



American National Standard for Financial Services

ANSI X9.111–2011 (R2017)

Penetration Testing within the Financial Services Industry



Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: January 14, 2011

Date Reaffirmed: April 14, 2017

American National Standards Institute

American National Standards, Technical Reports and Guides developed through the Accredited Standards Committee X9, Inc., are copyrighted. Copying these documents for personal or commercial use outside X9 membership agreements is prohibited without express written permission of the Accredited Standards Committee X9, Inc. For additional information please contact ASC X9, Inc., 275 West Street, Suite 107, Annapolis, MD 21401.

Contents

	Page
Foreword	v
Introduction	vi
1 Scope.....	14
2 Normative References	16
3 Terms and Definitions	16
3.1 Target of Evaluation.....	16
3.2 Penetration Test.....	16
3.3 Vulnerability Scan	16
4 Symbols and Abbreviated Terms	16
5 Significance of Penetration Test Activity	18
5.1 Broad Description	18
5.2 Penetration Testing as a Component of Risk Identification and Assessment	18
5.3 Limitations of Penetration Testing	20
5.3.1 Introduction	20
5.3.2 Time	20
5.3.3 Testing Scope / Availability of Target	20
5.3.4 Target Selection	20
5.3.5 Tester Qualifications.....	21
5.3.6 Penetration Testing Period and Meaning of Results.....	21
6 Penetration Testing Framework	22
6.1 Introduction / Overview	22
6.2 Test Activities	23
6.2.1 Specification of Penetration Test	23
6.2.2 Engagement Guidelines	23
6.2.3 Penetration Test Activity	23
6.2.4 Engagement Reporting.....	23
6.2.5 Remediation	24
7 Specification of Penetration Test	24
7.1 Introduction	24
7.2 Penetration Testing Parameters.....	25
7.2.1 TOE Selection	25
7.2.2 Logical Location of Tester	26
7.2.3 Tester Prior Knowledge.....	28
7.2.4 Test Intrusiveness.....	31
7.2.5 TOE System Status	32
7.2.6 Target Response Team Level of Awareness.....	33
7.3 Penetration Test Levels.....	34
8 Engagement Considerations	35
8.1 Introduction	35
8.2 Mutual Non-Disclosure Agreement	35
8.3 Engagement – Detailed Scope of Work Specifically Defining Activities.....	36
8.3.1 Overview	36
8.3.2 Rules of Engagement	36
8.3.3 Authorization/Confirmation Agreement (use of IPs and Timeframe)	37
8.3.4 Technical Points of Contact.....	37
8.4 Terms and Conditions and other Legal Aspects	37
9 Penetration Test Activity	39

9.1	Test Introduction.....	39
9.2	Passive Discovery.....	40
9.2.1	Passive Discovery Introduction	40
9.2.2	Public Information Gathering	40
9.2.3	Customer Provided Information	40
9.3	Active Discovery	40
9.3.1	Active Discovery Introduction	40
9.3.2	System Scanning	41
9.3.3	Application Centric Information Gathering	42
9.3.4	Customized Application / Source Code Review	42
9.3.5	Traffic Monitoring.....	42
9.3.6	Evasion Testing.....	42
9.3.7	Social Engineering.....	42
9.3.8	Physical Intrusion	42
9.4	Attack Planning	43
9.5	Attacks	43
9.5.1	Attack Introduction	43
9.5.2	Logical Attack.....	43
9.5.3	Physical Attack.....	44
9.5.4	Procedural Attack	44
10	Reporting	45
10.1	Delivery	45
10.2	Recommended Content.....	45
10.2.1	Executive Summary	45
10.2.2	Tester Profile and Qualifications	45
10.2.3	Test Objectives and Scope	45
10.2.4	Limitations of the Penetration Test.....	45
10.2.5	Test Details	45
10.2.6	Test Results/Findings	46
10.2.7	Industry Baseline Analysis	46
10.2.8	Remediation.....	46
10.3	Other Recommendations	48
11	Penetration Testing Support Activities.....	48
11.1	Introduction	48
11.2	Know Your Tools.....	48
	Annex A (informative) Attack Examples.....	49
A.1	Introduction	49
A.2	Network Attacks	49
A.3	Web Application Attacks	49

Figures

Figure 1 – Security Evaluation Process	18
Figure 2 – Security Evaluation and System Development Life Cycle.....	19
Figure 3 – Penetration Test Framework - Client Perspective	22
Figure 4 – Tester Logical Location for TOE Within Internal Network.....	26
Figure 5 – Tester Logical Location for TOE Within DMZ	27
Figure 6 – Tester Logical Location for a TOE with Related Component	28
Figure 7 – Penetration Test Methodology.....	39

Tables

Table 1 – TOE Examples	25
Table 2 – Penetration Testing and Tester Knowledge.....	30
Table 3 – Penetration Test Level of Intrusiveness.....	31
Table 4 – TOE Status.....	32
Table 5 – Response Team Awareness	33
Table 6 – Penetration Testing Levels	34
Table 7 – Public Information Gathering Techniques.....	40

Foreword

Approval of an American National Standard requires verification by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretation should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken to reaffirm, revise, or withdraw this standard no later than five years from the date of approval.

Published by

Accredited Standards Committee X9, Incorporated
Financial Industry Standards
275 West Street, Suite 107
Annapolis, MD 21401 USA
X9 Online <http://www.x9.org>

Copyright © 2017 ASC X9, Inc.

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without prior written permission of the publisher. Published in the United States of America.

Introduction

Penetration testing attempts to gather information about a network system and its associated security controls through a non-malicious attempt to circumvent, subvert, or defeat the Security Controls protecting the information assets of a company or other organization. The purpose of such testing is to discover and report vulnerabilities and misconfigurations in the design or implementation of such controls, so that flaws can be corrected, risks evaluated accurately, and the organization's overall security posture strengthened.

Penetration (pen) tests have become standard practice for many financial service organizations including financial institutions, payment processors and merchants. Further, pen test are often a requirement for state bank examiners and industry practices such as the Payment Card Industry (PCI) Data Security Standards (DSS). However, pen testing today often yields varying results due to differences in the level and scope of testing, reporting detail, quality of service, and professional standards of those organizations providing the penetration testing service. For penetration test results to be consistent, comparable, actionable, and provide tactical and strategic benefit to financial service organizations, it is imperative that accepted rules of engagement be followed and that penetration testing processes be based on defined practices, processes, and procedures.

The goals and intended results of this standard are as follows:

- To provide a standard specification of penetration testing, its appropriate application, value, and limitations.
- To specify standards for conducting penetration testing to produce results which are industry consistent, comparable, repeatable, actionable, traceable, and useful to the organization under evaluation.
- To provide common terms to facilitate communication pertaining to penetration testing and documentation of penetration test results, including a model format.
- To define parameters that decision makers can use to specify a penetration test.
- To provide financial organizations and penetration testers with guidelines for selecting and engaging penetration testing services.

Financial service organizations can benefit from this standard by understanding the rules of engagement for specifying, negotiating and accepting a penetration test with a penetration test service provider. Likewise penetration test service providers can benefit from this standard by following the rules of engagement for proposing, negotiating and providing a penetration test with a financial services organization. Further, third parties such as security assessors, auditors and bank examiners can benefit from this standard by relying on the rules of engagement for reviewing, interpreting and accepting penetration test reports. The financial services industry overall will benefit as a whole from this standard with a consistent, comparable and actionable penetration tests, results and reports.

Suggestions for the improvement or revision of this Standard are welcome. They should be sent to the X9 Committee Secretariat, Accredited Standards Committee X9, Inc., Financial Industry Standards, 275 West Street, Suite 107, Annapolis, MD 21401 USA.

This Standard was processed and registered for submittal to ANSI by the Accredited Standards Committee on Financial Services, X9. Committee approval of the Standard does not necessarily imply that all the committee members voted for its approval.

At the time this Standard was published, the X9 committee had the following members:

Roy DeCicco, X9 Chairman
Vincent DeSantis, X9 Vice-Chairman
Steve Stevens, Executive Director
Janet Busch, Program Manager

<i>Organization Represented</i>	<i>Representative</i>
ACI Worldwide	Doug Grote
ACI Worldwide	Cindy Rink
American Bankers Association	Tom Judd
American Bankers Association	Diane C. Poole
American Express Company.....	Ted Peirce
Apriva	Len Sutton
Bank of America.....	Andi Coleman
Bank of America.....	Daniel Welch
Certicom Corporation.....	Daniel Brown
Citigroup, Inc.	Mark Clancy
Citigroup, Inc.	Michael Knorr
Citigroup, Inc.	Karla McKenna
Citigroup, Inc.	Chii-Ren Tsai
Citigroup, Inc.	Gary Word
CUSIP Service Bureau.....	Gerard Faulkner
CUSIP Service Bureau.....	James Taylor
Deluxe Corporation	John FitzPatrick
Deluxe Corporation	Ralph Stlop
Diebold, Inc.	Anne Bayonet
Diebold, Inc.	Bruce Chapa
Discover Financial Services	Dave Irwin
Discover Financial Services	Deana Morrow
Federal Reserve Bank	Deb Hjortland
Federal Reserve Bank	Claudia Swendseid
First Data Corporation.....	Todd Nuzum
First Data Corporation.....	Rick Van Luvender
Fiserv.....	Bud Beattie
Fiserv.....	Kevin Finn
Fiserv.....	Lori Hood
Fiserv.....	Dan Otten
Fiserv.....	Skip Smith
FIX Protocol Ltd	Jim Northey
FSTC, Financial Services Technology Consortium	Christine Nautiyal
FSTC, Financial Services Technology Consortium	Daniel Schutzer
FSTC, Financial Services Technology Consortium	Michael Versace
Harland Clarke	John McCleary
Hewlett Packard	Larry Hines
Hewlett Packard	Gary Lefkowitz
IBM Corporation	Todd Arnold
IFSA	Dexter Holt
IFSA	Dan Taylor
Ingenico	Alexandre Hellequin
Ingenico	Steve McKibben
Ingenico	John Spence
J.P. Morgan Chase & Co	Robert Blair
J.P. Morgan Chase & Co	Roy DeCicco
J.P. Morgan Chase & Co	Edward Koslow

J.P. Morgan Chase & Co	Jackie Pagan
J.P. Morgan Chase & Co	Charita Wamack
J.P. Morgan Chase & Co	Glenn Benson
Key Innovations.....	Scott Spiker
Key Innovations.....	Paul Walters
KPMG LLP	Mark Lundin
MagTek, Inc.	Terry Benson
MagTek, Inc.	Jeff Duncan
MagTek, Inc.	Mimi Hart
MasterCard International.....	Mark Kamers
Merchant Advisory Group	Dodd Roberts
Metavante Image Solutions.....	Stephen Gibson-Saxty
NACHA The Electronic Payments Association	Nancy Grant
National Association of Convenience Stores	Michael Davis
National Association of Convenience Stores	Alan Thiemann
National Security Agency	Paul Timmel
NCR Corporation.....	David Norris
NCR Corporation.....	Steve Stevens
RMG-SWIFT.....	Jamie Shay
RouteOne	Mark Leonard
SWIFT/Pan Americas	Jean-Marie Eloy
SWIFT/Pan Americas	James Wills
The Clearing House	Vincent DeSantis
U.S. Bank	Brian Fickling
U.S. Bank	Gregg Walker
University Bank	Stephen Ranzini
University Bank	Michael Talley
VeriFone, Inc.	David Ezell
VeriFone, Inc.	Dave Faoro
VeriFone, Inc.	Allison Holland
VeriFone, Inc.	Doug Manchester
VeriFone, Inc.	Brad McGuinness
VeriFone, Inc.	Brenda Watlington
VISA	Brian Hamilton
VISA	John Sheets
VISA	Richard Sweeney
Wells Fargo Bank	Andrew Garner
Wells Fargo Bank	Mike McCormick
Wells Fargo Bank	Mike Rudolph
Wells Fargo Bank	Mark Tiggas
Wincor Nixdorf Inc.....	Ramesh Arunashalam
XBRL US, Inc.	Mark Bolgiano

At the time this standard was approved, the X9F subcommittee on Data and Information Security had the following members:

Richard Sweeney, X9F Chair
Sandra Lambert, X9F Vice Chair

<i>Organization Represented</i>	<i>Representative</i>
ACI Worldwide	Doug Grote
ACI Worldwide	Julie Samson
ACI Worldwide	Sid Sidner
American Bankers Association	Tom Judd
American Express Company.....	William J. Gray

American Express Company.....	Vicky Sammons
Bank of America.....	Daniel Welch
Bank of America.....	Andi Coleman
Certicom Corporation	Sandra Lambert
Certicom Corporation	Daniel Brown
Citigroup, Inc.	Mark Clancy
Citigroup, Inc.	Susan Rhodes
Citigroup, Inc.	Chii-Ren Tsai
Communications Security Establishment.....	Jonathan Hammell
Communications Security Establishment.....	Alan Poplove
Cryptographic Assurance Services	Jeff Stapleton
Cryptographic Assurance Services	Ralph Poore
CUSIP Service Bureau.....	James Taylor
CUSIP Service Bureau.....	Scott Preiss
DeLap LLP	Steve Case
DeLap LLP	Darlene Kargel
Deluxe Corporation	John FitzPatrick
Deluxe Corporation	Ralph Stlop
Depository Trust and Clearing Corporation	Robert Palatnick
Diebold, Inc.	Bruce Chapa
Discover Financial Services.....	Jordan Schaefer
Entrust, Inc.	Sharon Boeyen
Entrust, Inc.	Tim Moses
Entrust, Inc.	Miles Smid
Federal Reserve Bank	Deb Hjortland
Federal Reserve Bank	Claudia Swendseid
Ferris and Associates, Inc.....	J. Martin Ferris
First Data Corporation.....	Marc Madison
First Data Corporation.....	Lisa Curry
Fiserv.....	Mary Bland
Fiserv.....	Kevin Finn
Fiserv.....	Dennis Freiburg
Fiserv.....	Dan Otten
Fiserv.....	Bud Beattie
GEOBRIDGE Corporation.....	Jason Way
Harland Clarke	Joseph Filer
Harland Clarke.	John Petrie
Heartland Payment Systems.....	Roger Cody
Heartland Payment Systems.....	Glenda Preen
Hewlett Packard	Susan Langford
Hewlett Packard	Gary Lefkowitz
Hewlett Packard	Larry Hines
Hypercom	Isabel Bardsley-Garcia
Hypercom	Gary Zempich
IBM Corporation	Todd Arnold
IBM Corporation	Michael Kelly
InfoGard Laboratories, Inc.	Ken Kolstad
InfoGard Laboratories, Inc.	Doug Biggs
Ingenico.....	John Spence
J.P. Morgan Chase & Co	Robert Blair
J.P. Morgan Chase & Co	Kathleen Krupa
J.P. Morgan Chase & Co	Donna Meagher
J.P. Morgan Chase & Co	Jackie Pagan
J.P. Morgan Chase & Co	Edward Koslow
K3DES LLC.....	Azie Amini
Key Innovations.....	Scott Spiker

Key Innovations.....	Paul Walters
KPMG LLP	Mark Lundin
MagTek, Inc.	Terry Benson
MagTek, Inc.	Jeff Duncan
MagTek, Inc.	Mimi Hart
Marriott International	Jeff Lolley
MasterCard International.....	Jeanne Moore
MasterCard International.....	Michael Ward
Merchant Advisory Group	Dodd Roberts
National Institute of Standards and Technology	Lily Chen
National Institute of Standards and Technology	Elaine Barker
National Security Agency	Mike Boyle
National Security Agency	Paul Timmel
NCR Corporation.....	Charlie Harrow
NCR Corporation.....	Ali Lowden
NCR Corporation.....	Ron Rogers
NCR Corporation.....	Steve Stevens
NCR Corporation.....	Ally Whytock
NCR Corporation.....	David Norris
Pitney Bowes, Inc.....	Leon Pintsov
Pitney Bowes, Inc.....	Rick Ryan
RBS Group	Dan Collins
Rosetta Technologies	Jim Maher
Rosetta Technologies	Paul Malinowski
RSA, The Security Division of EMC.....	Steve Schmalz
Security Innovation.....	Mark Etzel
Security Innovation.....	William Whyte
STAR.....	Scott Quinn
STAR.....	Lilik Kazaryan
Surety, Inc.	Tom Klaff
Surety, Inc.	Dimitrios Andivahis
TECSEC Incorporated	Jay Wack
TECSEC Incorporated	Ed Scheidt
Thales e-Security, Inc.	Jose Diaz
Thales e-Security, Inc.	James Torjussen
The Clearing House	Henry Farrar
The Clearing House	Vincent DeSantis
The Clearing House	Susan Long
U.S. Bank	Peter Skirvin
U.S. Bank	Robert Thomas
Unisys Corporation.....	Navnit Shah
Unisys Corporation.....	David J. Concannon
University Bank	Stephen Ranzini
University Bank	Michael Talley
VeriFone, Inc.	David Ezell
VeriFone, Inc.	Dave Faoro
VeriFone, Inc.	Doug Manchester
VeriFone, Inc.	Brad McGuinness
VeriFone, Inc.	Brenda Watlington
VeriFone, Inc.	John Barrowman
VISA	John Sheets
VISA	Richard Sweeney
Voltage Security, Inc.	Terence Spies
Voltage Security, Inc.	Luther Martin
Wells Fargo Bank	Mike McCormick
Wells Fargo Bank	Ruven Schwartz

Wells Fargo Bank Mark Tiggas
Wincor Nixdorf Inc Michael Nolte

Under ASC X9, Inc. procedures, a working group may be established to address specific segments of work under the ASC X9 Committee or one of its subcommittees. A working group exists only to develop standard(s) or guideline(s) in a specific area and is then disbanded. The individual experts are listed with their affiliated organizations. However, this does not imply that the organization has approved the content of the standard or guideline. (Note: Per X9 policy, company names of non-member participants are listed only if, at the time of publication, the X9 Secretariat received an original signed release permitting such company names to appear in print.)

The X9F4 Cryptographic Protocols and Application Security group which developed this standard had the following members:

At the time this standard was approved, the X9F4 Cryptographic Protocol and Application Security working group which developed this standard had the following active members:

Jeff Stapleton, X9F4 Chair
Sandra Lambert, X9F4 Vice Chair
Douglas Biggs, X9.111 Editor

<i>Organization Represented</i>	<i>Representative</i>
ACI Worldwide	Doug Grote
ACI Worldwide	Julie Samson
ACI Worldwide	Sid Sidner
American Bankers Association	Tom Judd
American Express Company.....	William J. Gray
American Express Company.....	Vicky Sammons
Bank of America.....	Daniel Welch
Bank of America.....	Andi Coleman
Certicom Corporation	Sandra Lambert
Certicom Corporation	Daniel Brown
Citigroup, Inc.	Mark Clancy
Citigroup, Inc.	Susan Rhodes
Citigroup, Inc.	Chii-Ren Tsai
Communications Security Establishment.....	Jonathan Hammell
Communications Security Establishment.....	Alan Poplove
Cryptographic Assurance Services	Jeff Stapleton
Cryptographic Assurance Services	Ralph Poore
CUSIP Service Bureau.....	James Taylor
CUSIP Service Bureau.....	Scott Preiss
DeLap LLP	Steve Case
DeLap LLP	Darlene Kargel
Deluxe Corporation	John FitzPatrick
Deluxe Corporation	Ralph Stolp
Depository Trust and Clearing Corporation	Robert Palatnick
Diebold, Inc.	Bruce Chapa
Discover Financial Services	Jordan Schaefer
Entrust, Inc.	Sharon Boeyen
Entrust, Inc.	Tim Moses
Entrust, Inc.	Miles Smid
Federal Reserve Bank	Deb Hjortland
Federal Reserve Bank	Claudia Swendseid
Ferris and Associates, Inc.....	J. Martin Ferris
First Data Corporation.....	Marc Madison

First Data Corporation	Lisa Curry
Fiserv	Mary Bland
Fiserv	Kevin Finn
Fiserv	Dennis Freiburg
Fiserv	Dan Otten
Fiserv	Bud Beattie
GEOBRIDGE Corporation	Jason Way
Harland Clarke	Joseph Filer
Harland Clarke	John Petrie
Heartland Payment Systems	Roger Cody
Heartland Payment Systems	Glenda Preen
Hewlett Packard	Susan Langford
Hewlett Packard	Gary Lefkowitz
Hewlett Packard	Larry Hines
Hypercom	Isabel Bardsley-Garcia
Hypercom	Gary Zempich
IBM Corporation	Todd Arnold
IBM Corporation	Michael Kelly
InfoGard Laboratories, Inc.	Ken Kolstad
InfoGard Laboratories, Inc.	Doug Biggs
Ingenico	John Spence
J.P. Morgan Chase & Co	Robert Blair
J.P. Morgan Chase & Co	Kathleen Krupa
J.P. Morgan Chase & Co	Donna Meagher
J.P. Morgan Chase & Co	Jackie Pagan
J.P. Morgan Chase & Co	Edward Koslow
K3DES LLC	Azie Amini
Key Innovations	Scott Spiker
Key Innovations	Paul Walters
KPMG LLP	Mark Lundin
MagTek, Inc.	Terry Benson
MagTek, Inc.	Jeff Duncan
MagTek, Inc.	Mimi Hart
Marriott International	Jeff Lolley
MasterCard International	Jeanne Moore
MasterCard International	Michael Ward
Merchant Advisory Group	Dodd Roberts
National Institute of Standards and Technology	Lily Chen
National Institute of Standards and Technology	Elaine Barker
National Security Agency	Mike Boyle
National Security Agency	Paul Timmel
NCR Corporation	Charlie Harrow
NCR Corporation	Ali Lowden
NCR Corporation	Ron Rogers
NCR Corporation	Steve Stevens
NCR Corporation	Ally Whytock
NCR Corporation	David Norris
Pitney Bowes, Inc.	Leon Pintsov
Pitney Bowes, Inc.	Rick Ryan
RBS Group	Dan Collins
Rosetta Technologies	Jim Maher
Rosetta Technologies	Paul Malinowski
RSA, The Security Division of EMC	Steve Schmalz
Security Innovation	Mark Etzel
Security Innovation	William Whyte
STAR	Scott Quinn

STAR.....	Lilik Kazaryan
Surety, Inc.....	Tom Klaff
Surety, Inc.....	Dimitrios Andivahis
TECSEC Incorporated	Jay Wack
TECSEC Incorporated	Ed Scheidt
Thales e-Security, Inc.....	Jose Diaz
Thales e-Security, Inc.....	James Torjussen
The Clearing House	Henry Farrar
The Clearing House	Vincent DeSantis
The Clearing House	Susan Long
U.S. Bank	Peter Skirvin
U.S. Bank	Robert Thomas
Unisys Corporation.....	Navnit Shah
Unisys Corporation.....	David J. Concannon
University Bank	Stephen Ranzini
University Bank	Michael Talley
VeriFone, Inc.....	David Ezell
VeriFone, Inc.....	Dave Faoro
VeriFone, Inc.....	Doug Manchester
VeriFone, Inc.....	Brad McGuinness
VeriFone, Inc.....	Brenda Watlington
VeriFone, Inc.....	John Barrowman
VISA	John Sheets
VISA	Richard Sweeney
Voltage Security, Inc.....	Terence Spies
Voltage Security, Inc.....	Luther Martin
Wells Fargo Bank.....	Mike McCormick
Wells Fargo Bank.....	Ruven Schwartz
Wells Fargo Bank.....	Mark Tiggas
Wincor Nixdorf Inc.....	Michael Nolte

1 Scope

This standard specifies recommended processes for conducting penetration testing with financial service organizations. This standard describes a framework for specifying, describing and conducting penetration testing, and then relating the results of the penetration testing. This standard allows an entity interested in obtaining penetration testing services to identify the objects to be tested, specify a level of testing to occur, and to set a minimal set of testing expectations.

Included in this standard are:

- A conceptual framework for describing penetration testing, including
 - Roles and Responsibilities of participants
 - Types of penetration test
 - A generalized penetration testing cycle
 - General testing methodologies / techniques
 - Limitations of Penetration testing
 - Ranking of methodologies, bases of testing effort (testing levels)
- Engagement and scope of work considerations
- Test Report guidelines
- Testing requirements
 - Security of the testing environment
 - General practices and methodologies
 - Tester expertise

The following areas are explicitly out of the scope of this document as they highly depend on the specifics of the components/products used by the system (e.g., operating system, software applications, and machine architecture) and/or tester expertise, or the activity is not directly related to the process of penetration testing and does not fit the test framework:

- Local configuration audits
- Forensic analysis (e.g., evaluation of targets, review of local forensic evidence of penetration, chains of evidence.). Forensics involves detecting and investigating evidence of a real attack to assess the damage and apprehend the attacker. Penetration testing involves the discovery of vulnerabilities that could be used to attack the system.
- Specific exploit techniques
- Interpretation of results (e.g., pass/fail rating)
- Validation of penetration test service providers
- Testing of backup procedures (successful business continuity)

The audience for this standard includes:

- Financial service organizations who wish to engage an internal group or an external agency for a penetration test. Understanding the rules of engagement to specify, negotiate and accept a penetration test equally applies to both internal groups and external agencies.