

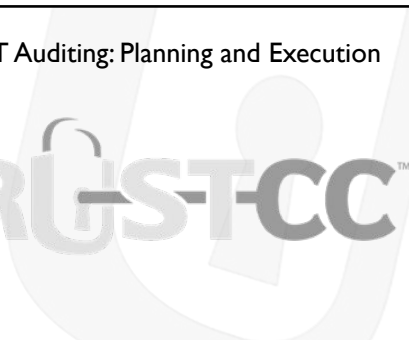
Tom Schauer
TrustCC
tschauer@trustcc.com
253.468.9750 - cell



Copyright TrustCC. All Rights Reserved.




Effective IT Auditing: Planning and Execution



TRUSTCC™

Copyright TrustCC. All Rights Reserved.

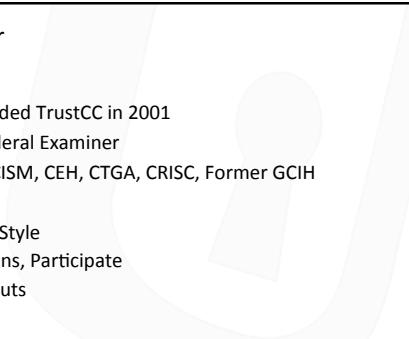


Tom Schauer


- ✓ Since 1986
- ✓ TrustCC Founded TrustCC in 2001
- ✓ State and Federal Examiner
- ✓ CISSP, CISA, CISM, CEH, CTGA, CRISC, Former GCIH

✓ Presentation Style

- Ask Questions, Participate
- Your Handouts




Copyright TrustCC. All Rights Reserved.



Hackers, Activists and Anarchists
The State of Information Security in 2013

By Tom Schauer
CISA, CISM, CISSP, CEH, CRISC, CTGA




Copyright TrustCC. All Rights Reserved.

Every week we steel millions of dollars worth of information... then we gave it back!

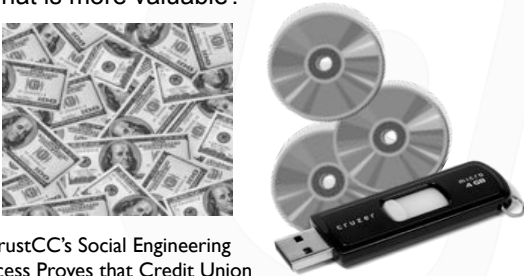
TrustCC has performed over 1600 IT Audits and Penetration Tests for nearly 400 Organizations.

Thus far in 2013, we've hacked into 53% of our clients from the Internet. Once on the inside we access sensitive information 75% of the time and Admin access 62% of the time.




Copyright TrustCC. All Rights Reserved.

What is more valuable?

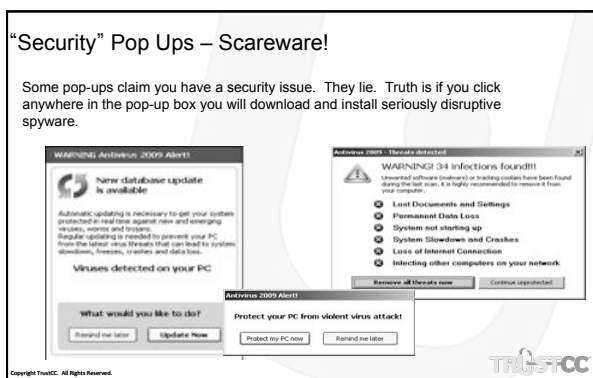


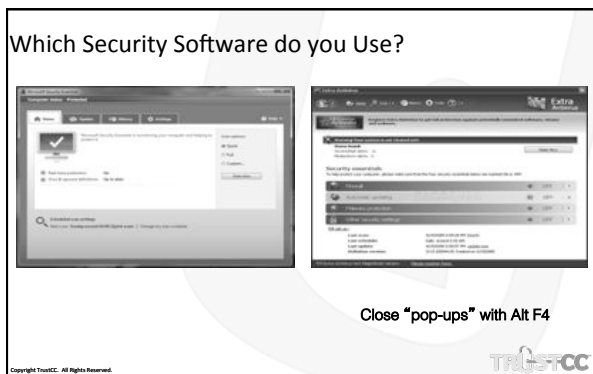
TrustCC's Social Engineering Success Proves that Credit Union Employees don't get it.



Copyright TrustCC. All Rights Reserved.







Vishing and Smishing

- Hello this is "Your" Bank calling...
- We've detected potentially fraudulent activity on your Visa card...
- Please call 800.123.4567...

- You call and are asked to confirm your account...

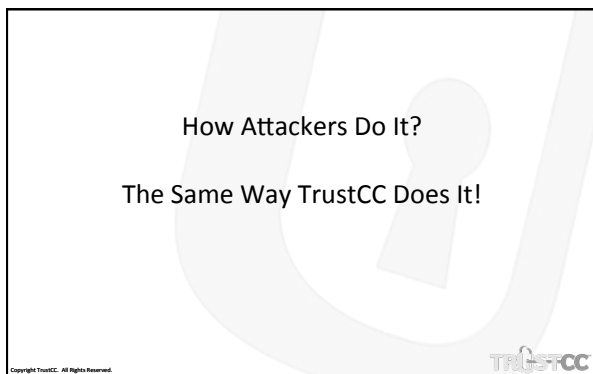
Copyright TrustCC. All Rights Reserved.





Copyright TrustCC. All Rights Reserved.



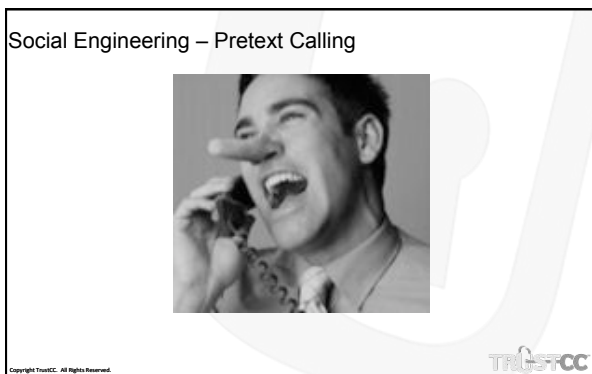


Copyright TrustCC. All Rights Reserved.









Social Engineering – The HVAC Guy



Copyright TRUSTCC. All Rights Reserved.





Copyright TRUSTCC. All Rights Reserved.





Copyright TRUSTCC. All Rights Reserved.



Thank you. You can generate your Visa gift card by clicking [HERE](#).

Gift Card Instructions:
Click the link above
When prompted, click "Run"
If a Microsoft Unverified Publisher warning pops up, click "Disregard and Run" and then "Run" again.
Your coupon will pop up after being generated.


Copyright TrustCC. All Rights Reserved.



After SE, We are on the Internal Network

- ✓ Every Month by Microsoft, Adobe Reader, Java, Flash, Office, Internet Explorer, etc.
- ✓ Weak Configs: Default Passwords, Promiscuous Access
- ✓ Exploit Vulnerabilities
- ✓ Metasploit: Point and Click Hacking
- ✓ Disable controls, create accounts, crack passwords, establish resilient access, delete log records.


Copyright TrustCC. All Rights Reserved.



Smaller Organizations do better

- ✓ Any financial institution with more than 5 branches is highly likely to be susceptible to Social Engineering
- ✓ When combined with users having "local admin rights"
- ✓ GAME OVER
- ✓ Must depend on technical controls, logging and alerts

Copyright TrustCC. All Rights Reserved.



Result: Online Account Takeover

- Financial Institution deploys multi-factor authentication and strong controls.
- Hacker successfully deploys Malware on customer/member computer
- Malware records and replays keystrokes
- Once Authenticated the Hacker executes a fraudulent funds transfer

Copyright TrustCC. All Rights Reserved.



We Don't DDOS but "They" Do.

✓Groups like Anonymous and "Cyber Fighters of Izz ad-Din al-Qassam" are wreaking havoc on larger (generally >\$5B) financial institutions. Recent guidance expects a written risk assessment, action, monitoring. For most FIs focus should be on outsourced website and online banking services.

✓How it works:

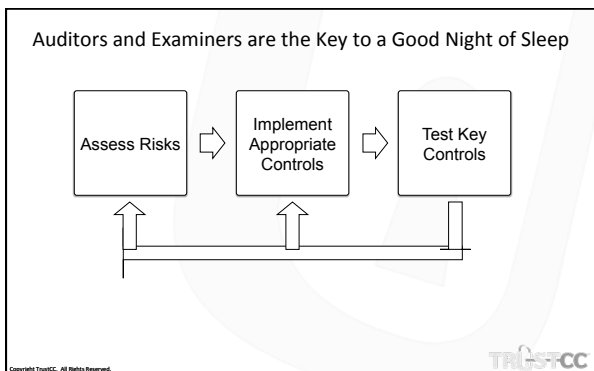
Copyright TrustCC. All Rights Reserved.





Copyright TrustCC. All Rights Reserved.





The Audit/Examination Challenge

- ✓ How do I audit/examine something that is so dynamic, so actively hostile, and something I am unfamiliar with....
 - ✓ Have a great plan
 - ✓ Either develop and retain skills OR partner with a provider
 - ✓ Execute the plan

Copyright TrustCC. All Rights Reserved. TRUSTCC

The Regulatory Environment

By Tom Schauer
CISA, CISM, CISSP, CEH, CRISC, CTGA

Copyright TrustCC. All Rights Reserved. TRUSTCC

In 1986...

- ✓The Office of the Comptroller of Currency
 - BC 229 – Information Security
 - BC 226 – End User Computing

- Do you think much has changed? See extract on next slide from 2001 OCC guidance.

Copyright TruSTCC. All Rights Reserved.



APPENDIX: LIST OF OCC ISSUANCES REGARDING INFORMATION SECURITY

- Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 66 Fed. Reg. 8614, 8632 (February 1, 2001), to be codified at 12 CFR Part 95, App. B
- OCC Alert 2000-09 Protecting Internet Addresses of National Banks (July 19, 2000)
- OCC Bulletin 2000-14 Infrastructure Threats-Intrusion Risks (May 15, 2000)
- OCC Alert 2000-01 Internet Security: Distributed Denial of Service Attacks (February 11, 2000)
- "Internet Banking" booklet in Comptroller's Monthbook (October 1999)
- OCC Bulletin 99-9 Infrastructure Threats from Cyber-Terrorism (March 15, 2000)
- Check Fraud-A Guide to Avoiding Losses (February 2000)
- OCC Bulletin 98-38 Technology Risk Management: PC Banking (August 24, 1998)
- OCC Advisory Letter 98-11 Pretext Phone Calling (August 20, 1998)
- OCC Advisory Letter 91-4 Use of Social Security Numbers for Automated Call Systems (July 24, 1991)
- OCC Banking Circular 229 Information Security (May 31, 1988)
- Banking Circular 226 End-User Computing (January 25, 1988)

Copyright TruSTCC. All Rights Reserved.



Fast Forward to 2013 – Security Regulations for All

- ✓Industry Agnostic: CSB 1386, PCI
- ✓Healthcare: HIPAA, HITech
- ✓Energy: NERC
- ✓Federal Government: FISMA
- ✓Banking: Gramm Leach Bliley Act and MORE

Copyright TruSTCC. All Rights Reserved.



Every Industry - CSB 1386 Compliance

Requires a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, to disclose any breach of the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Copyright TrustCC. All Rights Reserved.



IT Guidance for FIs

- ✓ Graham-Leach-Bliley Act (GLBA)
 - Part A – Privacy
 - Part B – Security
- ✓ Federal Financial Institution Examination Council (FFIEC) IT Booklets
- ✓ Sarbanes-Oxley (SOX) for Public Banks

Copyright TrustCC. All Rights Reserved.



GLBA Compliance

"Each financial institution shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards.

A financial institutions information security program shall be designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security of such information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer."

Copyright TrustCC. All Rights Reserved.



GLBA Relevant to IT Audit

- ✓ Assess Risks
- ✓ Test Key Controls identified in the Risk Assessment
- ✓ Report to the Board

Copyright TruCC. All Rights Reserved.



FFIEC IT Booklet & Guidance – Booklets

<http://thandbook.ffiec.gov/it-booklets.aspx>

- ✓ Audit – provides guidance to examiners and financial institutions on the characteristics of an effective information technology (IT) audit function. It is a foundation from which examiners can assess the quality and effectiveness of an institution's IT audit program. It describes the roles and responsibilities of the board of directors, management, and internal or external auditors; identifies effective practices for IT audit programs; and details examination objectives and procedures.
- ✓ Business Continuity Planning – provides guidance and examination procedures to assist examiners in evaluating financial institution and service provider risk management processes to ensure the availability of critical financial services.
- ✓ Development and Acquisition – provides examiners and financial institutions guidance for identifying and controlling development and acquisition risks. Development and acquisition is defined as "an organization's ability to identify, acquire, install, and maintain appropriate information technology systems." The process includes the internal development of software applications or systems and the purchase of hardware, software, or services from third parties.

Copyright TruCC. All Rights Reserved.



FFIEC IT Booklet & Guidance - Booklets


- ✓ E-Banking – provides guidance to examiners and financial institutions on identifying and controlling the risks associated with electronic banking (e-banking) activities. The booklet primarily discusses e-banking risks from the perspective of the services or products provided to customers.
- ✓ Information Security – protection of information assets. It is the process by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its operations.
- ✓ Management – assist examiners in evaluating financial institution risk management processes to ensure effective information technology (IT) management.
- ✓ Operations - risk management processes that promote sound and controlled operation of technology environments.
- ✓ Outsourcing Technology Services - assist examiners and bankers in evaluating a financial institution's risk management processes to establish, manage, and monitor IT outsourcing relationships.

Copyright TruCC. All Rights Reserved.



FFIEC IT Booklet & Guidance - Booklets


- ✓ Retail Payment Systems - provides guidance to examiners, financial institutions, and technology service providers (TSP) on identifying and controlling information technology (IT)-related risks associated with retail payment systems and related banking activities.
- ✓ Supervision of Technology Service Providers - governs the supervision of technology service providers (TSPs) and briefly summarizes the Federal Financial Institutions Examination Council (FFIEC) customer agencies' (agencies) expectations of financial institutions in the oversight and management of their TSP relationships. This booklet outlines the agencies' risk-based supervision approach, the supervisory process, and the examination ratings used for information technology (IT) service providers.
- ✓ Wholesale Payment Systems - provides guidance to examiners and financial institution management regarding the risks and risk-management practices when originating and transmitting large-value payments.



Copyright FFIEC. All Rights Reserved.

FFIEC IT Booklet & Guidance - Booklets

- ✓ Supervision of Technology Service Providers - governs the supervision of technology service providers (TSPs) and briefly summarizes the Federal Financial Institutions Examination Council (FFIEC) customer agencies' (agencies) expectations of financial institutions in the oversight and management of their TSP relationships. This booklet outlines the agencies' risk-based supervision approach, the supervisory process, and the examination ratings used for information technology (IT) service providers.
- ✓ Wholesale Payment Systems - provides guidance to examiners and financial institution management regarding the risks and risk-management practices when originating and transmitting large-value payments.






Copyright FFIEC. All Rights Reserved.

FFIEC Audit Guide

Table of Contents


Introduction	
IT Audit Roles and Responsibilities	
Internal Controls and System Requirements	
Audit Management	
Internal IT Audit Staff	
Examiner Management	
External Auditors	
Independence and Billing of External Auditors	
Independence	
Quality	
Internal Audit Program	
Risk Assessment and Risk-Based Auditing	
Program Elements	
Risk Rating System	
Audit Participation of Applicable Departments	
Enhancing Internal IT Audit	
Independence of the External Auditor Firm	
Examination of Organizations	
Planning, Methods of Testing, Sample Size	
Appendix A: Examination Procedures	
Appendix B: Glossary	
Appendix C: Laws, Regulations, and Guidance	

Copyright

Examiners want better tools

- ✓SANS 20 Critical Security Controls
 - Just security therefore incomplete
- ✓ISO27001&2, NIST 800 Series, COBIT5, etc...
- ✓CIS – Center for Internet Security



Copyright TrustCC. All Rights Reserved.

Critical Control	Effect on Attack Mitigation
1. Security of Authorized and Unauthorized Devices	Very High
2. Security of Authorized and Unauthorized Software	Very High
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High
4. Continuous Vulnerability Assessment and Remediation	Very High
5. Malware Defenses	High
6. Application Software Security	High
7. Wireless Device Control	High
8. Data Backup Capability	Moderately High to High
9. Security Staff Assessment and Appropriate Training to Fill Gaps	Moderately High to High
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Moderately High
11. Limitation and Control of Network Ports, Protocols, and Services	Moderately High
12. Controlled Use of Administrative Privileges	Moderately to Moderately High
13. Boundary Defense	Moderate
14. Maintenance, Monitoring, and Analysis of Security Audit Logs	Moderate
15. Controlled Access Based on the Need to Know	Moderate
16. Account Monitoring and Control	Moderate
17. State-Less Protection	Moderately Low to Moderate
18. Incident Response Capability	Moderately Low to Moderate
19. Secure Network Engineering	Low
20. Penetration Tests and Red Team Exercises	Low

VERY HIGH
These controls address the most critical vulnerabilities and are the most difficult to implement.

HIGH
These controls address the most critical vulnerabilities and are the most difficult to implement.

MODERATE
These controls address the most critical vulnerabilities and are the most difficult to implement.


LOW
These controls address the most critical vulnerabilities and are the most difficult to implement.



Copyright TrustCC. All Rights Reserved.

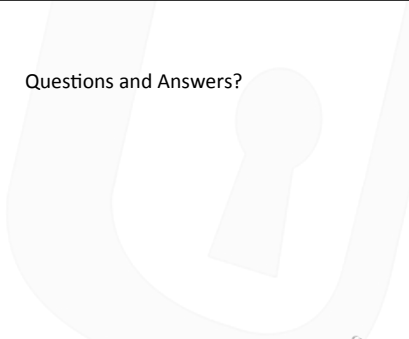
TrustCC Approach

- ✓Blend of Regulatory and Industry Guidelines
 - Approx 100 Security Controls (Primarily Technical)
 - Approx 130 IT Audit Controls (Physical & Administrative)
- ✓Most Competitors have a less granular approach
- ✓Advantages and Disadvantages



Copyright TrustCC. All Rights Reserved.

Questions and Answers?



Copyright TrustCC. All Rights Reserved.

TRUSTCC



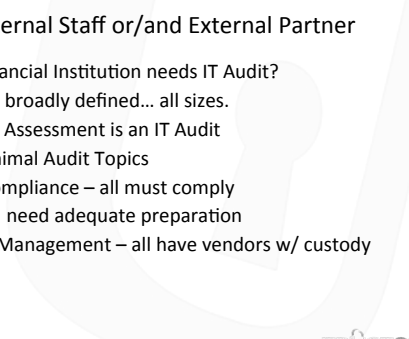
TRUSTCCTM

Copyright TrustCC. All Rights Reserved.

TRUSTCC

Staffing – Internal Staff or/and External Partner

- ✓What size Financial Institution needs IT Audit?
 - If IT Audit is broadly defined... all sizes.
 - ✓ A Security Assessment is an IT Audit
 - ✓ Other Minimal Audit Topics
 - GLBA Compliance – all must comply
 - BCP – all need adequate preparation
 - Vendor Management – all have vendors w/ custody



Copyright TrustCC. All Rights Reserved.

TRUSTCC

Hiring and Retaining IT Audit Staff

- ✓\$8B to \$10B seems to be “the” size
- ✓Most Internal FI IT Auditors lack deep technical skills

- ✓Salary and Benefits: \$60k to \$120k

- ✓Training and More Training or staff will fall behind

Copyright TruSTCC. All Rights Reserved.



Partnering

- ✓FFIEC Guide Recognizes the Necessity of Outsourcing
- ✓Experience: 1600 Assessments for nearly 400 FIs
- ✓Efficiency: 3 to 20 days and your IT audit and Security Assessment is done!
- ✓Benchmarking

- ✓Some are better than others. Network/Referrals is the best method to identify a great partner!

Copyright TruSTCC. All Rights Reserved.



6 Categories of IT Audits

- ✓General Computer Controls: Overview and Risk Based
- ✓Security Assessments: Technical Focus
- ✓Integrated Audit: Performed with Operational Audits
- ✓Specialty Deep Dives: Where/when risk warrants
- ✓Consultative Audits: Participation in IT Operations
- ✓Bank Compliance: SOX, FDICIA, etc.

Copyright TruSTCC. All Rights Reserved.



General Computer Controls

✓Scope

- Info Sec Policies/Training
- Risk Assessments
- Backup, Recovery, BCP
- Vendor Management
- Board Involvement
- General Physical Security
- Network Access Admin
- IT Governance
- SDLC, Change Management
- Core and Applications

✓Pitfalls

- If controls tested are not granular many important controls can be missed
- Difference between text book and "real" experience
- Difficult to align with forever changing examination scope
- IT could baffle with acronyms

Copyright TruSec. All Rights Reserved.



Security Assessments

✓Scope:

- Vulnerability Scanning
- Social Engineering
- Pen Testing: Exploitation
- Configuration Reviews
- Console Reviews
- Incident Response
- Other Testing

✓Common Pitfalls

- Too narrowly scoped
- Infrequent
- Not "integrated" with review of Admin and Physical controls

Copyright TruSec. All Rights Reserved.



Integrated Audits

✓Scope

- User Access to Key Applications
- Clean Desk / End of Day
- Physical Security
 - ✓Including IT Assets
- Segregation of Duties
- BCP Plan Review
- Training Verifications

✓Pitfalls

- Adds scope to already "tight" resource allocations
- Auditors may be uncomfortable

Copyright TruSec. All Rights Reserved.



Specialty “Deep Dives”

✓Scope – Risk/Regulatory

- Mobile Banking
- Mobile Devices
- Board iPads
- DDOS Protection
- Remote Deposit Capture
- Windows Active Directory & Group Policy

✓Pitfalls

- May be difficult to find talent
- What makes the “cut”?
- Where do you get an audit program?
- Perfect for Retainer or CoSource

Copyright TrustCC. All Rights Reserved.



Consultative Audits

✓Scope

- Develop Scorecards/ Methodology
- Participate in IT Committees
 - ✓IT Steering
 - ✓IT Change Control
 - ✓BCP
 - ✓Incident Response
- Project Advisory

✓Pit Falls

- Must Maintain Independence
- Challenging to “earn respect”
- Meetings and more Meetings

Copyright TrustCC. All Rights Reserved.





Copyright TrustCC. All Rights Reserved.




The Audit Process

- ✓ Risk Assess – Every 1 to 3 years
- ✓ Plan – Every year
- ✓ Execute - continuously
- ✓ Adjust – quarterly

- ✓ Repeat


Copyright TrustCC. All Rights Reserved.



Risk Assessment
A Critical IT Audit Component

By Tom Schauer
CISA, CISM, CISSP, CEH, CRISC, CTGA

Copyright TrustCC. All Rights Reserved.




Examiners Expect

- ✓ A Risk Management Culture
- ✓ GLBA Member/Customer Info Security RA is Primary

- ✓ Other Types of Risk Assessments
 - Business Impact Assessment
 - Authentication for Online-Banking
 - Audit Risk Assessment
 - DDOS Risk Assessment
 - New Tech Risk Assessment (ie. Board iPads)

Copyright TrustCC. All Rights Reserved.



Risk Assessment

The screenshot shows a web page with the following content:

- Table of Contents:**
 1. Evaluation
 2. Risk assessment in public health
 - 2.1. How the risk is determined
 - 2.2. Acceptable risk increase
 3. Risk assessment in auditing
 4. Concepts of quantitative risk assessment
 5. See also
 6. External links
 7. References
- Explanation:** Risk assessment may be the most important step in the risk management process, and may also be the most difficult and prone to error. Once risks have been identified and assessed, the steps to properly deal with them are much more straightforward.
- Graph:** A line graph showing Risk Level on the y-axis and Probability of occurrence of the adverse event on the x-axis. The curve shows a steep decline in risk level as probability increases, with a point labeled '1 per year'.

Risk Assessment – Threat Inventory

The diagram shows a house with the following labels:

- Threat:** A burglar icon with a key.
- Vulnerability:** Labels pointing to the roof, chimney, and front porch.
- Asset:** Labels pointing to the house and two cars parked in front.

Risk Assessment – Controls

The diagram shows the same house with security controls:

- Watch Dog:** A dog on a leash.
- Stronger Key:** A key icon.
- Alarm:** A bell icon.
- Guard:** A person standing by a gate.

What it is not...

- ✓ A Risk Assessment does not include TESTING the effectiveness of controls.
- ✓ So when we talk about Control testing, realize that it is a separate step that follows risk assessment and should be “tied” to the risk assessment.

Copyright TruSTCC. All Rights Reserved.



GLBA Information Security Risk Assessment

- ✓ Threat Based:
- ✓ Consider foreseeable threats, evaluate the impact should threat occur, document and identify key controls, evaluate the likelihood of the threat given the controls, conclude.

Copyright TruSTCC. All Rights Reserved.



GLBA - Reasonably Foreseeable Threats


- ✓ Passwords Guessed
- ✓ Malware
- ✓ Network Device Attack
- ✓ Workstation Attack
- ✓ Wireless Attack
- ✓ Server Attack
- ✓ Physical Security
- ✓ Social Engineering
- ✓ Backup Tapes Stolen
- ✓ Remote Access Attack
- ✓ Vendor Data Attack
- ✓ Online Banking Attack
- ✓ etc

Copyright TruSTCC. All Rights Reserved.




GLBA - Key Controls

- Anti-Malware
- System Configuration
- Firewalls
- IDS/IPS
- Policies and Standards
- Security Training
- Board Reporting
- Controls Testing
- Patching and Updates
- Encryption
- Visitor Controls
- etc

Copyright TrustCC. All Rights Reserved. 

Audit Risk Assessment – Possible Risk Factors


- ✓ Sensitivity to Executive Management
- ✓ Maturity of Practices and Procedures
- ✓ Extent of Change
- ✓ Longevity of Personnel Responsible
- ✓ Experience of Personnel Responsible
- ✓ Outsourced
- ✓ Sufficiency of Continuity Options
- ✓ Maturity of Logging and Monitoring
- ✓ Regulatory Issuance, Known Examiner Focus, or other Compliance Practice
- ✓ SANs Twenty Critical Controls
- ✓ Financial Risk
- ✓ Operational Risk
- ✓ Reputation Risk
- ✓ Period Since Last Review (internal or External)
- ✓ Last Review had Significant Findings
- ✓ Most Recent Audit Opinion

Copyright TrustCC. All Rights Reserved. 

Management Support

Is Management ready to embrace a risk management culture?

If not at the top, it won't happen.

Copyright TrustCC. All Rights Reserved. 

Risk Assessment Outcomes

We prefer that risk assessment influence audit planning rather than dictate audit planning.

Walk Through Sample – We use tools, you can do the same analysis and reporting without “efficiency” tools.

Copyright TrustCC. All Rights Reserved.



Why I like our Risk Assessment

- ✓ It is easy to use
- ✓ It can be done by IA, by Consultant or by Stakeholders
- ✓ It produces “relative” result... comparison to Avg.

- ✓ Influences the Audit Plan

Copyright TrustCC. All Rights Reserved.





Copyright TrustCC. All Rights Reserved.



The Audit Plan

Audit Plan and Schedule

Proposed 2011 IT Audit Schedule

Description	Performed By	Hours by IA	Hours by TrustCC	Quarter Planned
IT Risk Assessment and IT Audit Planning	IA and TrustCC	30	30	Q1
Data Loss Prevention - Deep Dive	IA	80	0	Q1
Mobile Banking - Deep Dive	IA and TrustCC	60	30	Q1
General Computer Controls Audit	TrustCC	20	80	Q2
Security Assessment	TrustCC	20	80	Q2
Data Center Modernization - Deep Dive	IA	40	0	Q2
Core Banking System - Deep Dive of Key Application	IA and TrustCC	80	40	Q3
Wire Transfer - Deep Dive of Key Application	IA	80	0	Q3
Change Management - Deep Dive	IA	120	0	Q4
Software Licensing - Deep Dive	IA	120	0	Q4
Totals:		890	230	

Copyright TrustCC. All Rights Reserved.



The Audit Plan

Integrated Audits: Access, BCP, Segregation of Duties, Physical Security, Training

- Branch Audits - Q1-Q4
- Real Estate Lending - Q2
- Collections - Q3
- Facilities - Q3

Consultative Audit Activity

- Quarterly Security Committee
- Q4 BCP Test
- Weekly Change Meeting
- Core Replacement Project

Copyright TrustCC. All Rights Reserved.





Copyright TrustCC. All Rights Reserved.



Transitioning to Tests of Key Controls

- ✓ Identify key controls in GLBA and Audit RA
- ✓ Determine skills needed
- ✓ Execute RFPs as necessary
- ✓ Coordinate Auditors

Copyright TrustCC. All Rights Reserved.



Tests of Key Controls – Testing Techniques

- ✓ Inquiry
- ✓ Inquiry and Observation
- ✓ Inquiry and Testing

Copyright TrustCC. All Rights Reserved.



Tests of Key Controls – Deficiency Ratings

- ✓ High
- ✓ Medium – High
- ✓ Medium

- ✓ Discussion Item
- ✓ Low- Medium
- ✓ Low

Copyright TrustCC. All Rights Reserved.



Tests of Key Controls – Work-Papers

- ✓Who did the work
- ✓Control Objectives
- ✓Notes about the environment and deficiencies noted

- ✓Is SAS65 needed? (Enough detail to re-perform and reach same conclusion)
 - ✓ This level of documentation is Time Consuming

- ✓Keeping documents and samples?

Copyright TruSTCC. All Rights Reserved.



Tests of Key Controls – Sample Sizes

- ✓Who will be relying on the audit work?

Copyright TruSTCC. All Rights Reserved.



Documentation Outcomes

We prefer documentation that provides evidence of testing but focuses effort on testing and consultation rather than documentation.

Walk Through Sample – We use tools, you can do the same analysis and reporting without “efficiency” tools.

Copyright TruSTCC. All Rights Reserved.



Why I like our Documentation Process

- ✓ It is easy to use
- ✓ Very Efficient
- ✓ Good Level of Documentation
- ✓ Granular
 - The BCP plan is sufficient to guide... vs.
 - The BIA..., Strategy aligns..., BCP updated..., Testing...
- ✓ Benchmarking
- ✓ Reports for Every Audience
- ✓ Graphical when effective

Copyright TrustCC. All Rights Reserved.





Copyright TrustCC. All Rights Reserved.



The sub \$200M Credit Union

- ✓ Standard Security Assessment
 - Annual Internal and External Vulnerability Scanning
 - Social Engineering (at least one form)
 - Limited Pen Testing and Exploitation
 - Limited Configuration Reviews and Console Reviews
 - Incident Response Review
- ✓ Value GCC Audit
 - Vendor Management
 - GLBA Compliance
 - Business Continuity Planning

Copyright TrustCC. All Rights Reserved.



The \$200M to \$600M Credit Union

- ✓Standard or Premium Security Assessment
- ✓Standard GCC Audit
- ✓Integrated Audits using IA resources
- ✓Maybe an outsourced "Deep Dive"

Copyright TrustCC. All Rights Reserved.



The >\$600M Credit Union

- ✓Premium Security Assessment
- ✓Premium GCC Audit
- ✓Integrated Audits
- ✓2 to 3 Deep Dives
- ✓Consultative Auditing

Copyright TrustCC. All Rights Reserved.

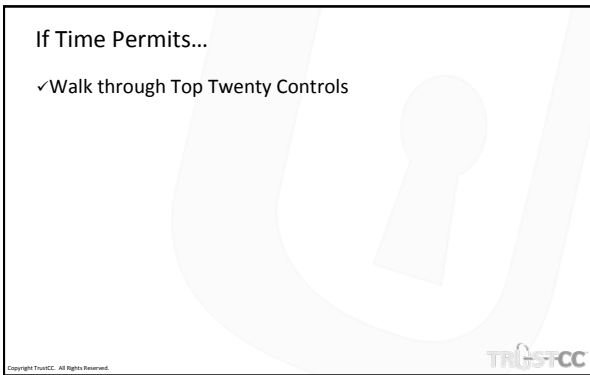


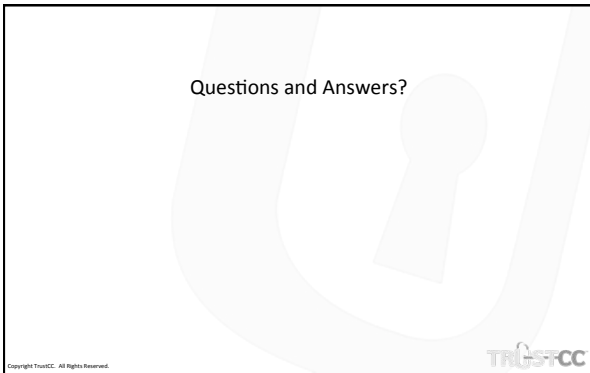
What does your Audit Plan look like?

Copyright TrustCC. All Rights Reserved.









www.trustiskey.com

TRUSTCC
Trusted IT Audit, Security and Compliance

HOME | FORCS | TRAINING MATERIALS | FORMS | NEWS AND UPDATES | REQUEST AN ARTICLE

TRUSTCC'S
BONDH required for Most Access

Thanks to V Compliance Security, Audit and Compliance
partner, Vite Encryption website designed specifically for our
Clients, State Examiners, and Prospective clients.

The content Host Configuration & Customized a few samples,
Prospective if Auditing site and Examiners see all content.To access at Logging / Mobile g the panel to the right.

TO REQUEST
Risk Assessment SFS.

Trust S&C's Training / Awareness Internal Users and is Copyrighted.
Registered Vendor Management within their organizations but may
NOT abuse organization.

Recent Posts - Login Required

- Four New Additions to our Team
- Social Networking - Risk or Reward
- GET LOW ON
- Contingency - Board Reporting
- Website Security and Operations Policy

Search this website
