

# Information Security Management for Community Banks

OCC7628-0

Sponsored by:

*Office of the Comptroller of the Currency*

---

## **Directions for the Web-based Portion of the Seminar**

**IMPORTANT: DO NOT THROW AWAY!!!**

**You will need these instructions on the day of the seminar.**

### **SYSTEM REQUIREMENTS and TESTING YOUR EQUIPMENT**

Please do this a day or two before the event.

Detailed system requirements can be found at:

<http://www.krm.com/system.htm>

Detailed directions on testing your equipment can be found at:

<http://www.krm.com/testing.htm>

### **TO CONNECT TO THE LIVE PROGRAM**







**You are entitled to ONE PC connection for this program.**

Please do this about 10 to 15 minutes prior to the start time of the program.

Close all of the applications that you may be running on your computer. Open your browser and go to:

<http://www.placeware.com/cc/krm>

An "Enter Meeting" sign-on screen will appear:

-  In the "Your Name" area, key in the PIN and Name of the person who registered for the program
-  In the "Meeting ID" area, key in **76280**
-  "Meeting Key" is NOT required, please leave this blank.
-  Click ENTER
-  Click Audience Entrance
-  If you are using Internet Explorer®, you may receive a message regarding the install of the Placeware console. On slower internet connections, this could take up to 20 minutes. This is completely optional. To bypass the install, just click on Open Audience Console.

If you see a message that says that no slides are available, please call us at 1-800-775-7654 or 715-833-5426.

If your system fails the tests, the results of these tests will be displayed on your screen. Please follow any directions that may appear.

**If you have questions, please contact us at 800-775-7654 or 715-833-5426.**



---

Comptroller of the Currency  
Administrator of National Banks

---

## **Information Security Management for Community Banks**

Virtual Seminar

**Tuesday, May 6, 2003**

**2:00 p.m. – 3:30 p.m. Eastern**

**1:00 p.m. – 2:30 p.m. Central**

**12:00 Noon – 1:30 p.m. Mountain**

**11:00 a.m. – 12:30 p.m. Pacific**

**Presented by:**

**John D. Hawke, Jr.**

**Clifford A. Wilke**

**Douglas Foster**

**Robert W Hurd**

**Deborah Katz**



---

Comptroller of the Currency  
Administrator of National Banks

---

## **A Web and Telephone Seminar**

# **Information Security Management for Community Banks**

Tuesday, May 6, 2003 and  
Wednesday, May, 7, 2003

**Speaker Biographies**  
**Electronic Polling Question**  
**PowerPoint Presentation**

## **John D. Hawke, Jr.**

### *Comptroller of the Currency*



John D. Hawke, Jr. was sworn in as the 28th Comptroller of the Currency on December 8, 1998. After serving for 10 months under a Recess Appointment, he was sworn in for a full five-year term as Comptroller on October 13, 1999.

The Comptroller of the Currency is the Administrator of National Banks. The Office of the Comptroller (OCC) supervises about 2,200 federally chartered commercial banks and about 52 federal branches and agencies of foreign banks in the United States comprising more than half of the assets of the commercial banking system. The Comptroller also serves as a Director of the Federal Deposit Insurance Corporation, the Federal Financial Institutions Examination Council, and the Basel Committee on Banking Supervision.

Prior to his appointment as Comptroller, Mr. Hawke served for 3 1/2 years as Under Secretary of the Treasury for Domestic Finance. In that capacity he oversaw the development of policy and legislation in the areas of financial institutions, debt management, and capital markets, and served as Chairman of the Advanced Counterfeit Deterrence Steering Committee and as a member of the board of the Securities Investor Protection Corporation. Before joining Treasury, Mr. Hawke was a Senior Partner at the Washington, D.C., law firm of Arnold & Porter, which he first joined as an associate in 1962. At Arnold & Porter he headed the Financial Institutions practice, and from 1987 to 1995 he served as Chairman of the firm. In 1975 he left the firm to serve as General Counsel to the Board of Governors of the Federal Reserve System, returning in 1978.

Mr. Hawke was graduated from Yale University in 1954 with a B.A. in English. From 1955 to 1957 he served on active duty with the U.S. Air Force. After graduating in 1960 from Columbia University School of Law, where he was Editor-in-Chief of the Columbia Law Review, Mr. Hawke was a law clerk for Judge E. Barrett Prettyman on the U.S. Court of Appeals for the District of Columbia Circuit. From 1961 to 1962 he served as counsel to the Select Subcommittee on Education in the House of Representatives.

From 1970 to 1987 Mr. Hawke taught courses on federal regulation of banking at the Georgetown University Law Center. He has also taught courses on bank acquisitions and financial regulation and serves as the Chairman of the Board of Advisors of the Morin Center for Banking Law Studies at Boston University School of Law.

In 1987 Mr. Hawke served as a member of a Committee of Inquiry appointed by the Chicago Mercantile Exchange to study the role of futures markets in connection with the stock market crash in October of that year.

Mr. Hawke has written extensively on matters relating to the regulation of financial institutions, and is the author of Commentaries on Banking Regulation, published in 1985. He was a founding member

of the Shadow Financial Regulatory Committee, and served on the committee until joining Treasury in April 1995.

Mr. Hawke is a member of the Cosmos Club, the Economic Club of Washington, and the Exchequer Club of Washington.

Born in New York City on June 26, 1933, Mr. Hawke resides in Washington, D.C. He was married in 1962 to the late Marie R. Hawke and has four adult children, Daniel, Caitlin, Anne, and Patrick, and two grandchildren, Spencer Patrick Hawke and Camerynn Marie Hawke.

## **Clifford A. Wilke**

*Director, Bank Technology Division*

*Office of the Comptroller of the Currency*



Clifford A. Wilke is director of Bank Technology at the Office of the Comptroller of the Currency in Washington, DC.

In that position, Mr. Wilke directs the formulation of policy and the development of examination tools and processes to supervise bank technology. He currently is a member of the OCC Privacy Working Group, National Risk Committee, and chairman of an internal team that is examining the issues surrounding Internet banking, account aggregation, and the future interaction of technology within the financial services industry.

Mr. Wilke joined the OCC after 17 years with Mobil Oil Corporation, and Mobil Oil Credit Corporation, where he led the development of the industry's first prepaid and multi-application card products (the Mobil GO CARD and Mobil MCI GO Card), and two of the six teams responsible for the initial development of Mobil SpeedPass. He has served on the board of directors of the Smart Card Forum and was one of the founders and chair of the Smart Card Forum Educational Institute, an organization dedicated to providing quality education in the field of smart cards to members of the public and private sectors.

Mr. Wilke is one of the co-authors of *Smart Cards — Seizing Strategic Business Opportunities*, published by McGraw-Hill and Company.

## **Douglas Foster**

*Technology Analyst*

*Bank Technology Division*



Douglas Foster is a technology analyst in the OCC's Bank Technology division, specializing in information security. He is the primary author of the FFIEC's Information Security booklet as well as several OCC bulletins and alerts. Technology is his second career; previously, he specialized in bank accounting and regulation and held positions, such as director, Financial Accounting of the Thrift Depositor Protection Oversight Board and chief accountant of the Corporate and Securities Division at the Office of Thrift Supervision (OTS). Mr. Foster is a certified information security systems professional (CISSP), certified information systems auditor (CISA), and certified public accountant (CPA).

## **Robert W. Hurd**

*National Bank Examiner*

*Southern District*



Robert Hurd is a national bank examiner in the Southern district of the Office of the Comptroller of the Currency (OCC). He joined the OCC as a financial intern in 1993 after serving overseas in the US Navy during the Gulf War.

Mr. Hurd earned a commission as a bank information technology specialist in 2000. He has spent most of his OCC career leading information technology examinations in community banks. He currently performs examinations in community, mid-size, and large banks, ranging in size from \$20 million to more than \$12 billion in total assets. Mr. Hurd is also involved with examinations of some of the largest information technology service providers in the financial industry.

Mr. Hurd was graduated with honors from Texas A&M University – Corpus Christi in 1995. He holds a Bachelors of Business Administration degree in finance. Mr. Hurd is a Certified Information Systems Auditor (CISA) and a Certified Information Systems Security Professional (CISSP).

## **Deborah Katz**

*Senior Counsel*

*Law Department*



Deborah Katz is a senior counsel in the Legislative and Regulatory Activities Division. She participated in drafting the Interagency Guidelines Establishing Standards for Safeguarding Customer Information and in the development of guidance on the joint final rule on Privacy of Customer Information. She is currently involved in drafting regulations implementing the USA PATRIOT Act.

Ms. Katz joined the OCC in 1986. She has been special assistant to the deputy chief counsel, and has worked in the Enforcement and Compliance, Bank Organization and Structure, and Legal Advisory Services divisions.

She received a B.S. from the Edmund E. Walsh School of Foreign Service, Georgetown University, in 1979, and a J. D., from the Benjamin Cardozo School of Law, Yeshiva University, in 1986. She is a member of the New York Bar.



**Polling Question**  
**5/6 and 5/7 Teleconference**

- 1. How many people are at your listening site? Press:**
  - 1 for one person**
  - 2 for two people**
  - 3 for three people**
  - 4 for four people**
  - 5 for five people**
  - 6 for six people**
  - 7 for seven people**
  - 8 for eight people**
  - 9 for nine or more people listening at your site.**



Office of the  
**Comptroller**  
of the **Currency**

# **Information Security Management for Community Banks**



Office of the  
**Comptroller**  
of the **Currency**

**Welcome**

**John D. Hawke, Jr.**  
**Comptroller of the Currency**

## **Agenda**

- Defining information security
- Understanding regulatory guidance
- Implementing the information security process
- Key management considerations

What is **“Security”**?

...and why is it important?

## **Essential Security Elements**

- Risk management
- People, process and technology
- Physical and cyber domains
- Continuous monitoring and updating

## Understanding Regulatory Guidance

	Regulation	Guidance/Expectations
Process	501(b) Security Guidelines	Primarily the FFIEC Information Security Booklet
Controls		Various bulletins, alerts, and advisory letters

## **501(b) GLBA Security Guidelines**

- Interagency Guidelines Establishing Standards for Safeguarding Customer Information



## **501(b) Security Guidelines**

- Purpose
- Scope
- Enforceability



Office of the  
**Comptroller**  
of the **Currency**

**501(b) Security Guidelines**

**Purpose**

- Ensure the security and confidentiality of customer information
- Protect against any anticipated threats or hazards to the security or integrity of such information
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer



Office of the  
**Comptroller**  
of the **Currency**

**501(b) Security Guidelines**  
**Scope**

- Meaning of “customer”
  - Personal, family or household purposes
  - Continuing relationship
- Meaning of “information”
  - Non-public personal information
  - Paper or electronic form



Office of the  
**Comptroller**  
of the **Currency**

**501(b) Security Guidelines  
Enforceability**

- Guidelines are located at 12 CFR Part 30,  
Appendix B
- Enforceable under Part 30 and 12 USC 1818

**501(b) Security Guidelines**  
**Information Security Program**

- Elements
  - Board oversight
  - Risk assessment
  - Management and control of risk

**501(b) Security Guidelines**  
**Information Security Program**

- Elements (continued)
  - Oversight of service providers
    - Due diligence
    - Contracts
    - Monitoring
  - Adjustment of the program

## **FFIEC Information Security Booklet**

- Consistent with 501(b) Security Guidelines
- Significant depth on each security process element
- Addresses all data and systems, not just customer information
- Written for institutions in general, not customized for any particular size or complexity

[http://www.ffiec.gov/ffiecinfobase/html\\_pages/it\\_01.html](http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html)

## **Roles and Responsibilities**

- Board of Directors
- Senior Management
- Information Security Officer
- Employees
- Vendors and Servicers



## **Board Guidance**

- Communicate expectations and requirements
- Describe risk measurements and acceptable residual risk
- Establish reporting obligations

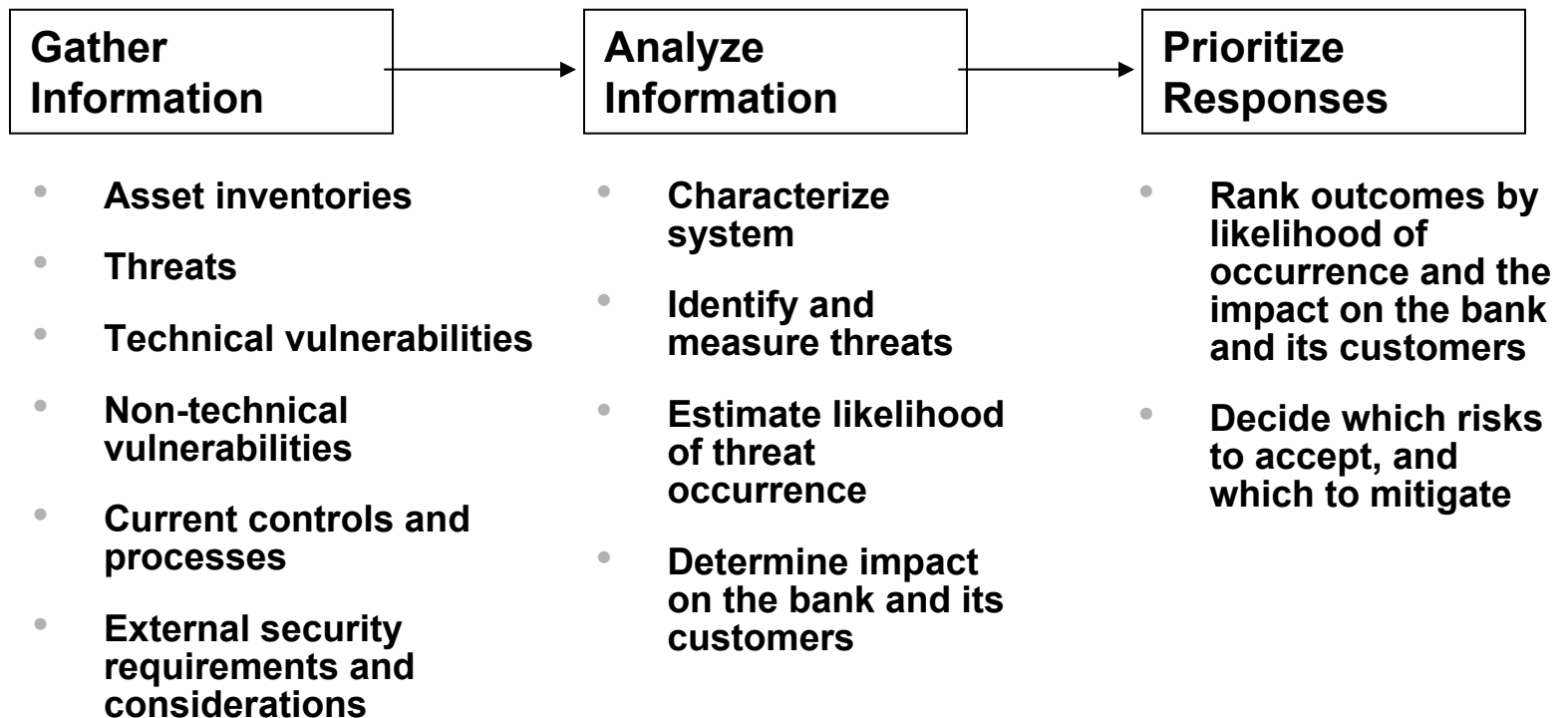
## **Implementing the Security Process**

- Risk assessment
- Strategy
- Controls
- Testing
- Monitoring and updating

## **Risk Assessment**

- Objectives:
  - Identify the risks you are willing, and not willing, to accept
  - Identify the systems and data that are most important to protect, and the related key controls
  - Identify the risks that can cause harm to customers

## Risk Assessment Steps



## **Gather Information**

- Three key questions:
  - What is being protected?
  - How is it protected?
  - What should it be protected from?

## **What is being protected?**

- Information
- Systems
- Infrastructure

*What really matters?*

## **How is it protected?**

- Controls, technical and non-technical
  - Policies
  - Practices
  - Vendor management
- Effectiveness of Controls

## **What should it be protected from?**

- Threats
  - Generally-targeted external attacks
  - Specifically-targeted and insider attacks
  - Unintentional violations
  - Environmental issues
- Vulnerabilities



## Risk Assessment Steps



- Asset inventories
- Threats
- Technical vulnerabilities
- Non-technical vulnerabilities
- Current controls and processes
- External security requirements and considerations

- **Characterize system**
- **Identify and measure threats**
- **Estimate likelihood of threat occurrence**
- **Determine impact on the bank and its customers**

- Rank outcomes by likelihood of occurrence and the impact on the bank and its customers
- Decide which risks to accept, and which to mitigate

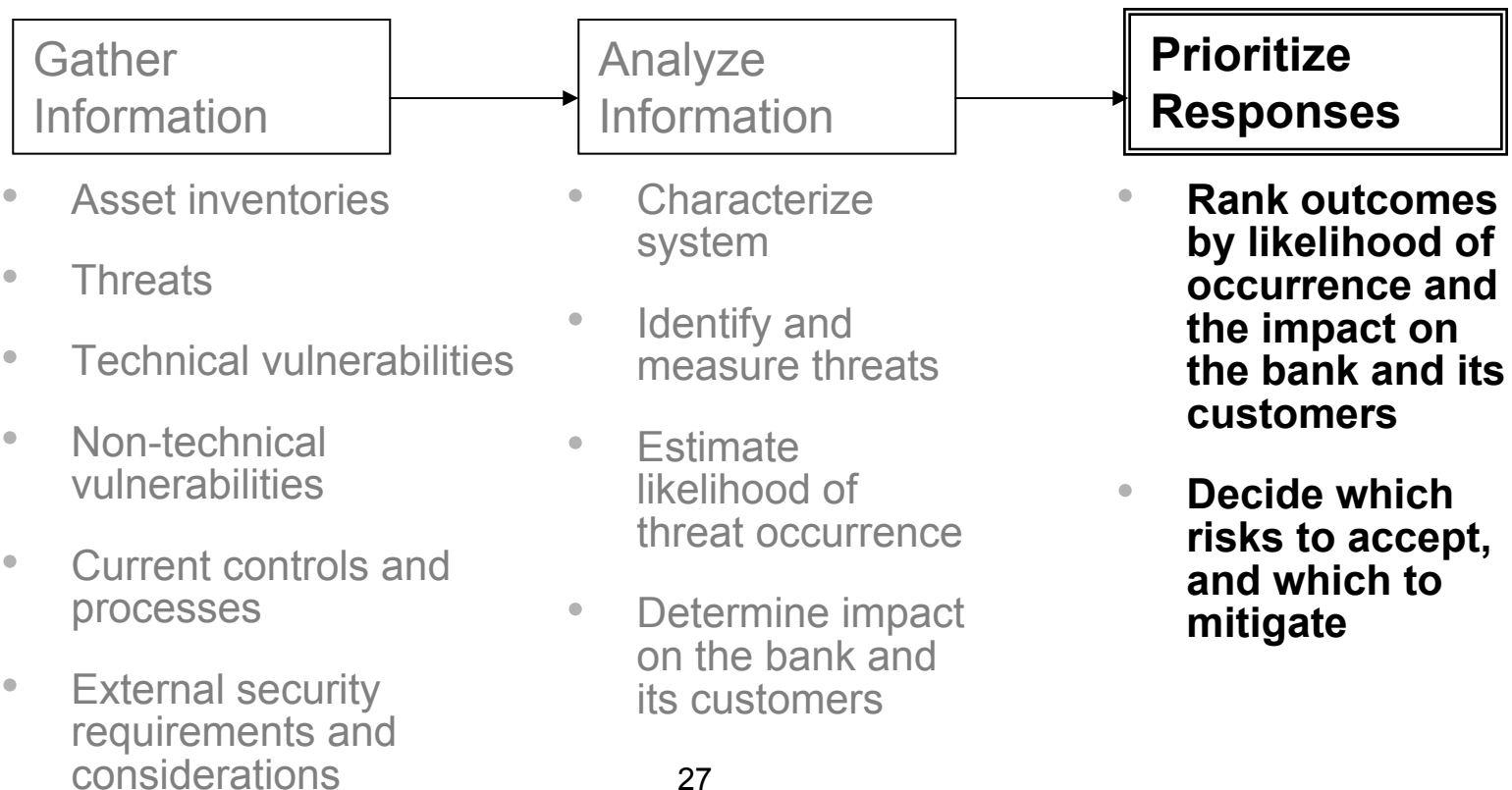
## **Analyze Information**

- Information security risk is measured by:
  - The likelihood that an event will occur
  - The impact of the event on the institution and its customers

## Analysis Illustration

Threats / Vulnerabilities	Controls	Effectiveness	Risk
<ul style="list-style-type: none"> <li>Internet worm attacks vulnerability in XYZ software, used in your e-banking and e-mail servers</li> </ul>	<ul style="list-style-type: none"> <li>Anti-virus</li> <li>Firewall</li> </ul>	<ul style="list-style-type: none"> <li><u>Minimal</u></li> <li>Anti-virus signatures can't be updated in sufficient time</li> <li>Firewall does not block based on packet contents</li> </ul>	<ul style="list-style-type: none"> <li><u>Likelihood</u> – Medium to high, because such worms appear regularly.</li> <li><u>Damage/Impact</u> – High transaction and reputation risk for the bank, high risk for customers</li> </ul>

## Risk Assessment Steps



## **Prioritize Response Illustration**

- The board of directors decided that all risks with a medium or greater likelihood and medium or greater damage/impact should be mitigated
- The risks posed in the previous example should be considered in a mitigation strategy
- Given the risk rating, management decided to address this risk immediately

## **Good Risk Assessment Practices**

- Involve many disciplines
- Be systematic
- Use an integrated approach
- Enforce accountability
- Document your work
- Learn from it
- Update it regularly

## **Risk Assessment Tools**

- Develop your own tools
- Consider commercially available tools

*A vulnerability assessment is not a risk assessment!*

## **Risk Assessment Direction**

- Self-directed
- Self-directed with technical assistance from consultants
- Consultant directed with bank personnel assistance
- Consultant performed



**Who directed your last information security risk assessment? Press:**

1. Self-directed
2. Self-directed with technical assistance from consultants
3. Consultant directed with bank personnel assistance
4. Consultant performed

## **Risk Mitigation Strategy**

- Objective – Develop a plan to mitigate the risks.

## **Risk Mitigation Strategy**

- Common considerations
  - Prevention, detection, response
  - People, process, technology

## Risk Mitigation Strategy – One approach

**Threat/Vulnerability:**

	<b>People</b>	<b>Process</b>	<b>Technology</b>
<b>Prevention</b>			
<b>Detection</b>			
<b>Response</b>			

**Residual Risk:**

## **Communicating the Strategy**

- Policies, procedures, standards
- Roles and responsibilities
  - Job descriptions
  - Authorized use policy
  - Awareness training

**What do you view as the most significant challenge in developing an effective risk mitigation strategy? Press:**

1. Technical expertise
2. Regulatory guidance
3. Board support
4. None of the above

## Agenda

- ✓ Defining information security
- ✓ Understanding regulatory guidance
- ✓ Implementing the security process
  - ✓ Risk assessment
  - ✓ Strategy
    - Controls
    - Testing
    - Monitoring and updating
- Key management considerations

## **Controls**

- Technical controls -- examples
  - Access (Network, O/S, and application system)
  - Encryption
  - Malicious code protections
  - Systems development, acquisition, and maintenance
  - Data destruction
  - Logging and data collection
  - Intrusion detection





Office of the  
**Comptroller**  
of the **Currency**

**Technical Controls**  
**Access**

- Who has the ability to access your bank's systems, digitally and physically?
  - How is that access controlled?



Office of the  
**Comptroller**  
of the **Currency**

**Technical Controls**  
**Encryption**

- If someone obtains unauthorized access to data, can they read it?
  - What is encrypted, and what is not?
  - What if you don't encrypt?

**Technical Controls**

**Malicious Code Protections**

- Can unauthorized programs from outside enter the bank's system?
  - Where is malicious code detected?
  - How effective is identification and blocking?
  - Do employees load software without your knowledge?

**Technical Controls**  
**Systems Development**

- Are systems and software purchased by the bank evaluated for security?
  - What criteria is used, and how does that criteria relate to the bank's needs?
  - What support exists for security alerts and updating?
  - Are systems configured to meet bank security expectations?

**Technical Controls**  
**Systems Maintenance**

- What about new vulnerabilities?
  - How does the vulnerability management process work?
  - How long does it take you to find out about and address a new vulnerability?

**Technical Controls**  
**Data Destruction**

- Is data in danger of being revealed when it is discarded?
  - Are electronic records eliminated from systems that are no longer used?
  - Are paper records shredded or otherwise destroyed?

## **Technical Controls**

# **Logging and Data Collection**

- Can the bank identify and reconstruct unauthorized system activities?
  - Who reviews the logs?
    - How frequently?
    - What training is necessary?
  - What is logged?
    - Is enough logged to affix responsibility, and reconstruct activity?
  - Where is it logged?
    - How long is it kept?

**Technical Controls**  
**Intrusion Detection**

- Does the intrusion detection system detect intrusions, or only detect potential attacks?
  - Who finds out about IDS alerts, when, and what, do they do with the information?
  - Do they have sufficient training and knowledge?



## **Controls**

- Non-technical controls -- examples
  - Physical security
  - Insurance
  - Personnel-related controls
  - Intrusion detection and response
  - Vendor management
  - Business continuity considerations



Office of the  
**Comptroller**  
of the **Currency**

**Non-technical Controls**  
**Physical Security**

- How are unauthorized people kept away from bank facilities, records, and information?
- How is access monitored and recorded?
- How difficult is it to steal computers?



Office of the  
**Comptroller**  
of the **Currency**

**Non-technical Controls**  
**Insurance**

- What coverage exists for security events?
- What has the insurance company done to review the bank's security, and what were the results of that review?
- How does your insurance limit the bank's risk?



Office of the  
**Comptroller**  
of the **Currency**

**Non-technical Controls**  
**Personnel**

- How are employees made aware of their security responsibilities?
- How do you make sure each employee is capable of performing their security responsibility?
- How do you train employees to guard against deception?
- How do you protect yourself against employee carelessness?

**Non-technical Controls**  
**Intrusion Detection and Response**

- How does your staff recognize a security event?
- Do they know what to do when they recognize an event?
- Do you have the necessary expertise available at all times to respond to an event?

**Non-technical Controls**  
**Vendor Management**

- Has your vendor historically maintained a secure environment?
- Are your security requirements a part of the vendor contract?
- How do you know the vendor is fulfilling those requirements?
- What if a security incident occurs at the vendor, are you told, and are procedures in place for a coordinated response?

**Non-technical Controls**  
**Vendor Management**

- Is your vendor's reporting sufficient for you to monitor the vendor's security?
  - SAS 70 may not be sufficient
  - Other reporting is not mature
  - You may have to negotiate your own vendor reporting responsibilities

**Non-technical Controls**  
**Business Continuity Considerations**

- Does your business continuity plan have security built-in?
- Are your personnel trained in the security roles they may assume?
- Have you tested the security controls as a part of your business continuity plan?



**What controls present the most challenges to your bank? Press:**

1. Intrusion detection systems
2. Vulnerability and patch management
3. Vendor management
4. Encryption
5. None of the above

## Testing

- Objective: Validate that the security risks are mitigated as expected
- Process:
  - Define the test program
  - Develop test plans
  - Perform the tests
  - Analyze the results
  - Respond based on risk

## **Independent Testing**

- Types of testing
  - Audit
  - Assessment
  - Penetration test

## **Independent Testing**

- Key factors
  - Scope
  - Personnel
  - Notifications
  - Controls
  - Frequency

## **Monitoring and Updating**

- Internal events
  - Security events
  - System changes
  - Personnel and organizational changes

## **Monitoring and Updating**

- External events
  - Technical vulnerabilities
  - Attack trends and exploits
  - Possible data sources:
    - Mailing lists
    - Information sharing organizations
    - General news sources

## Agenda

- ✓ Defining information security
- ✓ Understanding regulatory guidance
- ✓ Implementing the security process
  - ✓ Risk assessment
  - ✓ Strategy
  - ✓ Controls
  - ✓ Testing
  - ✓ Monitoring and updating
- Key management considerations

## **Key Management Considerations**

- Understand the environment
  - Internal and external
  - People, process, and technology
  - Vulnerabilities and controls
  - Pace of change and ability to react
  - Role as provider and consumer of services



## **Key Management Considerations**

- Personnel management
  - Assign, monitor, and enforce security roles and responsibilities
  - Ongoing training
- Risk Assessment
  - Risk identification and ranking
  - Ownership of the risk assessment
  - Explicitly accept risks

## **Key Management Considerations**

- Strategy
  - Identify key controls
  - Active vendor management
  - Sufficient technical expertise
- Controls
  - Identify employees responsible for each control
  - Integrate technical controls with personnel controls

## **Key Management Considerations**

- Testing
  - Preparation and adherence to test plan
  - Test plans based on risk
  - Scope covers key controls
- Monitoring and Updating
  - Monitoring and participating in information sharing groups
  - Effective vulnerability management
  - Ongoing board involvement



Comptroller of the Currency  
Administrator of National Banks  
U.S. Department of the Treasury



**Search this Site:**

[Search Tips](#)

**What's New**

[About the OCC](#)

[Banker Education](#)

[Careers at the OCC](#)

[Community Affairs](#)

[Corporate Applications](#)

[CRA Information](#)

[Customer Assistance](#)

[Electronic Banking](#)

[FOIA](#)

[Issuances](#)

[News Releases](#)

[Publications](#)

[Public Information](#)

[Regulatory Information](#)

[Related Sites](#)

[Speeches](#)

[NATIONAL](#)

**BankNet**

DEPARTMENT OF  
THE TREASURY

FIRSTGOV

The Office of the Comptroller of the Currency (OCC) charts, regulates, and supervises national banks to ensure a safe, sound, and competitive banking system that supports the citizens, communities, and economy of the United States.

---

April 8, 2003

[News Release 2003-28](#), Regulators Issue Interagency Paper On Sound Practices To Strengthen the Resilience Of The U.S. Financial System.

OCC 2003-14, Interagency Paper on Sound Practices to Strengthen the Resilience of the U. S. Financial System, 04/08/2003

This bulletin announces an interagency paper that intends to ensure the recovery and resumption of vital clearing and settlement activities in the event of the wide-scale disruption of financial markets. Key financial firms are expected to adopt four practices that are based on long-standing principles of business-continuity planning. [WORD ASCII](#)

- [Interagency Paper](#)

---

April 7, 2003

[News Release 2003-27](#), Bankers Assessed Civil Money Penalties and Barred from Banking After Compromising Confidential Customer Financial Information.

- [Stipulation and Consent Order](#)
- [Stipulation and Consent Order](#)



The June, September, and December 2002 issues of the [Quarterly Journal](#), are now available on-line.

All three issues feature the quarterly "Condition and Performance of Commercial Banks" and include information on bank mergers, national bank financial performance, speeches and congressional testimony, and interpretations. The September issue also includes the "Appeals Process" from the Office of the Ombudsman, and special



Office of the  
**Comptroller**  
of the **Currency**

## **Resources**

- NIST [csrc.nist.gov](http://csrc.nist.gov)
- CERT/CC [www.cert.org](http://www.cert.org)
- ISO [www.iso.org](http://www.iso.org)
- NIPC [www.nipc.gov](http://www.nipc.gov)

## **Additional Resources**

- OCC Guidance
- FFIEC Security Handbook
- Information Sharing
- User Groups

# Questions?

## To Order Telephone Seminar Publications —

PREPAYMENT IS REQUESTED. Please complete the form below with check made payable to the Comptroller of the Currency and return to: Comptroller of the Currency, Attn: Accounts Receivable, 250 E St., S.W., Mail Stop 4-8, Washington, DC 20219.

PUBLICATIONS

AMOUNT

<input type="checkbox"/> <b>Outsourcing Your Audit Function, April 2002</b>	\$ _____
<input type="checkbox"/> <b>Risk Management Principles for Third-Party Relationships, August 2002</b>	\$ _____
<input type="checkbox"/> <b>USA Patriot Act and Its Impact on Sound Anti-Money Laundering Programs, December 2002</b>	\$ _____

Each package consists of the handouts, a transcript of the seminar, and a tape of the seminar. \$75.

TOTAL AMOUNT ENCLOSED \$ \_\_\_\_\_

Name of Firm: \_\_\_\_\_

Attention: \_\_\_\_\_

Address: \_\_\_\_\_

City /State/Zip: \_\_\_\_\_

Phone Number: \_\_\_\_\_

Taxpayer Identification Number (TIN, EIN, SSN) \_\_\_\_\_ .

This number may be used for the collection and reporting of any delinquent amount arising from doing business with the federal government per 31 USC 7701.



# Office of the Comptroller of the Currency Program Evaluation

***This form is electronically tallied. Please mark only one circle for each question.  
Do not mark outside the circles.***

**Information Security Management for Community Banks: May 6, 2003 OCC7628-0**

**Scale Definition: 1 - Excellent 2 - Good 3 - Fair 4 - Poor**

- |   | 1                     | 2                     | 3                     | 4                     |
|---|-----------------------|-----------------------|-----------------------|-----------------------|
| 1. Overall rating of program .....                                  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2. Similarity of actual program content to advertised content ..... | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 3. Ease of registration .....                                       | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 4. Audibility of seminar .....                                      | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

**Presenter: Overall Effectiveness**

- |                         |                       |                       |                       |                       |
|-------------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| 5. Cliff A. Wilke ..... | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 6. Douglas Foster ..... | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 7. Robert W. Hurd ..... | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 8. Deborah Katz .....   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

**Participant Information**

9. How many people listened at your site?  
 1     2     3     4     5     6-10     11-15     16-20     21+
10. Would you participate in another virtual seminar? .....  Y     N

What was your overall impression of the program and format?

Would you participate in a credit related telephone seminar? If so, what particular credit topic would be of most interest to you, e.g., loan review, lending limits and exceptions, loan grading, ALLL, etc.

**Name of Participant (optional):** \_\_\_\_\_

**PLEASE FAX COMPLETED FORM TO 1-800-472-5138**

