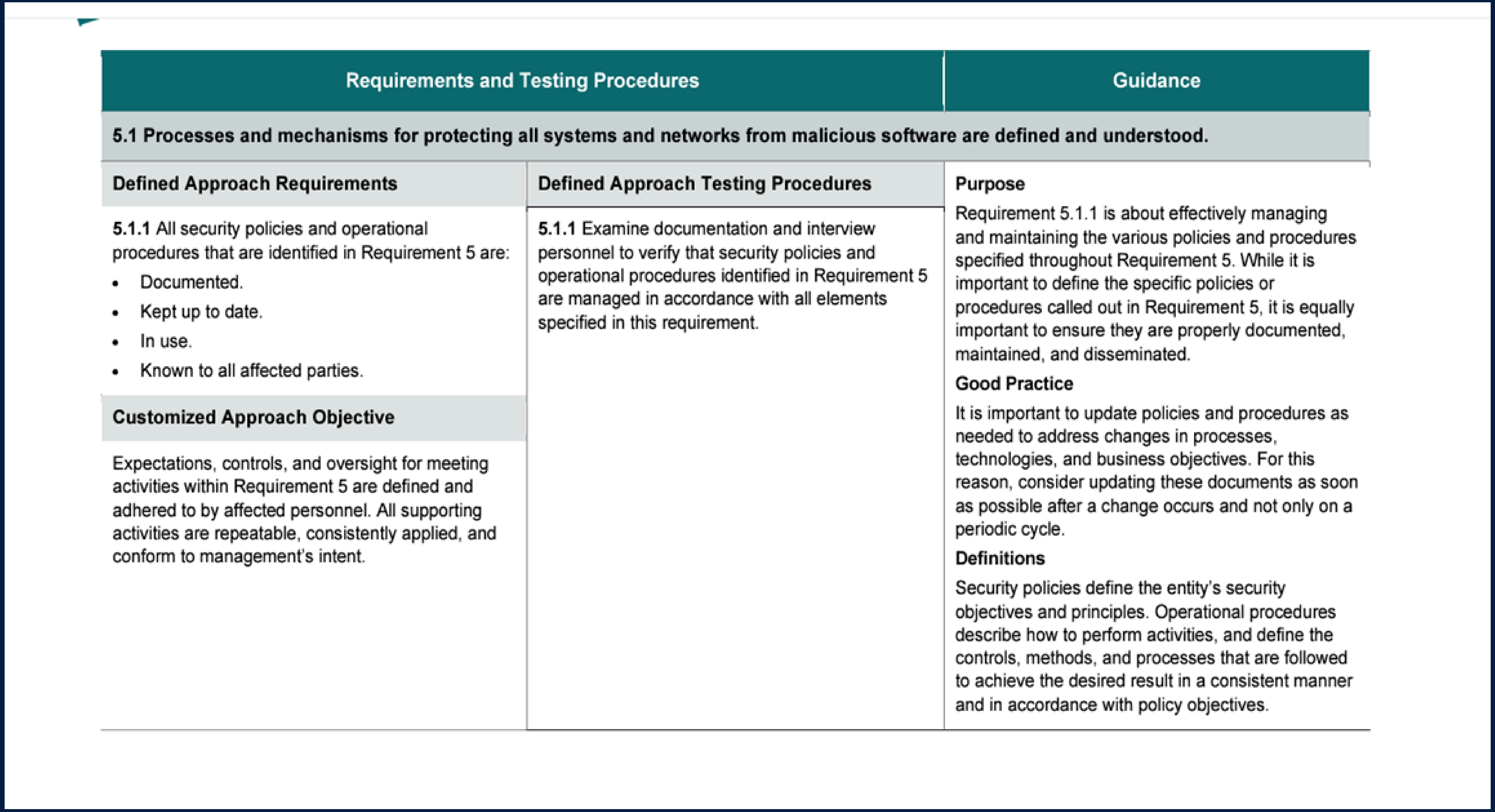
Recommendations:

- Up-to-date antivirus software, as well as software or hardware firewall, are essential to preventing the loss of data through malware attacks like Trojans and viruses.
- It is essential to keep operating system patches up to date on workstations, servers, and infrastructure appliances, as well as patches for software like Java, Flash, and Silverlight.
- We suggest the use of our ACH and Check Positive Pay services to help ensure that all transactions are legitimate. These services help prevent fraudulent activity in the event that your account payment information is compromised (lost/stolen/washed checks, routing number and account number). Please contact us at 866-534-2341 or contact your Treasury Management officer for additional information about these services.
- Use a dedicated PC for accessing republicbank.com, which is not used for any other purpose other than financial transactions.
- Limit the number of employees with logical and physical access to sensitive account information.
- Request us to set up your users with Dual-Control for ACH and wire transactions, which will result in two employees needing to be involved on the release of funds through these specific networks (Wire & ACH).

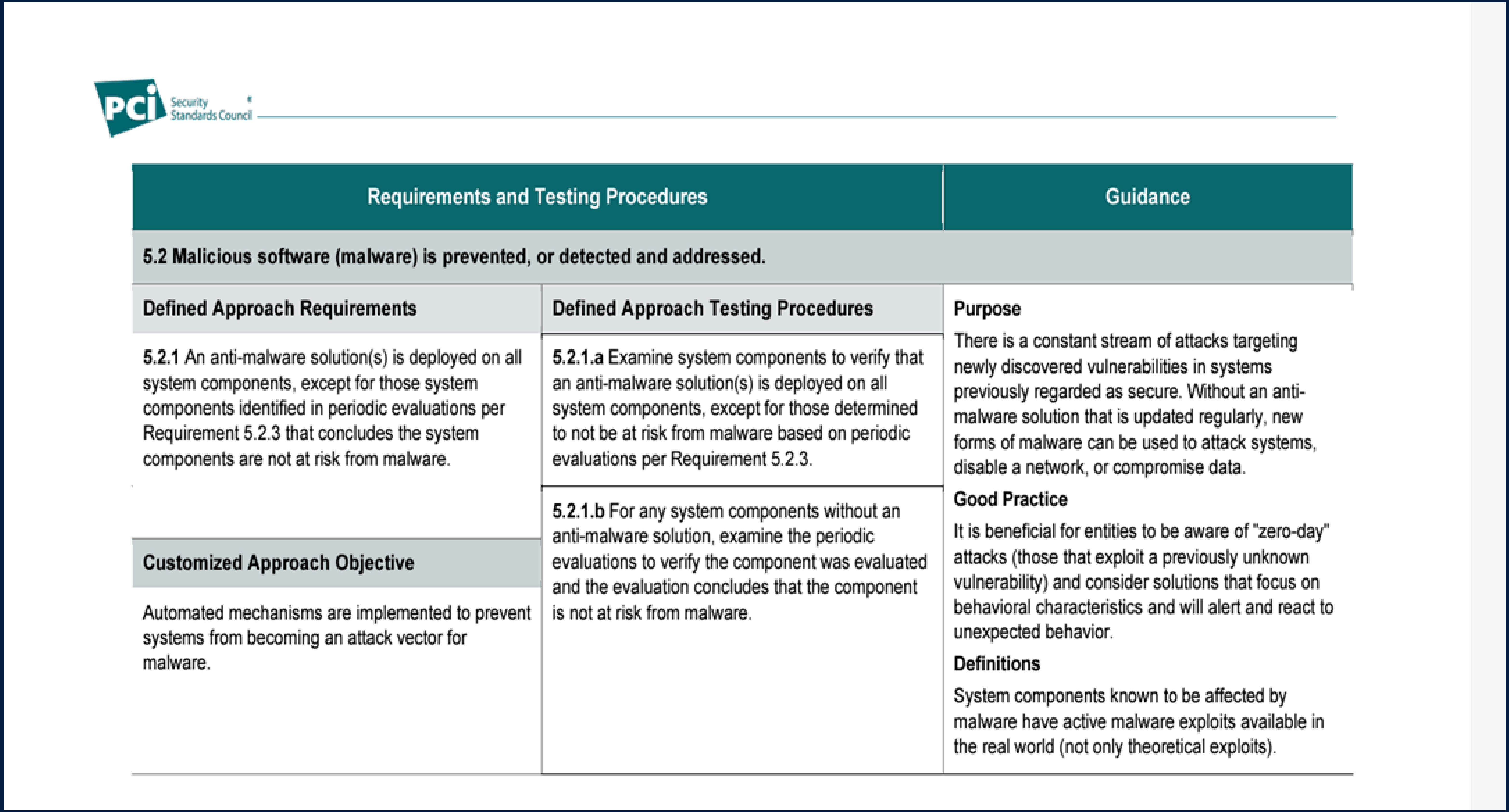
BASED ON
RISK ASSESSMENT RECOMMENDATIONS
BY THE
FINANCIAL INSTITUTION...

- UP-TO-DATE ANTIVIRUS SOFTWARE, AS WELL AS SOFTWARE OR HARDWARE FIREWALL, ARE ESSENTIAL TO PREVENTING THE LOSS OF DATA THROUGH MALWARE ATTACKS LIKE TROJANS AND VIRUSES.

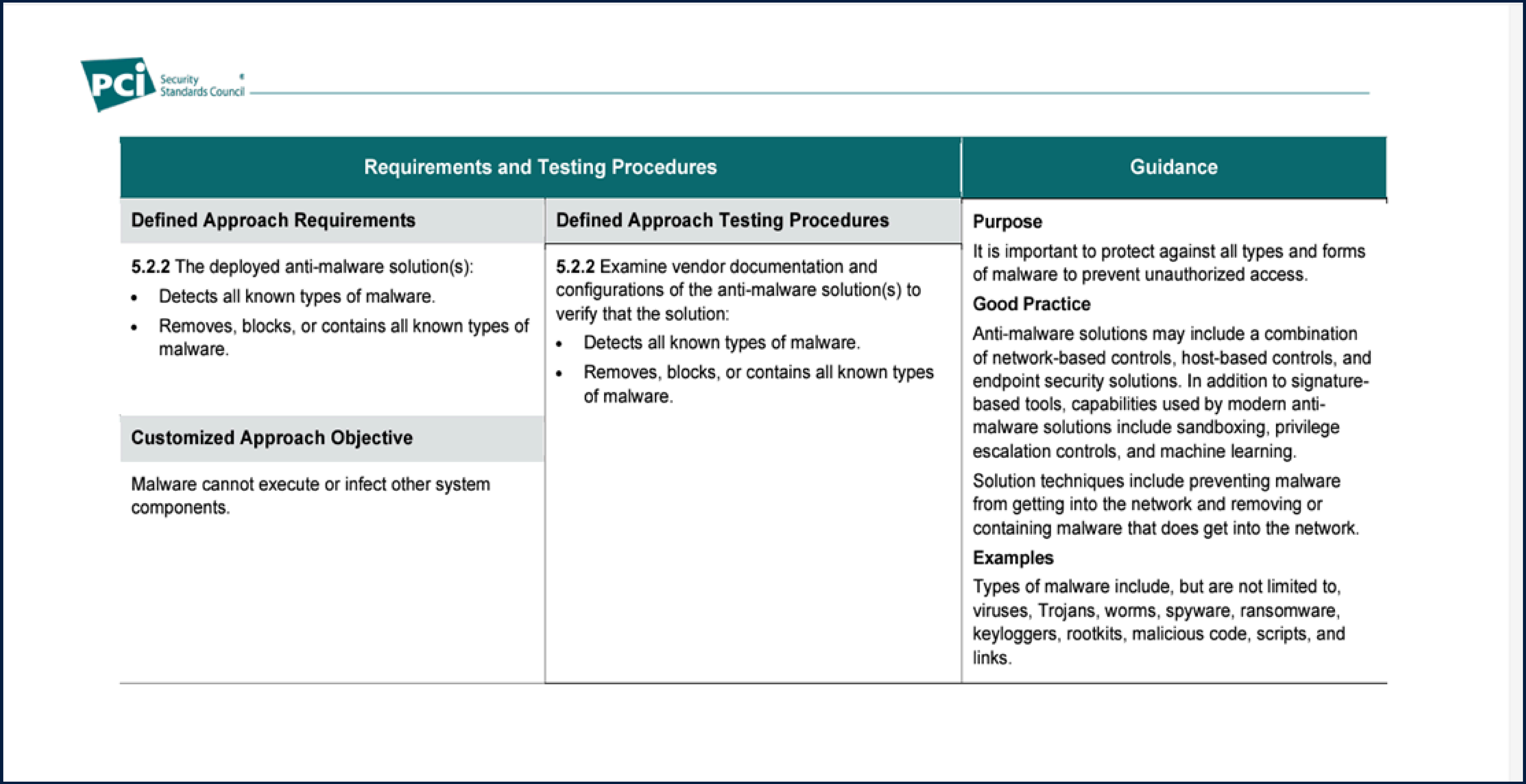
REQUIREMENT 5: PROTECT ALL SYSTEMS AND NETWORKS FROM MALICIOUS SOFTWARE



Requirements and Testing Procedures		Guidance
5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 5.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 5. While it is important to define the specific policies or procedures called out in Requirement 5, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
5.1.1 All security policies and operational procedures that are identified in Requirement 5 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**5.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 5 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 5 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		



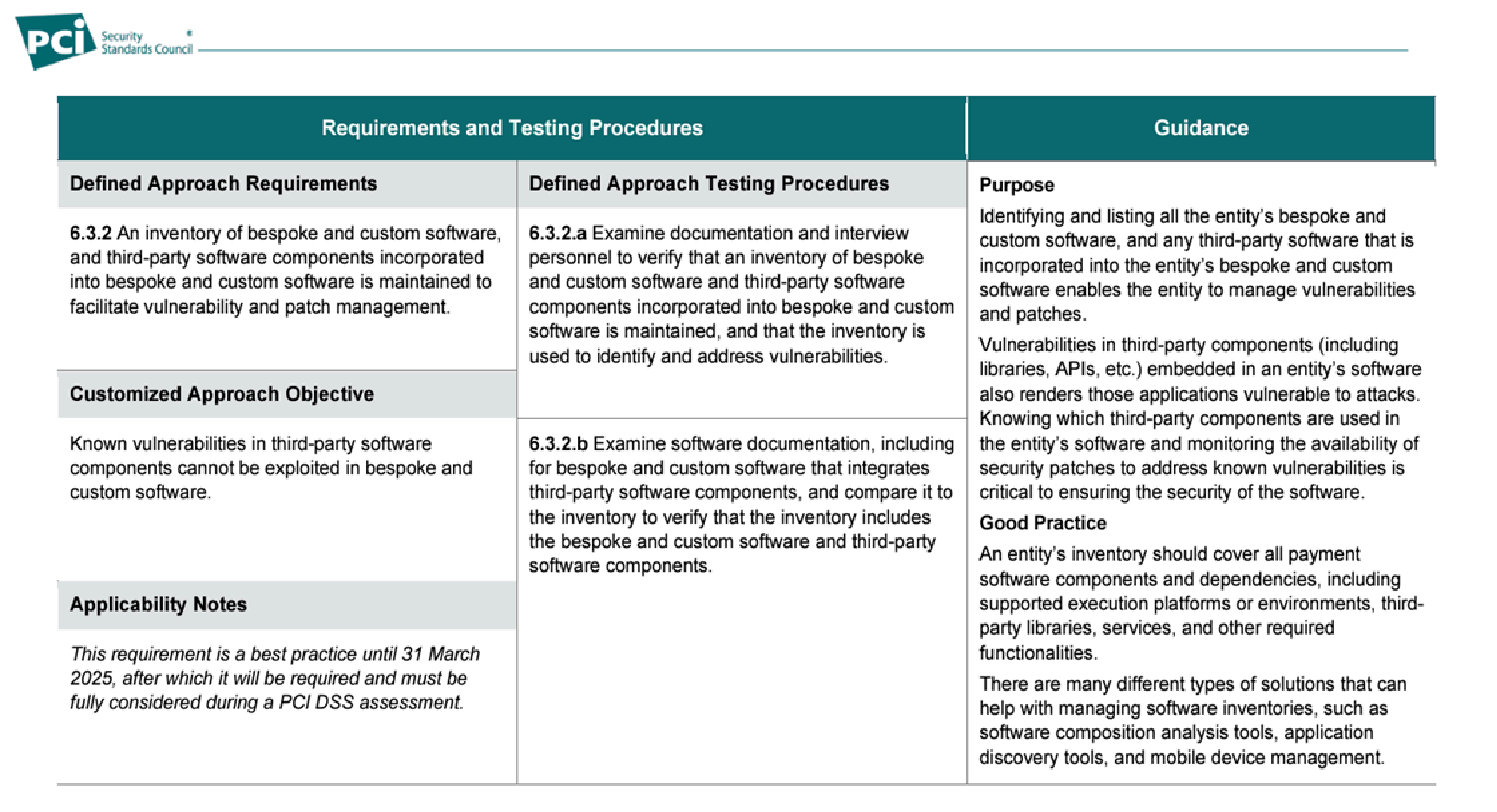
Requirements and Testing Procedures		Guidance
5.2 Malicious software (malware) is prevented, or detected and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** There is a constant stream of attacks targeting newly discovered vulnerabilities in systems previously regarded as secure. Without an anti-malware solution that is updated regularly, new forms of malware can be used to attack systems, disable a network, or compromise data. **Good Practice** It is beneficial for entities to be aware of "zero-day" attacks (those that exploit a previously unknown vulnerability) and consider solutions that focus on behavioral characteristics and will alert and react to unexpected behavior. **Definitions** System components known to be affected by malware have active malware exploits available in the real world (not only theoretical exploits).
5.2.1 An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.	**5.2.1.a** Examine system components to verify that an anti-malware solution(s) is deployed on all system components, except for those determined to not be at risk from malware based on periodic evaluations per Requirement 5.2.3.	
Customized Approach Objective	**5.2.1.b** For any system components without an anti-malware solution, examine the periodic evaluations to verify the component was evaluated and the evaluation concludes that the component is not at risk from malware.	
Automated mechanisms are implemented to prevent systems from becoming an attack vector for malware.		



Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** It is important to protect against all types and forms of malware to prevent unauthorized access. **Good Practice** Anti-malware solutions may include a combination of network-based controls, host-based controls, and endpoint security solutions. In addition to signature-based tools, capabilities used by modern anti-malware solutions include sandboxing, privilege escalation controls, and machine learning. Solution techniques include preventing malware from getting into the network and removing or containing malware that does get into the network. **Examples** Types of malware include, but are not limited to, viruses, Trojans, worms, spyware, ransomware, keyloggers, rootkits, malicious code, scripts, and links.
5.2.2 The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.	**5.2.2** Examine vendor documentation and configurations of the anti-malware solution(s) to verify that the solution: • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.	
Customized Approach Objective		
Malware cannot execute or infect other system components.		

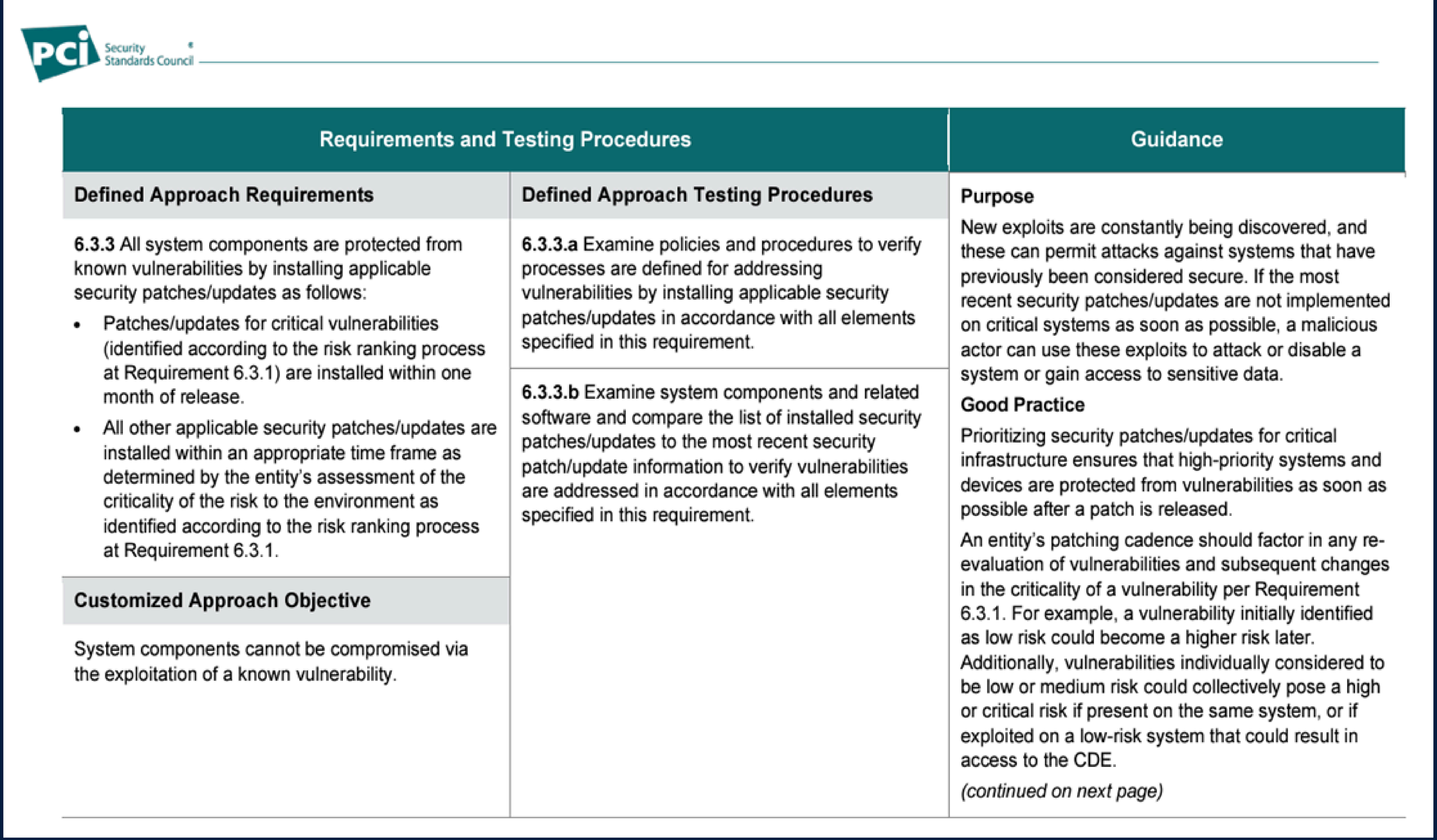
- IT IS ESSENTIAL TO KEEP OPERATING SYSTEM PATCHES UP TO DATE ON WORKSTATIONS, SERVERS, AND INFRASTRUCTURE APPLIANCES, AS WELL AS PATCHES FOR SOFTWARE LIKE JAVA, FLASH, AND SILVERLIGHT.

REQUIREMENT #6: DEVELOP AND MAINTAIN SYSTEMS AND SOFTWARE.



PCI Security Standards Council

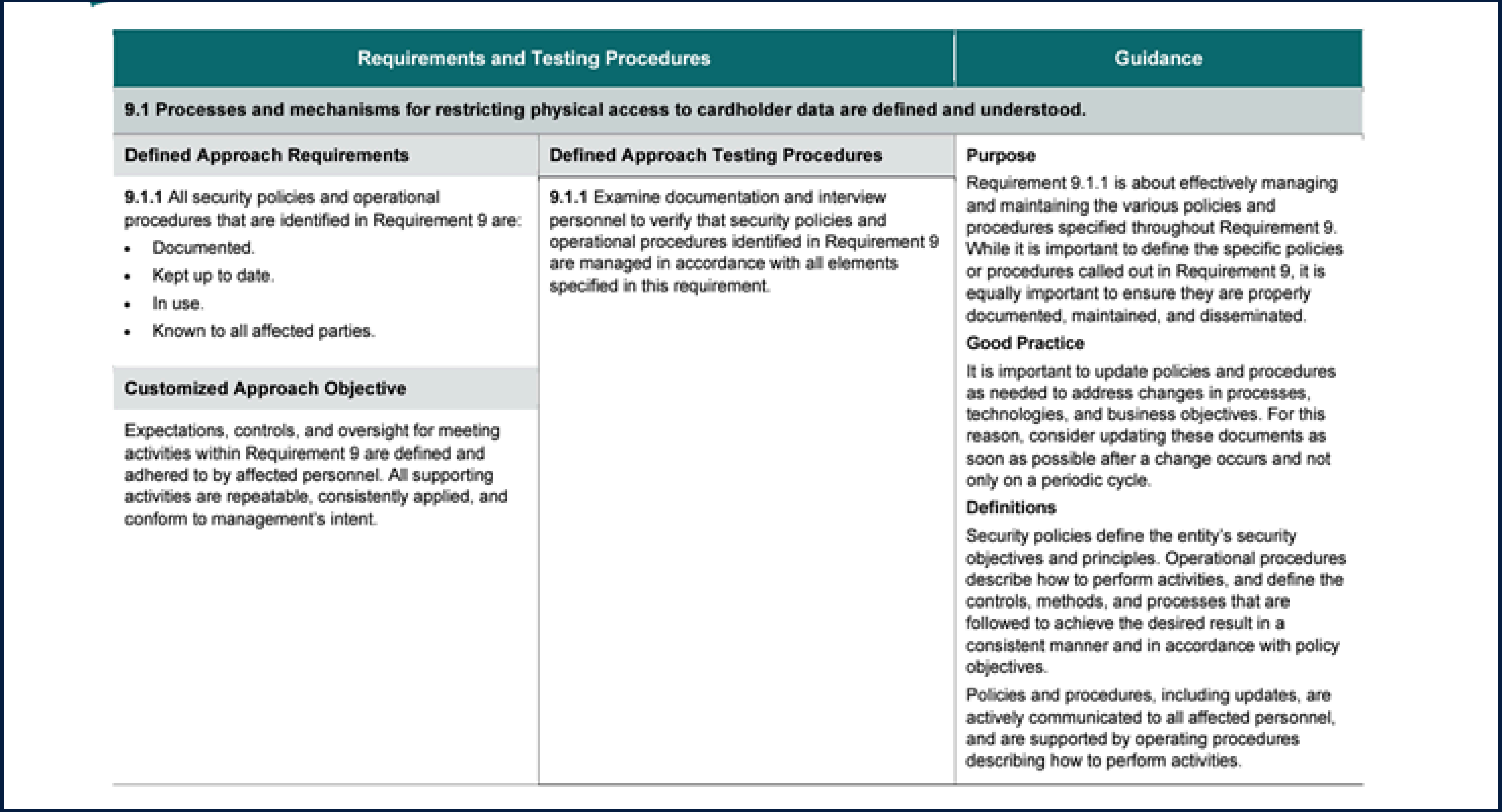
Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Identifying and listing all the entity's bespoke and custom software, and any third-party software that is incorporated into the entity's bespoke and custom software enables the entity to manage vulnerabilities and patches. Vulnerabilities in third-party components (including libraries, APIs, etc.) embedded in an entity's software also renders those applications vulnerable to attacks. Knowing which third-party components are used in the entity's software and monitoring the availability of security patches to address known vulnerabilities is critical to ensuring the security of the software. **Good Practice** An entity's inventory should cover all payment software components and dependencies, including supported execution platforms or environments, third-party libraries, services, and other required functionalities. There are many different types of solutions that can help with managing software inventories, such as software composition analysis tools, application discovery tools, and mobile device management.
6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	**6.3.2.a** Examine documentation and interview personnel to verify that an inventory of bespoke and custom software and third-party software components incorporated into bespoke and custom software is maintained, and that the inventory is used to identify and address vulnerabilities.	
Customized Approach Objective		
Known vulnerabilities in third-party software components cannot be exploited in bespoke and custom software.	**6.3.2.b** Examine software documentation, including for bespoke and custom software that integrates third-party software components, and compare it to the inventory to verify that the inventory includes the bespoke and custom software and third-party software components.	
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		



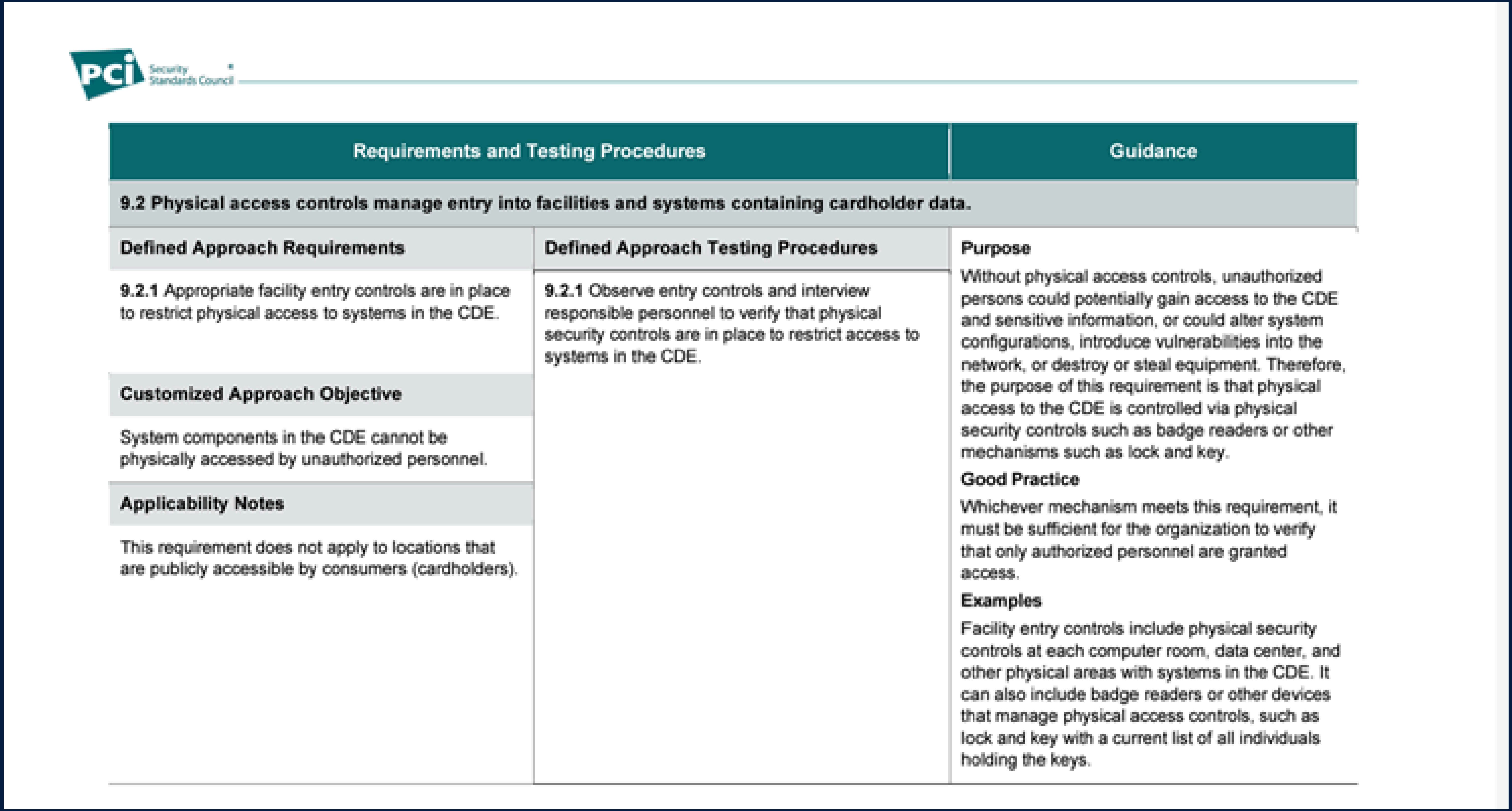
Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** New exploits are constantly being discovered, and these can permit attacks against systems that have previously been considered secure. If the most recent security patches/updates are not implemented on critical systems as soon as possible, a malicious actor can use these exploits to attack or disable a system or gain access to sensitive data. **Good Practice** Prioritizing security patches/updates for critical infrastructure ensures that high-priority systems and devices are protected from vulnerabilities as soon as possible after a patch is released. An entity's patching cadence should factor in any re-evaluation of vulnerabilities and subsequent changes in the criticality of a vulnerability per Requirement 6.3.1. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities individually considered to be low or medium risk could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE. *(continued on next page)*
6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Patches/updates for critical vulnerabilities (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity's assessment of the criticality of the risk to the environment as identified according to the risk ranking process at Requirement 6.3.1.	**6.3.3.a** Examine policies and procedures to verify processes are defined for addressing vulnerabilities by installing applicable security patches/updates in accordance with all elements specified in this requirement. **6.3.3.b** Examine system components and related software and compare the list of installed security patches/updates to the most recent security patch/update information to verify vulnerabilities are addressed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
System components cannot be compromised via the exploitation of a known vulnerability.		

- LIMIT THE NUMBER OF EMPLOYEES WITH LOGICAL AND PHYSICAL ACCESS TO SENSITIVE ACCOUNT INFORMATION.

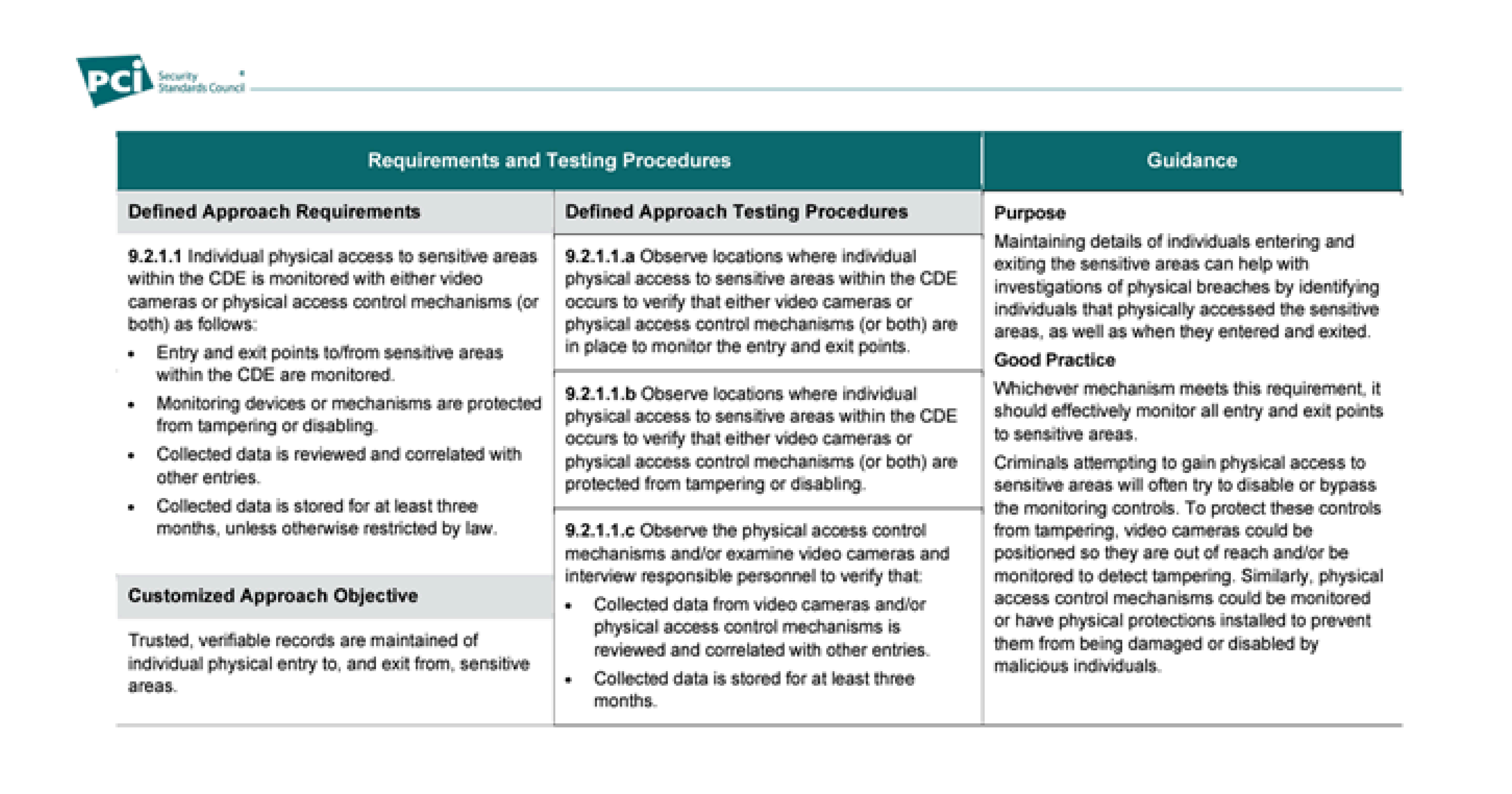
REQUIREMENT# 9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA



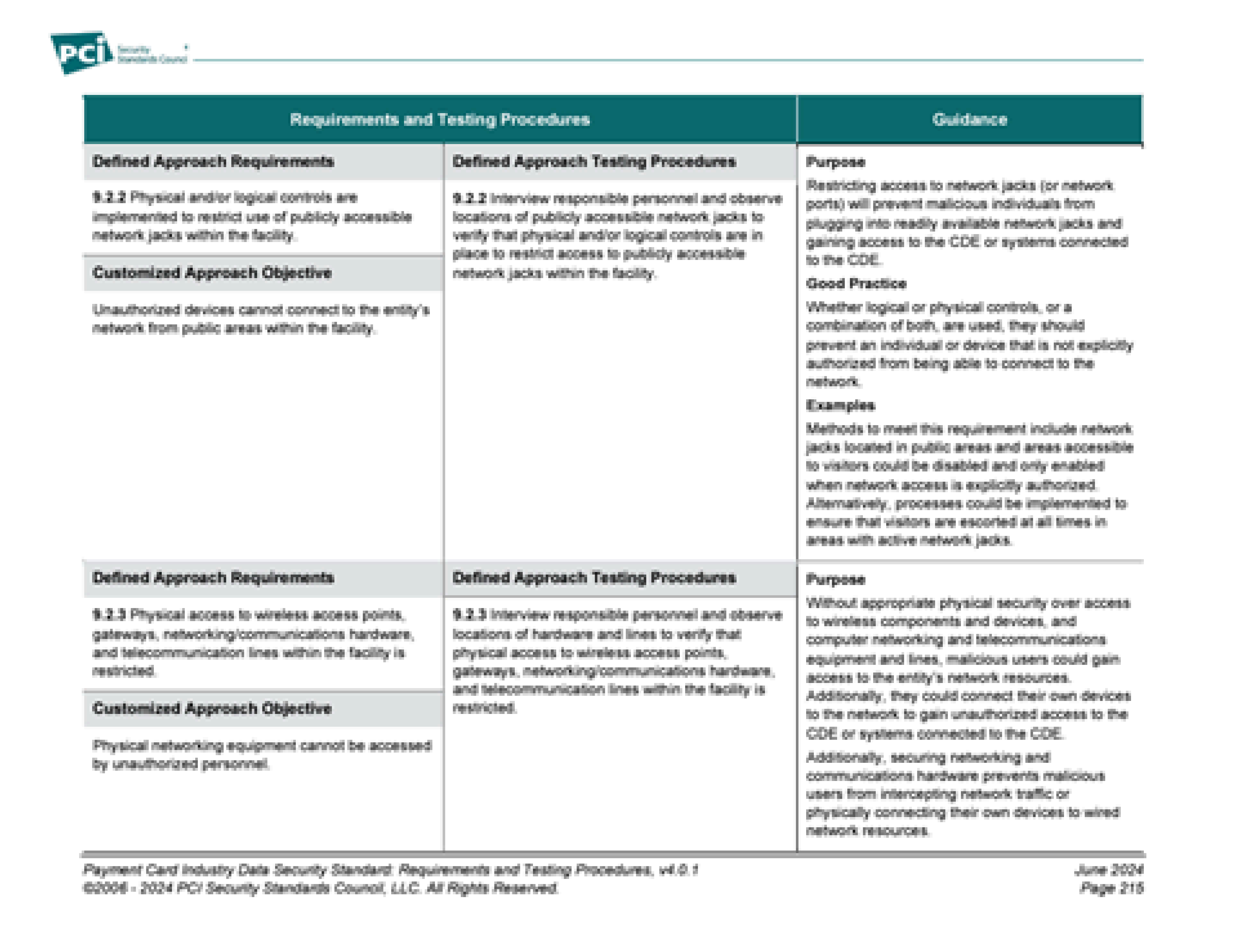
Requirements and Testing Procedures		Guidance
9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 9.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 9. While it is important to define the specific policies or procedures called out in Requirement 9, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives. Policies and procedures, including updates, are actively communicated to all affected personnel, and are supported by operating procedures describing how to perform activities.
9.1.1 All security policies and operational procedures that are identified in Requirement 9 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**9.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 9 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		



Requirements and Testing Procedures		Guidance
9.2 Physical access controls manage entry into facilities and systems containing cardholder data.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without physical access controls, unauthorized persons could potentially gain access to the CDE and sensitive information, or could alter system configurations, introduce vulnerabilities into the network, or destroy or steal equipment. Therefore, the purpose of this requirement is that physical access to the CDE is controlled via physical security controls such as badge readers or other mechanisms such as lock and key. **Good Practice** Whichever mechanism meets this requirement, it must be sufficient for the organization to verify that only authorized personnel are granted access. **Examples** Facility entry controls include physical security controls at each computer room, data center, and other physical areas with systems in the CDE. It can also include badge readers or other devices that manage physical access controls, such as lock and key with a current list of all individuals holding the keys.
9.2.1 Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	**9.2.1** Observe entry controls and interview responsible personnel to verify that physical security controls are in place to restrict access to systems in the CDE.	
Customized Approach Objective		
System components in the CDE cannot be physically accessed by unauthorized personnel.		
Applicability Notes		
This requirement does not apply to locations that are publicly accessible by consumers (cardholders).		



Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
9.2.1.1 Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: • Entry and exit points to/from sensitive areas within the CDE are monitored. • Monitoring devices or mechanisms are protected from tampering or disabling. • Collected data is reviewed and correlated with other entries. • Collected data is stored for at least three months, unless otherwise restricted by law.	**9.2.1.1.a** Observe locations where individual physical access to sensitive areas within the CDE occurs to verify that either video cameras or physical access control mechanisms (or both) are in place to monitor the entry and exit points.	**Purpose** Maintaining details of individuals entering and exiting the sensitive areas can help with investigations of physical breaches by identifying individuals that physically accessed the sensitive areas, as well as when they entered and exited. **Good Practice** Whichever mechanism meets this requirement, it should effectively monitor all entry and exit points to sensitive areas. Criminals attempting to gain physical access to sensitive areas will often try to disable or bypass the monitoring controls. To protect these controls from tampering, video cameras could be positioned so they are out of reach and/or be monitored to detect tampering. Similarly, physical access control mechanisms could be monitored or have physical protections installed to prevent them from being damaged or disabled by malicious individuals.
	9.2.1.1.b Observe locations where individual physical access to sensitive areas within the CDE occurs to verify that either video cameras or physical access control mechanisms (or both) are protected from tampering or disabling.	
Customized Approach Objective Trusted, verifiable records are maintained of individual physical entry to, and exit from, sensitive areas.	**9.2.1.1.c** Observe the physical access control mechanisms and/or examine video cameras and interview responsible personnel to verify that: • Collected data from video cameras and/or physical access control mechanisms is reviewed and correlated with other entries. • Collected data is stored for at least three months.	



Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Restricting access to network jacks (or network ports) will prevent malicious individuals from plugging into readily available network jacks and gaining access to the CDE or systems connected to the CDE. **Good Practice** Whether logical or physical controls, or a combination of both, are used, they should prevent an individual or device that is not explicitly authorized from being able to connect to the network. **Examples** Methods to meet this requirement include network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.
9.2.2 Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.	**9.2.2** Interview responsible personnel and observe locations of publicly accessible network jacks to verify that physical and/or logical controls are in place to restrict access to publicly accessible network jacks within the facility.	
Customized Approach Objective		
Unauthorized devices cannot connect to the entity's network from public areas within the facility.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without appropriate physical security over access to wireless components and devices, and computer networking and telecommunications equipment and lines, malicious users could gain access to the entity's network resources. Additionally, they could connect their own devices to the network to gain unauthorized access to the CDE or systems connected to the CDE. Additionally, securing networking and communications hardware prevents malicious users from intercepting network traffic or physically connecting their own devices to wired network resources.
9.2.3 Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.	**9.2.3** Interview responsible personnel and observe locations of hardware and lines to verify that physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.	
Customized Approach Objective		
Physical networking equipment cannot be accessed by unauthorized personnel.		