Open PCI DSS Scoping Toolkit

Open Scoping Framework Group

August 24, 2012

Open PCI DSS Scoping Toolkit

1 Executive Summary

Successful PCI DSS compliance depends upon the correct identification of the scope of the assessment. An overly narrow scope can jeopardize cardholder data, while an overly broad scope can add unnecessary cost and effort to the PCI compliance program. Subjective interpretation of the PCI DSS guidance results in a wide variance in practice among both QSAs and Participating Organizations.

The PCI Scoping Toolkit ("the Toolkit") provides a structured method for determining which system components in an organization's computing environment are within the scope of assessment. The Toolkit consists of definitions, three scoping categories, a decision tree and illustrative scoping scenarios. The Toolkit helps organizations and assessors determine correct scope of assessment, provides a common framework to discuss risks to cardholder data and facilitates discussion of controls, and is intended to be consistent with the spirit and intent of the PCI DSS.

We believe the Toolkit to be consistent with the spirit and intent of the PCI DSS. However, the Toolkit is not endorsed by the PCI Security Standards Council in any way, nor is it the product of an official Special Interest Group.

2 Copyright and Authors

For more information, please email:
pciscopingtoolkit@itrevolution.net

http://www.itrevolution.com

Document editors:

- Dorian Cougias, Unified Compliance Framework
- Phil Cox, RightScale
- Gene Kim, IT Revolution Press
- Ruth Xovox, ExoIS

We want to acknowledge the hard work of the forty-seven other practitioners who have contributed to this work since March 2009. We eagerly look forward to the time when all of these individuals can be publicly recognized for their contribution to this work.

3 Problem Statement

Successful PCI DSS compliance depends upon the correct identification of the scope of the assessment. When scoping errors occur, organizations will not focus on what matters most. An overly narrow scope of assessment could potentially jeopardize cardholder data, while an overly broad scope potentially adds unnecessary cost and effort to achieving PCI compliance.

Exacerbating this problem is the subjective interpretation of the PCI DSS guidance within the community of QSAs and Participating Organizations, resulting in a wide variance in practice.

Of particular note, it is widely believed that all PCI DSS control requirements must be applied to all system components in the scope of the assessment. Consequently, organizations fearing a prohibitively high cost of compliance will go to enormous lengths to incorrectly designate system components "out of scope," jeopardizing PCI compliance outcomes.

As a result, even the most experienced practitioners in the PCI Community have expressed that further guidance is needed to properly define the scope of assessment and its implications on the required controls.

4 Introduction to the Open PCI DSS Scoping Toolkit

The Open PCI DSS Scoping Toolkit ("the Toolkit") provides a structured method for determining which system components in an organization's computing environment are within the PCI Scope of Assessment.

The Toolkit categorizes system components according to several factors:

- Whether cardholder data is being stored, processed or transmitted.
- The functionality that the system component provides (e.g. authorization, authentication, performance monitoring, etc.).
- The connectivity between the system component and the cardholder data environment (CDE).

The Toolkit is intended to be used after the organization has located and documented where cardholder data is stored, processed and transmitted; documented relevant business process work flows and system data flows; and gained an understanding of the physical/logical computing environments and existing controls in place protecting cardholder data (CHD).

This Toolkit can be used by both large and small organizations to help critically evaluate the system components that comprise the scope of assessment. The primary difference between large and small organizations will be the number of system components that are evaluated using the Toolkit. A small organization may have one CDE consisting of ten system components, while a larger organization may have multiple CDEs consisting of thousands of system components.

We believe the Toolkit to be consistent with the spirit and intent of the PCI DSS. However, the Toolkit is not endorsed by the PCI Security Standards Council in any way, nor is it the product of an official Special Interest Group.

4.1 About this Document

This document includes the following sections:

- **Definitions** – provides definitions of terms used in this document and within the PCI DSS, and describes the expansion or clarification of those terms proposed by the Toolkit.
- **Categorization of System Components** – defines the characteristics of system component categories defined by the Toolkit and lists the implications of each.
- **Scoping Decision Tree** – diagrams each step in the decision process and lists the criteria for each decision.
- **Scoping Scenarios** – provides illustrative examples of typical situations found in organizations' environments and shows how each system component would be categorized using the scoping decision tree.

4.2 Benefits of Using the Toolkit

Use of the Toolkit provides the following benefits:

- Aids in determination of which system components are in and out of the scope of assessment.
- Facilitates communication between organizations and assessors by providing a common language to describe the computing environment and risks to cardholder data.
- Provides a framework to categorize and identify the different types of system components, each with a different risk profile associated with it.
- Provides a thought process to reduce the scope of assessment, by isolating and controlling access to the CDE, re-architecting the control environment or by implementing further controls.

4.3 What the Toolkit Does Not Address

Although addressing the people and processes around cardholder data is a necessary part of any PCI compliance program, the Toolkit focuses almost entirely on categorizing the system components that comprise an organization's computing environment.

In addition, the Toolkit does not define what PCI DSS controls are required for each Toolkit category. Because every organization is different, it is up to each organization and its assessor to determine the nature, extent and effectiveness of each control to adequately mitigate the risks to cardholder data.

4.4 The Toolkit Within the PCI Compliance Lifecycle

The following table outlines the major steps in a typical PCI DSS compliance program, and where the Toolkit fits:

Steps that Precede Use of the Toolkit	*Confirm the Accuracy of the Assessment Scope*	1. Document the organization's business and data workflows for known and potential instances where cardholder data is stored, processed, or transmitted. After gaining a complete understanding of all people, process, and technology-related interactions with the cardholder data, identify and document all locations and flows of the cardholder data[1].
	Evaluate the Business Need for Each Location and Flow of CHD	2. For each instance identified above, evaluate the business need to handle cardholder data: • If cardholder data is not needed, don't collect it and securely delete what has been collected. • If the cardholder data is required, consider migrating or consolidating it elsewhere in the

[1] As required by the PCI DSS v2.0.

		CDE to reduce scope, improve control, and mitigate risk.
Toolkit Steps	*Use the Decision Tree to Categorize Systems*	3. Use the Scoping Decision Tree to determine whether each system component is in the scope of assessment, and assign it a specific scoping sub-category. **Note:** The result of categorizing each system component helps identify the relevant risks to the CDE. Completing this step can be used in support of PCI DSS requirement 12.1.2 (i.e., perform an annual risk assessment that identifies threats and vulnerabilities)
Steps that Follow Use of the Toolkit	*Evaluate Scoping Conclusions and Consider Further Reducing the Scope of Assessment*	4. Consider the risk implications of the scoping conclusions and identify potential opportunities to further reduce assessment scope (e.g., re-architecting business processes, data flows, and/or the control environment).
		5. Evaluate each in-scope system component against all PCI DSS requirements for applicability and necessity, based on the risk to cardholder data and the overall control environment.
		6. Architect, design, implement and document the controls required to adequately mitigate the identified risk to cardholder data.
		7. Assess the controls for design and operating effectiveness, at the level of both the system components and the environment.

5 Definitions and Terms Used in This Document

This section presents definitions sourced from PCI DSS version 2.0 and the PCI DSS Glossary, and then provides the Toolkit definition and clarification of any differences.

5.1 Organization

"Organization" is used as the equivalent to "entity under assessment", as defined in the PCI DSS. Examples of entities under assessment include but are not limited to merchants and service providers.

5.2 Assessor

"Assessor" is used to refer to all types of assessors (e.g., QSAs, ISAs, self-assessing organizations).

5.3 System Component

"System component" refers to any network component, server, or application. System components can be:

- **Virtual components** – include but are not limited to virtual machines, virtual routers/switches, virtual appliances, virtual desktops/applications and hypervisors.
- **Network components** – include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- **Servers** – include but are not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name Service (DNS) servers.
- **Applications** – include all purchased and custom applications, including internal and external (e.g., Internet) applications.

Note: The Toolkit will use the term "device" as a synonymous term for "system component".

5.4 Cardholder Data Environment (CDE)

The PCI DSS defines the CDE to be "the people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components."

The Toolkit further adds the following definitions of activities that occur in the CDE:

- **Processing** – when cardholder data is actively being used by a system component (e.g., entered, edited, manipulated, printed, viewed)

- **Storing** – when cardholder data is inactive or at rest (e.g., located on electronic media, system component memory, paper)
- **Transmitting** – when cardholder data is being transferred from one location to another (e.g., data in motion).

5.5 Scoping Process, Scope of Assessment and In-Scope Components

The PCI DSS defines scoping to be "the process of identifying all system components, people, and processes to be included in a PCI DSS assessment to accurately determine the scope of assessment."

The Toolkit uses these definitions as-is, but clarifies the control implication of system components in the scope of assessment. In practice, too many organizations and assessors incorrectly conclude that all in-scope system components must meet all PCI DSS control requirements. Consequently, organizations will go to extreme lengths to make system components "out of scope," fearing a prohibitively high cost of compliance.

The Toolkit facilitates the correct determination of the scope of assessment, and provides the basis to analyze the applicability and necessity of each PCI DSS control requirement.

Note that the Toolkit does not prescribe which controls should apply to specific system components. The organization under assessment is responsible for defining the scope of assessment. The assessor is responsible for validating the scoping conclusions and effectiveness of controls. All in-scope system components must be explicitly included in the risk assessment required in PCI DSS requirement 12.1.2, and justification for reduced controls must be documented.

5.6 Segmentation

The PCI DSS Glossary defines network segmentation as what "isolates system components that store, process, or transmit cardholder data from systems that do not. Adequate network segmentation may reduce the scope of the cardholder data environment and thus reduce the scope of the PCI DSS assessment. Network segmentation is not a PCI DSS requirement."

The PCI DSS uses the term "segmentation" to be equivalent to total isolation between system components. However, this definition does not match the way this term is used in common practice in computer networking. In addition the PCI DSS does not take into account the common practice of limiting or controlling network access between system components.

To eliminate ambiguity of the term "segmentation," the Toolkit instead uses one of the two following terms:

- **Isolation** – achieved when network traffic between two system components is not permitted.

- **Controlled access** – achieved when access between system components is restricted to defined parameters. Restrictions may include endpoint identifiers (e.g., user identity, address), type of traffic (e.g., logical port, protocol, service, application), the direction from which the connection is initiated (e.g., inbound, outbound), etc.

The mechanism providing the isolation or controlled access functionality may be either logical or physical. Examples of mechanisms include network and host-based firewalls, virtual routing and switching appliances, and access control lists.

As supported by PCI DSS 2.0 (page 11), the Toolkit requires the organization to assert that all controls providing isolation or controlled access functionality are designed and operating effectively, which the assessor must verify.

5.7 Applicability

Applicability refers to a determination of whether a PCI DSS control logically applies to the system component being reviewed. An example of this is the requirement for encryption key rotation, which is applicable to systems that store encrypted cardholder data, but is not applicable to systems that do not.

5.8 Necessity

Necessity refers to a determination, following a risk assessment, of whether a PCI DSS control is needed to mitigate risk to cardholder data from that system component.

6 Scoping Categories and Definitions

The PCI DSS categorizes system components as being either in or out of the scope of assessment. However, to better enable correct scoping, the Toolkit defines three categories of system components, and highlights the different types of risks associated with each category. Doing so makes more evident which system components are the most important to protect, based on the types of risk they pose to cardholder data.

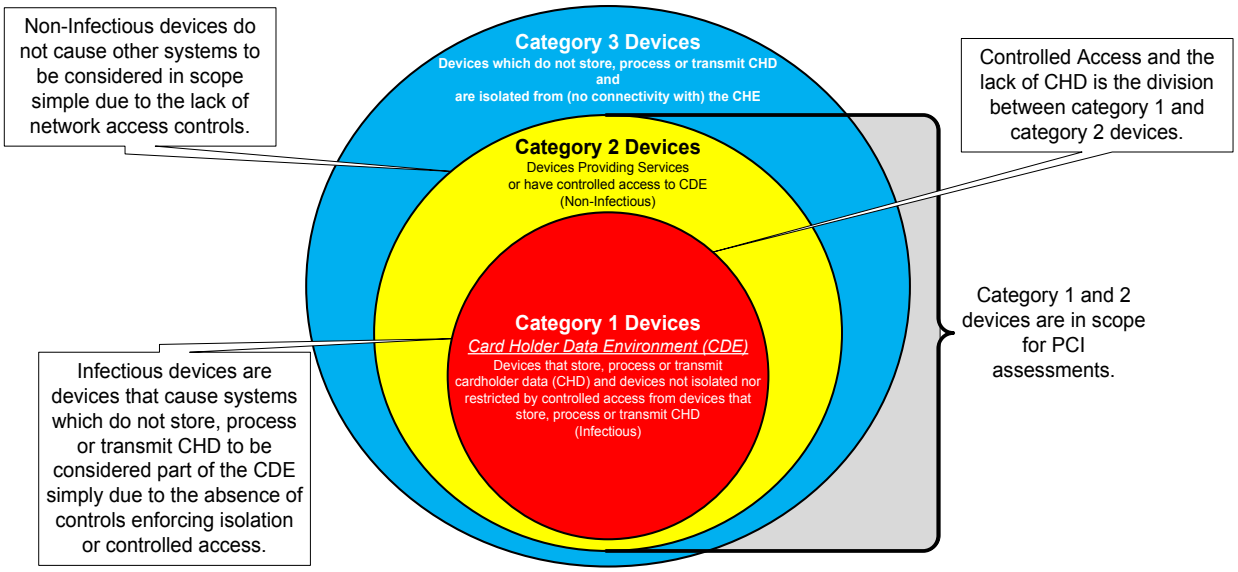
Every system component within an organization's computing environment can be categorized into one and only one of the following:

- **Category 1** – System components that process, store or transmit cardholder data or are not isolated or restricted through controlled access from other Category 1 system components.
- **Category 2** – System components that have controlled access to a Category 1 system component.
- **Category 3** – System components that are isolated from all Category 1 system components.

Categorizing each system component into one of these categories achieves several key results:

- Identifies all system components that are within the scope of assessment.
- Aids in documenting risks to cardholder data as each system component within the environment is analyzed.
- As Category 2 system components are further sub-categorized, helps clarify risks to cardholder data.
- Enables the objective evaluation of PCI DSS controls for applicability and necessity.

The following graphic shows the three, mutually exclusive categories:



6.1 Category 1 System Components

A system component is considered Category 1 if it stores, transmits or processes cardholder data. In addition, the Toolkit introduces the concept of "infectious" to address the impact of a Category 1 system component on other devices.

A system component that stores, processes or transmits cardholder data (i.e., Category 1a) is said to be "infectious." All devices that have unrestricted network access to that Category 1a device become Category 1b devices, even if they do not store, process or transmit cardholder data.

Therefore, two kinds of system components fall into Category 1:

Category 1a	Devices that store, process or transmit cardholder data
Category 1b	Devices that do not store, process or transmit cardholder data, but, are "infected by" Category 1a devices due to the absence of controlled access or isolation.

Implications of Category 1 system components:

- All Category 1 system components are "infectious."
- All Category 1 system components are always within the scope of assessment.
- Each Category 1 system component must be evaluated against all PCI DSS requirements to determine the applicability of each requirement.
- All applicable PCI DSS control requirements are necessary for every Category 1 device.

6.2 Category 2 System Components

Category 2 system components do not store, process or transmit cardholder data but have controlled access to and/or from Category 1 devices. This controlled access must:

- Limit network traffic to only that which is required for business operations.
- Be justified and documented.

Category 2 system components are further defined in the following manner:

Category 2a	System components which, through controlled access, provide security services (e.g., authentication) to a Category 1 device.
Category 2b	System components which, through controlled access, can initiate an inbound connection to a Category 1 device.
Category 2c	System components which, through controlled access, can only receive a connection from a Category 1 device (i.e., cannot initiate a connection).
Category 2x	System components which, through indirect and controlled access, have the ability to administer Category 1 devices. **Note:** Category 2x devices have no direct access to/from Category 1 devices.

Implications of Category 2 system components:

- Category 2 system components have controlled access to the CDE.
- Category 2 system components are not "infectious."
- Category 2 system components are always within the scope of assessment.
- Each Category 2 system component must be evaluated against all PCI DSS requirements to determine the "applicability" of each requirement, as well as the "necessity" of each control based on an assessment of the risk to the CDE and the overall control environment.
- Category 2 system components must be adequately protected to prevent Category 3 devices from being a valid vector of attack.

6.3 Category 3 System Components

Category 3 system components do not store, process or transmit cardholder data; and are isolated from and do not provide any services to any Category 1 device. Therefore, Category 3 system components are not in the scope of assessment.

6.4 Summary of Categories

The following table summarizes the scoping categories and sub-categories:

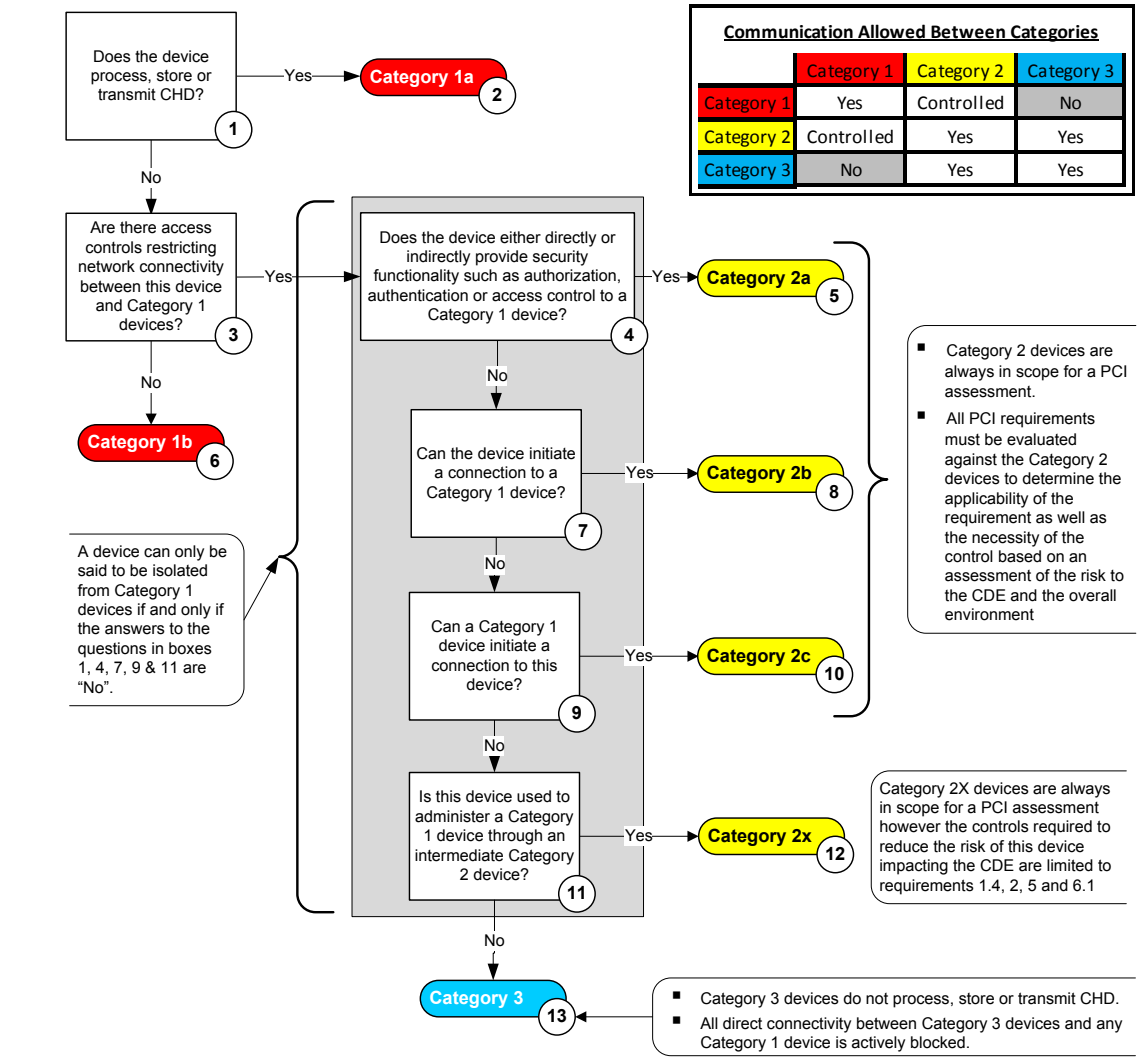
Category	Description	Method of Segmentation	CHD?	Access with CHE?	Service/Auth	Risk/Vector of Attack	In Scope for a PCI Assessment
1a	Systems that store, process or transmit cardholder data (CHD).	N/A	Yes	Yes	YES/NO	Yes	Yes
1b	Systems with unrestricted network access to a 1a device; a "directly attached" system.	Open	No	Yes	YES/NO	Yes	Yes
2a	Systems that, through controlled access, provide security services to any Category 1 device.	Controlled Access	No	Yes	YES	Yes	Yes
2b	Systems that, through controlled access, can initiate an inbound connection to a Category 1 device.	Controlled Access	No	Yes	YES/NO	Yes	Yes
2c	Systems that through controlled access cannot initate connections to, but receive an initiated connection from a Category 1 device.	Controlled Access	No	Only From CDE	YES/NO	Yes	Yes
2x	Systems that, through indirect access, have the ability to administer a Category 1 device. Note 2x devices have no direct access to/from Category 1 devices.	Controlled Access	No	Indirect	No	Yes	Yes
3	Systems that do not store, process or transmit CHD. All network traffic between Category 3 and Category 1 devices is restricted (isolated).	Isolated	No	No	No	No	No

7 Scoping Decision Tree

The following diagram shows the detailed decision tree which applies the concepts introduced in the previous section.

PCI Scoping Decision Tree

Category	Description	Vector of Attack	In Scope
1a	Systems that store, process or transmit cardholder data (CHD).	Yes	Yes
1b	Systems with unrestricted network access to a 1A device; a "directly attached" system.	Yes	Yes
2a	Systems that, through controlled access, provide security services to any Category 1 device.	Yes	Yes
2b	Systems that, through controlled access, can initiate an inbound connection to a Category 1 device.	Yes	Yes
2c	Systems that through controlled access cannot initate connections to, but receive an initiated connection from a Category 1 device.	Yes	Yes
2x	Systems that, through indirect access, have the ability to administer a Category 1 device. Note 2x devices have no direct access to/from Category 1 devices.	Yes	Yes
3	Systems that do not store, process or transmit CHD. All network traffic between Category 3 and Category 1 devices is restricted (isolated).	No	No



8 Conclusion

The PCI Community has articulated the need for further guidance to determine the correct scope of assessment. To address this need, the PCI Technology Scoping Toolkit provides a structured method for determining which system components in an organization's computing environment are within the scope of assessment.

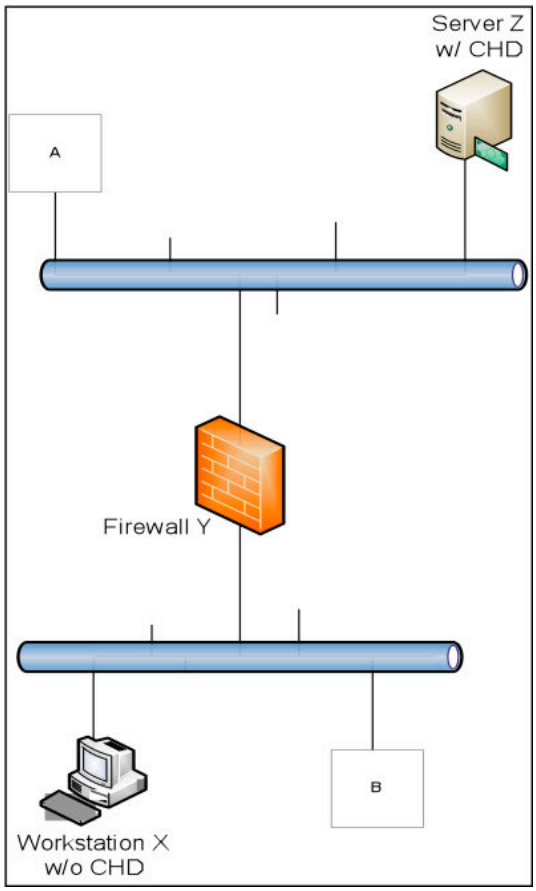
The Toolkit also provides the basis to analyze the applicability and necessity of each PCI DSS control requirement, even though it does not prescribe which controls apply to specific system components.

The Toolkit is intended to help organizations and assessors determine an accurate scope of assessment, provide a common framework for discussing risks to cardholder data and controls that address that risk, while remaining consistent with the spirit and intent of the PCI DSS.

9 Appendix A: Scoping Scenarios

The following scenarios illustrate the application of the Toolkit. Because all environments and organizations are different; each organization should evaluate all system components in its environment using the Toolkit.

9.1 Scenario 1: Domain controller relied upon by a Category 1 device



The device in question is an Active Directory domain controller (DC) providing authentication services to Server Z with CHD.

Workstation X has no CHD and does not manage a Category 1 system.

Location of device: Position A

Network Access Controls:

- Firewall Y allows Authentication traffic between Workstation X and the DC in Position A.
- Firewall Y denies all other traffic between Workstation X and the DC in Position A.
- Firewall Y denies all traffic between Workstation X and Server Z.
- No other network access controls are in place.

9.1.1 Decision tree for Firewall Y

Box	Answer for Box	Outcome
1	No, Firewall Y does not process, store or transmit CHD.	Go to box 3
3	Yes, Firewall Y itself provides access controls that restrict network connectivity.	Go to box 4
4	Yes, Firewall Y provides security functionality to a Category 1 device.	Go to box 5
5	Therefore Firewall Y is a Category 2a device.	**Category 2a**

9.1.2 Decision Tree for Server Z

Box	Answer for Box	Outcome
1	Yes, Server Z processes, stores or transmits CHD.	Go to box 2
2	Therefore Server Z is a Category 1a device.	**Category 1a**

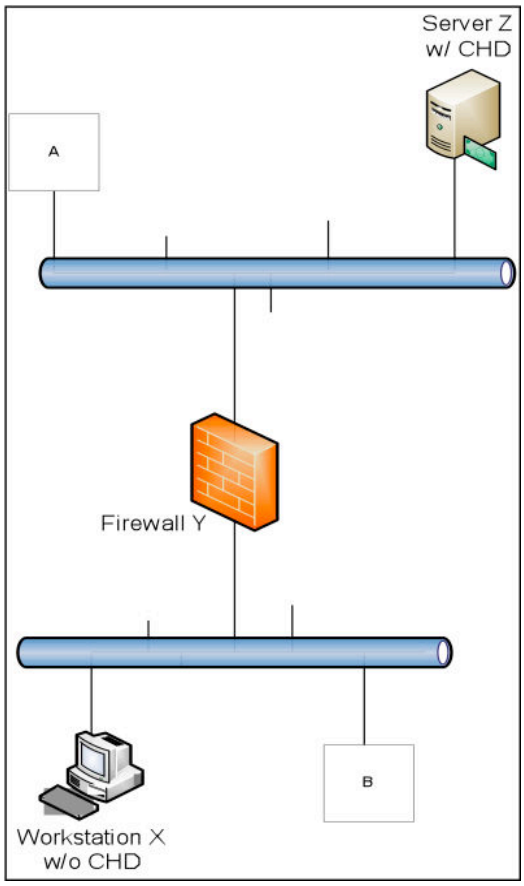
9.1.3 Decision Tree for domain controller in position A

Box	Answer for Box	Outcome
1	No, the DC does not process, store or transmit CHD.	Go to box 3
3	No, the DC has no access controls restricting access to Category 1 devices.	Go to box 6
6	Therefore the DC is a Category 1b device.	**Category 1b**

9.1.4 Decision Tree for Workstation X

Box	Answer for Box	Outcome
1	No, Workstation X does not process, store or transmit CHD.	Go to box 3
3	Yes, Firewall Y provides access controls that restricts network connectivity to Category 1 devices.	Go to box 4
4	No, Workstation X does not provide services to Server Z.	Go to box 7
7	Yes, Workstation X has the ability to initiate a connection to a Category 1 device (DC in Position A).	Go to box 8
8	Therefore Workstation X is a Category 2b device.	**Category 2b**

9.2 Scenario 2: Domain controller separated from but relied upon by a Category 1 device



The device in question is a domain controller (DC) providing authentication services to Server Z with CHD.

Workstation X has no CHD and does not manage a Category 1 system.

Location of device: Position B

Network Access Controls:

- Firewall Y allows authentication traffic between the DC in Position B and Server Z.
- Firewall Y denies all other traffic between the DC in Position B and Server Z.
- Firewall Y denies all traffic between Workstation X and Server Z.
- No other network access controls are in place.

9.2.1 Decision tree for Firewall Y

Box	Answer for Box	Outcome
1	No, Firewall Y does not process, store or transmit CHD.	Go to box 3
3	Yes, Firewall Y provides access controls that restrict network connectivity.	Go to box 4
4	Yes, Firewall Y provides security functionality to a Category 1 device.	Go to box 5
5	Therefore Firewall Y is a Category 2a device.	**Category 2a**

9.2.2 Decision Tree for Server Z

Box	Answer for Box	Outcome
1	Yes, Server Z processes, stores or transmits CHD.	Go to box 2
2	Therefore Server Z is a Category 1a device.	**Category 1a**

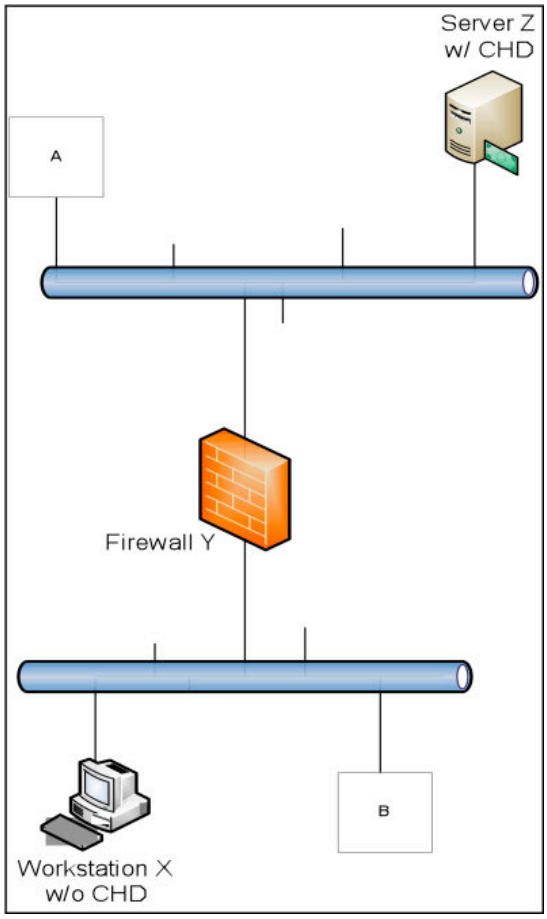
9.2.3 Decision Tree for DC in position B

Box	Answer for Box	Outcome
1	No, the DC does not process, store or transmit CHD.	Go to box 3
3	Yes, Firewall Y . provides access controls that restrict network connectivity to Category 1 devices.	Go to box 4
4	Yes, the DC provides authentication services for Server Z.	Go to box 5
5	Therefore the DC is a Category 2a device.	**Category 2a**

9.2.4 Decision Tree for Workstation X

Box	Answer for Box	Outcome
1	No, Workstation X does not process, store or transmit CHD.	Go to box 3
3	Yes, Firewall Y provides access controls that prevent access between Workstation X and Category 1 devices.	Go to box 4
4	No, Workstation X does not provide services to Server Z.	Go to box 7
7	No, Firewall Y denies Workstation X from initiating a connection to Server Z.	Go to box 9
9	No, Firewall Y denies Server Z from initiating a connection to Workstation X.	Go to box 11
11	No, Workstation X does not directly or indirectly administer Category 1 devices.	Go to box 13
13	Therefore Workstation X is a Category 3 device.	

9.3 Scenario 3: “Jump Box” login server



The device in question is a "Jump Box" Server that allows only SSH inbound and outbound traffic. Inbound traffic is controlled by username/password. An administrator using Workstation X, SSHs to the “Jump Box” Server and then SSHs from the “Jump Box” Server to administer Server Z. Controls are in place so neither the “Jump Box” nor the administrative workstation has access to CHD.

No CHD is processed, stored or transmitted to the “Jump Box” Server or to Workstation X.

Location of device: Position B

Network Access Controls:

- Firewall Y allows SSH traffic only between the “Jump Box” Server and Server Z.
- Firewall Y denies all other traffic between the Linux Server and Server Z.
- Firewall Y denies all traffic between Workstation X and Server Z.
- The “Jump Box” Server denies all inbound traffic except SSH.
- No other network access controls are in place.

9.3.1 Decision tree for Firewall Y

Box	Answer for Box	Outcome
1	No, Firewall Y does not process, store or transmit CHD.	Go to box 3
3	Yes, Firewall Y provides access controls that restrict network connectivity.	Go to box 4
4	Yes, Firewall Y provides security functionality to a Category 1 device.	Go to box 5
5	Therefore Firewall Y is a Category 2a device.	**Category 2a**

9.3.2 Decision Tree for Server Z

Box	Answer for Box	Outcome
1	Yes, Server Z processes, stores or transmits CHD	Go to box 2
2	Therefore Server Z is a Category 1a device.	**Category 1a**

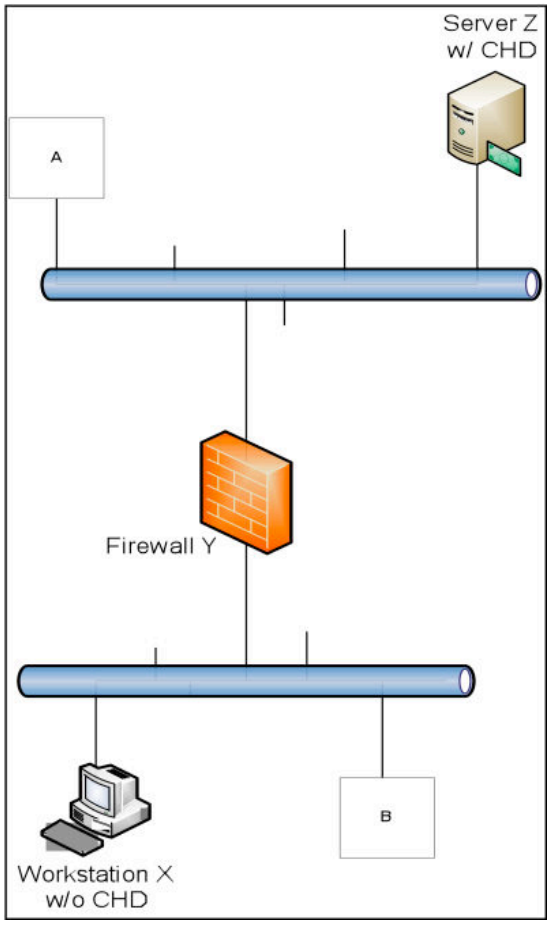
9.3.3 Decision Tree for the "Jump Box" Server in position B

Box	Answer for Box	Outcome
1	No, the “Jump Box” Server does process, store or transmit CHD	Go to box 3
3	Yes, Firewall Y provides access controls that restrict access to Category 1 devices.	Go to box 4
4	No, the “Jump Box” Server does not provide authentication services for Server Z.	Go to box 7
7	Yes, the “Jump Box” Server can initiate a connection to Server Z.	Go to box 8
8	Therefore the “Jump Box” Server is a Category 2b device.	**Category 2b**

9.3.4 Decision Tree for Workstation X

Box	Answer for Box	Outcome
1	No, Workstation X does process, store or transmit CHD	Go to box 3
3	Yes, Firewall Y provides access controls that prevent access to Category 1 devices.	Go to box 4
4	No, Workstation X does not provide services to Server Z	Go to box 7
7	No, Firewall Y denies Workstation X the ability to initiate a connection to Server Z.	Go to box 9
9	No, Firewall Y denies Server Z the ability to initiate a connection to Workstation X.	Go to box 11
11	Yes, Workstation X is used to administer a Category 1 device using an intermediate Category 2 device; the “Jump Box” Server.	Go to box 12
12	Therefore Workstation X is a Category 2x device.	**Category 2x**

9.4 Scenario 4: Hotel front desk workstation/dumb terminal



The device in question is a front desk dumb terminal running a Citrix client, on which cardholder data is entered. The dumb terminal has no listening network ports, is physically secured with no access to USB, SD or flash card ports and local administrator accounts are known only to authorized administrators. All application security functionality is provided at the Citrix Server located in position A.

Workstation X is a workstation with no CHD and does not manage any CDE devices.

Location of device: Position B

Network Access Controls:

- Firewall Y allows only encrypted Citrix traffic between the dumb terminal client in position B and the Citrix Server in position A.
- Firewall Y denies all other traffic between the dumb terminal client and the Citrix server in position B and Server Z.
- Firewall Y denies all traffic between Workstation X and the Citrix server in position B and Server Z.
- The dumb terminal Citrix client by configuration can only connect to the Citrix service in location A. The configuration allows for no other traffic inbound or outbound.
- No other network access controls are in place.

9.4.1 Decision tree for Firewall Y

Box	Answer for Box	Outcome
1	Yes, Firewall Y processes, stores or transmits CHD.	Go to box 2
2	Therefore Firewall Y is a Category 1a device.	Category 1a

9.4.2 Decision Tree for Server Z

Box	Answer for Box	Outcome
1	Yes, Server Z processes, stores or transmits CHD.	Go to box 2
2	Therefore Server Z is a Category 1a device.	Category 1a

9.4.3 Decision Tree for Citrix Server in position A

Box	Answer for Box	Outcome
1	Yes, the Citrix Service processes, stores or transmits CHD	Go to box 2
2	Therefore the Citrix Server is a Category 1a device.	Category 1a

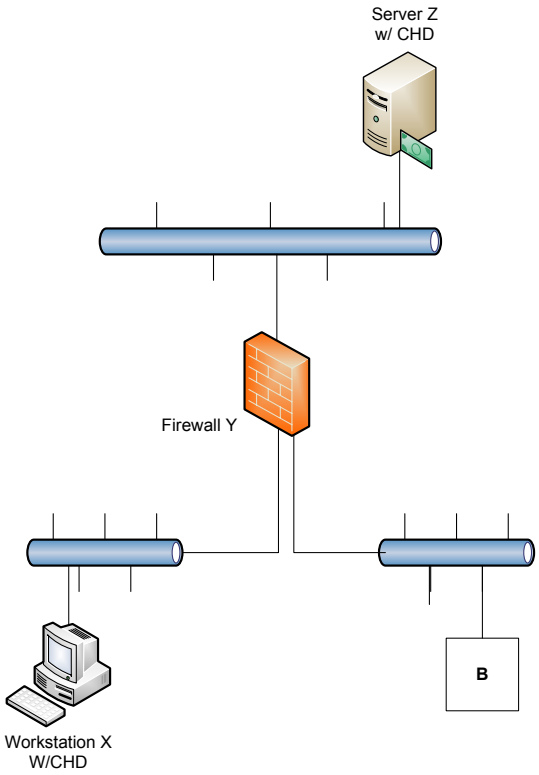
9.4.4 Decision Tree for the dumb terminal Citrix Client at position B

Box	Answer for Box	Outcome
1	Yes, the dumb terminal processes, stores or transmits CHD	Go to box 2
2	Therefore the dumb terminal client is a Category 1a device.	Category 1a

9.4.5 Decision Tree for Workstation X

Box	Answer for Box	Outcome
1	No, Workstation X does not process, tore, or transmit CHD.	Go to box 3
3	Yes, Firewall Y provides access controls that prevent access to the Virtual Application Server and Server V. The fact that the virtual terminal has no active listing ports and thus cannot accept inbound initiated connections is an isolation control. Also, the dumb terminal can only communicate with the Virtual Application Server in position A.	Go to box 4
4	No, Workstation X does not provide services to Category 1 systems.	Go to box 7
7	No, Firewall Y denies Workstation X from initiating a connection to the Citrix Server and Server Z. **Note:** No listening network ports on dumb terminal.	Go to box 9
9	No, Firewall Y denies the Citrix Server and Server Z from initiating a connection to Workstation X. **Note:** The dumb terminal is only allowed to communicate with Citrix Server via encrypted session.	Go to box 11
11	No, Workstation X does not directly or indirectly administer Category 1 devices.	Go to box 13
13	Therefore Workstation X is a Category 3 device.	**Category 3**

9.5 Scenario 5: Segmented general user workstation on corporate network segment



The device in question is a general user workstation on the corporate network that does not store, process, or transmit CHD. The workstation also does not access any resources in the CDE.

Workstation X is a Customer Service Representative workstation used to process credit card payments.

Server Z is a server running a payment application processing credit card payment transactions.

Location of device: Position B

Network Access Controls:

- Firewall Y allows CHD transaction data between Workstation X and Server Z
- Firewall Y denies all other traffic between Workstation X and Server Z
- Firewall Y denies all traffic between General User Workstation in Position B and Server Z
- Firewall Y denies all traffic between General User Workstation in Position B and Workstation X.
- No other network access controls are in place.

9.5.1 Decision tree for Firewall Y

Box	Answer for Box	Outcome
1	Yes, Firewall Y processes, stores or transmits CHD.	Go to box 2
2	Therefore Firewall Y is a Category 1a device.	**Category 1a**

9.5.2 Decision Tree for Server Z

Box	Answer for Box	Outcome
1	Yes, Server Z processes, stores or transmits CHD.	Go to box 2
2	Therefore Server Z is a Category 1a device.	**Category 1a**

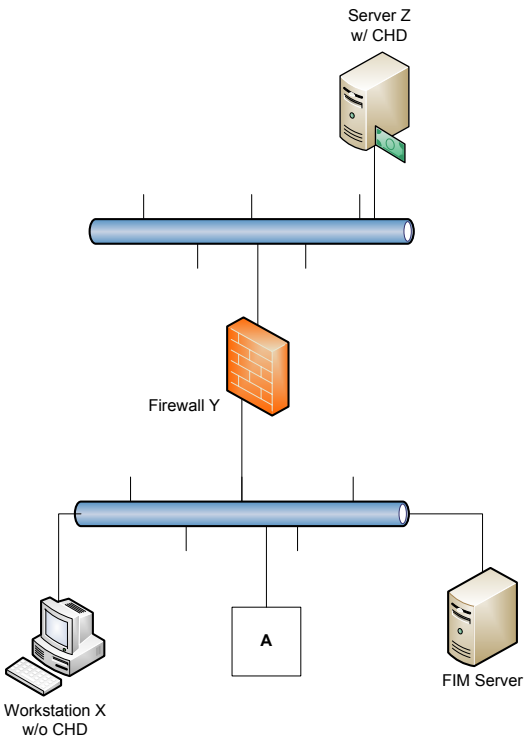
9.5.3 Decision Tree for Workstation X

Box	Answer for Box	Outcome
1	Yes, Workstation X process, stores or transmits CHD.	Go to box 2
2	Therefore Workstation X is a Category 1a device.	**Category 1a**

9.5.4 Decision Tree for General User Workstation in position B

Box	Answer for Box	Outcome
1	No, General User Workstation does not process, store or transmit CHD.	Go to box 3
3	Yes, General User Workstation is isolated from both Workstation X and Server Z . **Note:** The access control lists on Firewall Y contain the infectious nature of the firewall.	Go to box 4
4	No, General User Workstation does not provide services to Workstation X or Server Z.	Go to box 7
7	No, Firewall Y denies General User Workstation from initiating a connection to both Workstation X and Server Z.	Go to box 9
9	No, Firewall Y denies both Workstation X and Server Z and from initiating a connection to General User Workstation.	Go to box 11
11	No, Workstation X does not directly or indirectly administer Category 1 devices.	Go to box 13
13	Therefore Workstation X is a Category 3 device.	**Category 3**

9.6 Scenario 6: General user workstation on corporate network segment



The device in question is a general user workstation on the corporate network in Position A that does not access to CHD and does not access any resources in the CDE.

Workstation X is an administrative workstation used to manage the File Integrity Monitoring (FIM) server. It does not have access to CHD or any resources in the CDE.

The File Integrity Monitoring (FIM) server provides FIM services to Server Z with CHD.

Location of device: Position A

Network Access Controls:

- Firewall Y allows FIM traffic data between FIM Server and Server Z.
- Firewall Y denies all traffic between Workstation X and Server Z.
- Firewall Y denies all traffic between Workstation in Position A and Server Z.
- No other network access controls are in place.

9.6.1 Decision tree for Firewall Y

Box	Answer for Box	Outcome
1	No, Firewall Y does not process, store or transmit CHD.	Go to box 3
3	Yes, Firewall Y provides access controls that restrict network connectivity.	Go to box 4
4	Yes, Firewall Y provides security functionality to a .Category 1 device.	Go to box 5
5	Therefore Firewall Y is a Category 2a device.	**Category 2a**

9.6.2 Decision Tree for Server Z

Box	Answer for Box	Outcome
1	Yes, Server Z process, store or transmit CHD.	Go to box 2
2	Therefore Server Z is a Category 1a device.	**Category 1a**

9.6.3 Decision tree for FIM Server

Box	Answer for Box	Outcome
1	No, FIM Server does not process, store or transmit CHD.	Go to box 3
3	Yes, access controls are in place to control access between FIM Server and Category 1 devices.	Go to box 4
4	Yes, FIM Server provides security services to Server Z.	Go to box 5
5	Therefore FIM Server is a Category 2a device.	**Category 2a**

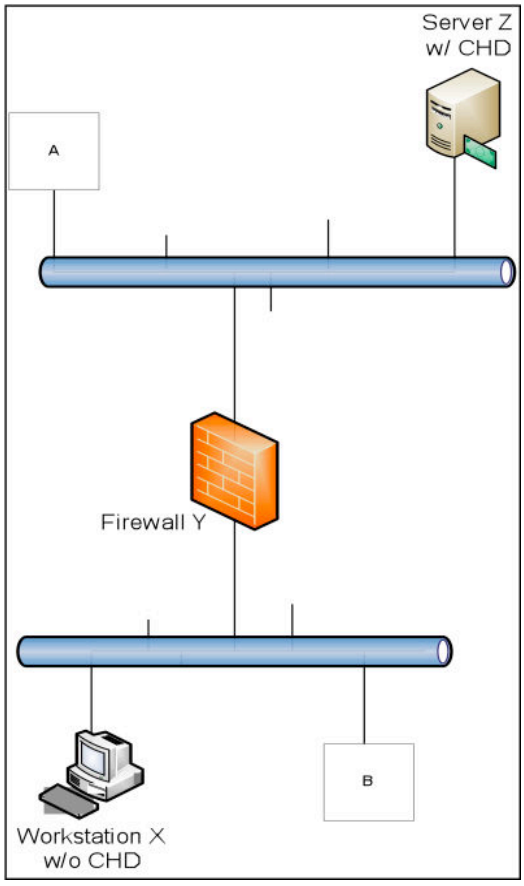
9.6.4 Decision Tree for Workstation X

Box	Answer for Box	Outcome
1	No, Workstation X does not process, store or transmit CHD.	Go to box 3
3	Yes, Workstation X is isolated from Category 1 devices.	Go to box 4
4	No, Workstation X does not provide security services to Category 1 devices.	Go to box 7
7	No, Workstation X does not have the ability to initiate a connection to a Category 1 device.	Go to box 9
9	No, a Category 1 device cannot initiate a connection to Workstation X.	Go to box 11
11	No, Workstation X does not directly or indirectly administer Category 1 devices.	Go to box 13
13	Therefore Workstation X is a Category 3 device.	**Category 3**

9.6.5 Decision Tree for General User Workstation in position A

Box	Answer for Box	Outcome
1	No, General User Workstation does not process, store or transmit CHD.	Go to box 3
3	Yes, General User Workstation is isolated from Category 1 devices.	Go to box 4
4	No, General User Workstation does not provide security services to Category 1 devices.	Go to box 7
7	No, Firewall Y denies General User Workstation from initiating a connection to Category 1 devices.	Go to box 9
9	No, Firewall Y denies Server Z from initiating a connection to General User Workstation.	Go to box 11
11	No, Workstation X does not directly or indirectly administer Category 1 devices.	Go to box 13
13	General User Workstation is a Category 3 device.	**Category 3**

9.7 Scenario 7: Patch Management Server on corporate network segment



The device in question is a patch management server on the corporate network that manages patching for workstations on the corporate network. The patch management server does not access to CHD and does not access any resources in the CDE.

Workstation X is an administrative workstation used to manage the operating system and application on Server Z in the CDE but does not have access to CHD.

Server Z is a database server in the CDE that stores CHD.

Location of device: Position A

Network Access Controls:

- Firewall Y allows RDP traffic from Workstation X and Server Z.
- Firewall Y denies all traffic between Patch Management Server in Position A and Server Z.
- No other network access controls are in place.

9.7.1 Decision tree for Firewall Y

Box	Answer for Box	Outcome
1	No, Firewall Y does not process, store or transmit CHD.	Go to box 3
3	Yes, Firewall Y provides access controls that restrict network connectivity.	Go to box 4
4	Yes, Firewall Y provides security functionality to a Category 1 device.	Go to box 5
5	Therefore Firewall Y is a Category 2a device.	**Category 2a**

9.7.2 Decision Tree for Server Z

Box	Answer for Box	Outcome
1	Yes, Server Z processes, stores or transmits CHD.	Go to box 2
2	Therefore Server Z is a Category 1a device.	**Category 1a**

9.7.3 Decision Tree for Workstation X

Box	Answer for Box	Outcome
1	No, Workstation X does not process, store or transmit CHD.	Go to box 3
3	Yes, Firewall Y provides access controls that restrict network connectivity to Category 1 devices.	Go to box 4
4	No, Workstation X does not provide security services to Category 1 devices.	Go to box 7
7	Yes, Workstation X has the ability to initiate a connection to a Category 1 device.	Go to box 8
8	Therefore Workstation X is a Category 2b device.	**Category 2b**

9.7.4 Decision Tree for Patch Management Server in position A

Box	Answer for Box	Outcome
1	No, Patch Management Server does not process, store or transmit CHD.	Go to box 3
3	Yes, Patch Management Server is isolated from Category 1 devices.	Go to box 4
4	No, General User Workstation does not provide security services to Category 1 devices.	Go to box 7
7	No, Firewall Y denies the Patch Management Server from initiating a connection to Category 1 devices.	Go to box 9
9	No, Firewall Y denies Server Z from initiating a connection to General User Workstation.	Go to box 11
11	No, Workstation X does not directly or indirectly administer Category 1 devices.	Go to box 13
13	Therefore General User Workstation is a Category 3 device.	**Category 3**

10 Appendix B: Frequently Asked Questions

10.1 Can a system component end up in more than one scoping category?

No. The scoping categories are all mutually exclusive, so a system component can only belong to one category or sub-category.

10.2 Why are there so many Category 2 sub-categories, if they are all in the scope of assessment?

The Category 2a, 2b, 2c and 2x each have a different type of risk they pose to cardholder data, which an organization can use to evaluate the necessity and applicability of PCI DSS controls.

10.3 Why doesn't the Toolkit specify which PCI DSS control requirements apply for each sub-category?

The Toolkit states that all applicable PCI DSS controls are required for Category 1 and 2a system components and that no PCI DSS controls are required for Category 3 system components.

However, because every organization and CDE is unique, it would impossible to provide more specific guidance on which PCI DSS controls are required for every type of Category 2b, 2c and 2x system component. The Toolkit does provide the basis for an organization and its assessor to discuss what the relevant risks are and the controls required to mitigate them.

10.4 Is it true that Scenario 4 concludes that a view-only dumb terminal that displays CHD is not a Category 2 device, but is a Category 1 device?

Yes. Because cardholder data is being entered into the dumb terminal, it is "processing" cardholder data and is therefore subject to all of the PCI DSS requirements.

As a Category 1 system component, all other system components that do not have isolation or controlled access will become "infected," causing them to become a Category 1b system component.

In order to restrict other workstations on the same network from being "infected," the dumb terminals must be isolated (e.g., using a host-based or network-based firewalls, etc.). Scenario 4 states that no listening ports are open on the dumb terminal. The firewall enforces this restriction.

10.5 I have a Category 2 system component that is "connected to" the CDE, but it does not pose any risk to the CDE. Can I now make it Category 3 system component?

No. The system component is Category 2 because it is has controlled access to the CDE. Consequently, an organization changing the system component to Category 3 violates the Toolkit category definitions and would result in a scoping error.

However, if through a risk assessment, an organization confirms that there are sufficient controls that adequately mitigate the risk of compromising the CDE, then no additional controls are required. The results of the risk assessment must be documented to present a rationalization for controls applied to the specific Category 2 device. The assessor then must validate your risk assessment and confirm the control rationalization.

Note that Category 2a system components require all applicable DSS controls. If it can be rationalized that not all DSS controls are required, then it is likely that the system component is not actually Category 2a.

10.6 The Toolkit repeatedly states that for Category 2x system components, such as administrative workstations, not all PCI DSS controls are applicable or necessary. How does one determine which controls are required?

Note: the recommendations in this FAQ apply to Category 2x system components only if they are indeed Category 2x. If any Category 2x device accesses cardholder data in any way, it is actually a Category 1a device.

Every organization and CDE is unique, as are the system components that comprise the scope of assessment. However, the following thought process might be used to determine the PCI DSS controls required for Category 2x devices:

Identification of risks: The primary risk posed by Category 2x system components is that if those devices are compromised, they could allow unauthorized access into the Category 1 devices being managed.

Understanding reliance on controls: The organization concludes that it can rely on the controls that provide isolation and controlled network access, limiting all Category 2x devices to their management functions. Furthermore, the organization determines that all required PCI DSS controls on all Category 1, 2a, 2b and 2c systems (i.e., everything else in the scope of assessment) are designed and operating effectively.

Selection of controls: The organization would then look at the twelve broad PCI DSS control categories (and again, note that this is just an illustrative example: any organization will actually have to perform their own analysis to match their situation) as shown in the following table.

The organization would then evaluate the twelve PCI DSS control categories (i.e., sections) to determine applicability and necessity of the control requirements to mitigate the risks documented above, as shown in the following table:

Note: this is provided for illustrative purposes only.

PCI DSS Section	**Result of Organization X's Evaluation of a Specific Type of Category 2x Administrative Workstation**
1. Install and maintain a firewall configuration to protect cardholder data.	This section is not applicable because this workstation is not a firewall.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.	This section is applicable, but will be enforced through the standard corporate build process.
3. Protect stored cardholder data.	This section is not applicable because no cardholder data is stored on this workstation.
4. Encrypt transmission of cardholder data across open, public networks.	This section is not applicable because this workstation does not transmit cardholder data.
5. Use and regularly update anti-virus software or programs.	This section is applicable to all in-scope systems commonly affected by malware, which includes this workstation. This will be enforced through the corporate build process.
6. Develop and maintain secure systems and applications.	This section is applicable to all in-scope systems, including this workstation. Particular attention should be paid to the patching requirements in PCI DSS Section 6. This will be enforced through the corporate build process.
7. Restrict access to cardholder data by business need to know.	This section is not applicable because this workstation does not store, process or transmit cardholder data.
8. Assign a unique ID to each person with computer access.	This section is applicable, but will be enforced through the corporate identity management process.
9. Restrict physical access to cardholder data.	This section is not applicable because this workstation does not store, process or transmit cardholder data.
10. Track and monitor all access to network resources and cardholder data.	This section is applicable, but note that any event only needs to be captured once, and that it can be captured by any device in the infrastructure (PCI FAQ 9236). For instance, when an administrator uses this workstation to configure a firewall, such activities may be best logged from the firewall itself. This will be enforced through the

	corporate build process.
11. Regularly test security systems and processes.	This section is applicable and will be enforced through the corporate vulnerability management process.
12. Maintain a policy that addresses information security for all personnel.	This section is applicable and will be enforced through the corporation information security management system.

For the example workstation evaluated above, the organization may then conclude that it can fulfill the Category 2x control requirements above through an effective anti-virus deployment, patch management and workstation build standard.