SCHNEIDER DOWNS

INSIGHT • INNOVATION • EXPERIENCE

Top Ten Key IT Controls

Every Banking Executive Should have in Place

Eric Wright

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



What are IT controls?

- They are specific activities performed by a person or system that have been designed to prevent or detect the occurrence of a risk that could threaten your information technology infrastructure and supported business applications.
- IT controls are generally grouped into two broad categories:
  - **General controls** commonly include controls over data center operations, system software acquisition and maintenance, logical security, and application system development and maintenance.
  - **Application controls** such as computer matching and edit checks are programmed steps within application software; they are designed to help ensure the completeness and accuracy of transaction processing, authorization, and validity.
- Examples:

• Strong password policy	ITGC
• Encryption of mobile devices	ITGC
• Anomaly detection system	Application

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



Why IT controls

- Senior management and the board of directors have an increased responsibility for identifying, assessing, prioritizing, managing, and controlling risks.
- Developing a clearer understanding of the business risks that an organization faces on a daily basis is becoming increasingly more important in achieving an organization's mission and business objectives, increasing customer confidence, and increasing shareholder value.
- IT, which is becoming ever more complex and sophisticated, is revolutionizing businesses. The majority of organizations, large and small, rely on IT to initiate, record, process and report financial data. IT controls are pervasive and effect all that we do.
- The ability to rely on general IT controls enable an organization the luxury of relying on the application controls that are built into many of the ERP systems sold today.

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE

Change

- Reliance on IT Automation
- Electronic Transactions

Increased Risk

- Public Networks
- Reliance on Third Parties
- Data flowing beyond the walls
- Successful Breaches
- Global Presence
- Mobile Devices

Increased Threats

- Professional Attackers
- Attacks originate around the world
- Knowledgeable Attackers

Increased Control Requirements

- Automated controls
- Regulatory Environment
- Data integrity
- Reliance on electronic data
- Unacceptable level of data losses

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE

Top IT Controls - Criteria

- How Did We Identify the Top Ten Control Areas?
  - Guidance from audit methodology governing bodies (e.g. COSO, ISACA, AICPA, FFIEC, OCC, FDIC, Federal Reserve)
  - Industry trends and surveys
  - Regulatory requirements
  - Impact to your business
  - Risk factors
  - Discussions with clients
  - Personal experience

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE

Reasonable Approach

- Controls presented are organized into control areas or families.
- Not every control family may be appropriate for every organization.
- Not every control within an area may be appropriate for every situation.
- Controls designed and implemented according the process and levels of identified risks.

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



1) IT Governance

- Key Risks
  - IT goals and objectives are misaligned with business goals and strategy
  - Value provided by IT does not contribute to corporate objectives
  - IT processes ineffective and inconsistent
- Potential Impact
  - IT increases the risk to organization
  - Increased cost with minimal value
- Recommended Control Activities
  - Development of a strategic planning process
  - Metrics must be established and regularly monitored to evaluate the performance of the overall IT objectives
  - CIO reporting to or attending executive board meetings at which IT's contribution to enterprise goals is discussed
  - IT Policy development and maintenance process
  - Compliance and risk management
  - Management of Change

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



2) Continuous Monitoring and Incident Management

- Key Risk
  - Unauthorized business activities are not detected in a timely fashion
- Potential Impact
  - Data theft
  - Fraud
  - Financial misstatement
- Recommended Control Activities
  - Implement segregation of duties based on job descriptions
  - Identify key business application risks that can be monitored electronically (e.g. suspicious transactions based on thresholds)
  - Identify key system settings that should not be changed without authorization
  - Implement continuous monitoring software and/or reporting to alert management when suspicious or unauthorized activity takes place

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE

2) Continuous Monitoring and Incident Management

- **Anti-virus and Malware software –** definition files need to be up to date.
  - **According to Symantec, 1,100 new viruses are created every month**
- **Email Spam Filters –** Emails are one of the largest sources of viruses. Consider using a tiered approach to filtering email.

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



3) Information Security

- Key Risks
  - Undetected compromise or attacks (Security Metrics)
  - Failure to meet regulatory requirements (PCI, GLB, Privacy)
  - Loss or disclosure of sensitive or critical information assets
- Potential Impact
  - Loss of customers/clients (consumer confidence)
  - Decrease in value of organization (stock)
  - Lawsuits/fines
  - Damaged reputation
- Recommended Control Activities
  - Approach security as a process
  - Periodic vulnerability and penetration testing – including wireless and application
  - Implement Intrusion Detection/Prevention monitoring (Managed Security Services)
  - Monitoring of security patches and alerts



3) Information Security - Recommended Control Activities (continued)

- Encrypt laptop hard drives, external hard drives, PDAs, and external hard drives where sensitive information might be stored
- Encrypt fields in applications and databases where sensitive information is presented and stored
- Restrict access to application modules and databases where sensitive information is accessible
- Background checks for employees who have access to customer information
- A Layered Approach to Security

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE

Why the need for increase in security monitoring

- Failure of organizations to police themselves and to uphold a reasonable standard for integrity and data security has led to federal and state compliance mandates.
- Large number of data breaches and the massive size of the larger events (TJX, Heartland, Sony, Citi)
- Changing of the guard in Washington brought renewed intensity for network security and data protection along with State and location government regulations.
- **Cyber Czar** – New White House Office of cyber security reports to the National Security Council and National Economic Council. (Howard Schmidt)

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE

Why the need for increase in security monitoring (continued)

- Expansion to a global marketplace and global data sharing. Origin of threats has expanded to a world wide audience – International laws lagging, International enforcement not defined, Foreign Business ethics questionable
- Illegal For-Profit enterprises are being developed to market and sell information obtained from the theft of data and credentials – credit card purchases, medical coverage, investment accounts – all focused on stealing ones identity
- Changes in type of services offered and the way they are delivered

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE

FDIC – Release of FIL-50-2011

- In 2005, the FFIEC issued guidance entitled *Authentication in an Internet Banking Environment.*
  - This FFIEC guidance supplements the FDIC's supervisory expectations regarding customer authentication, layered security, and other controls in an increasingly hostile online environment.
  - The FDIC expects institutions to upgrade their controls for high-risk online transactions through:
    - Yearly risk assessments;
    - For consumer accounts, layered security controls;
    - For business accounts, layered security controls consistent with the increased level of risk posed by business accounts; and
    - More active consumer awareness and education efforts.
  - Layered security controls should include processes to detect and respond to suspicious activity and, for business accounts, administrative controls.
  - Certain types of device identification and challenge questions should no longer be considered effective controls.

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



What is the Minimum Acceptable Level of Layered Security

- Detect and Respond to Suspicious Activity
  - Collecting and analyzing customers habits and investigating when unusual activities are incurred. (Anomaly detection system)
- Control of Administrative Functions
  - Granting Privileges to change system or application configurations
- Device Identification
  - Use of traditional cookies and IP addressing are no longer sufficient
  - Recommending the use of “one time” cookies that combine PC configuration, IP addressing and geo-location identification
  - Can no longer be considered a primary control
- Challenge Questions
  - Can no longer be considered a primary control

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



Other Layered Security Controls to Consider

- Out of Band Verification for transactions
- Positive Pay and Debit Blocks
- Dual customer authentication
- Controls over account activities – dollar thresholds, processing windows, transaction volume limits
- IP reputation blocking
- Customer Awareness and Education

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE

Example – Lack of Security Monitoring

- TJX Companies
  - Eight major U.S. retailers were allegedly hacked by members of an international gang that admitted in a Securities and Exchange Commission filing in March 2007 that 45.7 million payment-card records had been stolen by unknown intruders.
  - Once inside the companies' networks, the alleged hackers installed "sniffer" programs that would capture card numbers, as well as password and account information, as the numbers were processed. According to a report in *The Wall Street Journal* in March 2007, the hackers left encrypted messages in the TJX systems to tell each other which files had been copied. Activity continued for 17 months.
  - The cost of this breach has been estimated at $256 million.

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



Example – Lack of Security Monitoring

- **Heartland Payment Systems**
  - Leading payment processing company was compromised by intruders that hacked into its computers that process 100 million payment card transactions per month for 175,000 merchants.
  - Intruders had access to Heartland's system for "longer than weeks" in late 2008 (USA Today Interview). Heartland was alerted to the breach by reports of suspicious transactions from Visa and MasterCard.
  - There were two elements to the breach, one of which was a keylogger that got through our firewall, Then subsequently they were able to propagate a sniffer onto some of the machines in the network. The sniffer was actually grabbing the transactions as they floated across the network.

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



Example – Lack of Security Monitoring

- June 9, 2011, Citigroup issued a press release indicating the 250,000 customer accounts had been compromised a month earlier. After further investigation, the true number of accounts that were compromised was 360,000 and cost Citigroup $2.7 million to cover the fraudulent transactions.
- Valley National Bank – 348 customer accounts were compromised on May 27, 2011. Using skimmers and cameras to capture account and pin numbers, the hacker made fake ATM cards and defrauded the bank of $280,000.
- Twelve days ago Kaspersky, a computer security firm, discovered the Gauss virus on more than 2,500 PCs in banks located in Lebanon, Israel and Palestine. This virus was specifically designed to spy on banking transactions and steal account and password information as data is transmitted.

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



4) Data Privacy

- Key Risk
  - Sensitive information is lost or stolen
- Potential Impact
  - Lawsuits/fines
  - Loss of funding
  - Data theft
  - Negative impact on reputation
- Recommended Control Activities
  - Identify sensitive information gathered/stored by your organization (e.g. SSNs, credit card numbers)
  - Eliminate the collection of sensitive information not needed
  - Document policies for collecting, storing, e-mailing, and reporting of sensitive information

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



4) Data Privacy

- Recommended Control Activities (continued)
  - Develop a data classification schema based on the risk exposure for certain data types
  - Train employees on proper handling of sensitive information
  - Create procedures for securely disposing of sensitive data

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE

What information are you required by law to secure

Financial institutions must implement an information security program that includes administrative, technical, and physical safeguards designed to achieve the following objectives:

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

Personally Identifiable Information (PII):

- Individuals name, consisting of the individual's first name or first initial and last name, in combination with…
- Social Security Number
- Drivers License Number or State Identification Number
- Credit Card, Debit Card, Financial Account Numbers

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE

Data Privacy - Breaches

- Source: Privacy Rights Clearinghouse
  - http://www.privacyrights.org
- A listing of all reported data breaches involving private information in the US since 2005
- Total number of reported breaches in 2011: 557
- Total number of RECORDS stolen in 2011: 30,678,619
- Total number of breaches so far in 2012: 54
- Total number of RECORDS stolen so far in 2012: 9,659,657
- In 2011, 50 of the 557 breaches (9%) came from financial service industry

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE

Data Privacy - Breaches

- 70% of data breaches are off network devices
- 19 people a minute become victims of identity theft due to data breaches
- A typical Fortune 1000 company can not locate 2% of their PCs on any given day.
- A typical Fortune 1000 financial institution loses one lap top a day.

SCHNEIDER DOWNS

INSIGHT ■ INNOVATION ■ EXPERIENCE

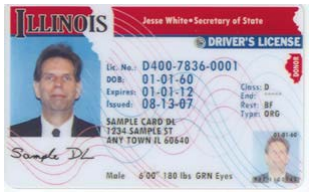
Understanding the Risk of The Market Value of Your Sensitive Data

	Trojan to steal account information	$980-$4,900
	Birth certificate	$147
	Medical billing data	$78-$294
	PayPal account logon and password	$6

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE

Credit Card Number with PIN **$490**
Without a PIN **$6 -$24**



Drivers License **$147**

Social Security Card **$98**

SCHNEIDER DOWNS

INSIGHT ■ INNOVATION ■ EXPERIENCE

Sell cvv2 a 100% live - good& cheap....!!! and - Windows Internet Explorer

http://www.iabolish.com/sell-

Sell cvv2 a 100% liv...

Free Classifieds, Ads, Advertising

Buy and Sell for free - Post as many ads as you like - it is fast, easy and for free. No registration required to post United States classifieds.

Home | Post free classifieds | Contact us

HOME
POST FREE AD
CONTACT US

CATEGORIES
Art, Antiques, Collectibles
Babies and Kids
Business and Industrial
Cars and Vehicles
- Auto Accessories
- Auto Parts
- Bikes
- Boats
- Campers
- Cars
- Motorcycles
- Other
- RVs
- SUVs
- Trucks
- Vans

Clothes and Accessories
Computers and Internet
Electronics
Health and Beauty
Home and Garden
Jobs
Music, Movies and Books

Report Abuse

Email this Ad

Post# A3614

Sell cvv2 a 100% live - good& cheap....!!! and (Texas)

Posted on: Thursday, 16 July, 2009 07:05
Reply to: *(Use contact form below)*

Price : (Not Provided)

Description:

Sell cvv2 a 100% live - good& cheap....!!! and share free socks.

I have a shop with 200,000 Cvv2 of all countries around the world
we always keep the prestige at first, you trust us totally to do business.
if you want to contac us when we are not online, please send your messages by my Yahoo Messenger then we can contact you as soon as possible.

Contact to me :
My yahoo nick : perfect_cvv2
My mail : perfect_cvv2@ymail.com
Hello, I'm a good seller, I have many friend hackers

My cvv are the best for you

Ccv US is $ 1.5per ccv(50ccv and up is 1$)
Ccv UK is $ 4 per ccv (50ccv and up is 3$)
Ccv Ca is $ 4 per ccv (50ccv and up is 3$)
Ccv EU is $ 7 per ccv (50ccv and up is 6$)
Ccv Au is $ 5 per ccv(50ccv and up is 4$)
Ccv Italy is 15 $ per ccv(50ccv and up is 12$)

UNITED STATES
Alabama
Alaska
Arizona
Arkansas
California
Colorado
Connecticut
Delaware
District of Columbia
Florida
Georgia
Hawaii
Idaho
Illinois
Indiana
Iowa
Kansas
Kentucky
Louisiana
Maine
Maryland
Massachusetts
Michigan
Minnesota
Mississippi
Missouri
Montana
Nebraska
Nevada
New Hampshire
New Jersey
New Mexico
New York
North Carolina
North Dakota
Ohio
Oklahoma
Oregon
Pennsylvania
Rhode Island
South Carolina
South Dakota

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE

What is a privacy incident going to cost me?

Ponemon Institute 2010 (cont.)

- Data Breaches from malicious attacks are up 7% from 2009 having doubled the year before. The cost per compromised record for these types of breaches has skyrocketed to $214 per record. This increase reinforces the extreme danger hostile breaches pose.

- Class Action suits from breach victims have yet to gain traction as it is difficult to prove damages. (It's just a matter of time)

- Average cost of a data breach in 2009 was $6,751,451

- Your reputation

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



Summary of Ponemon Institute, LLC's 2010 Annual Study: Cost of a Data Breach:

- Continued trend of increased average cost per breach, $7.2 million
- Direct costs increased 22% to $73 per record. (legal counsel, notification letters, credit monitoring, etc.) The increase is driven by the rising legal defense costs.

Cost by industry class	Per record
Average	$214
Education	$112
Retail	$185
Healthcare	$301
Financial Institutions	$353

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



Unplanned Cash Flow

- State and/or Federally Mandated Notification Costs
- Forensic Investigation, Data Restoration Expenses, Assets Damage
- Brand Preservation:

  Voluntary Notification, Credit Monitoring, Public Relations Expense
- Defense and Indemnity Expense from 3rd party allegations
- Regulatory Defense Costs
- Regulatory Fines and Penalties
- Business Income Loss



5) Identity and Access Management

- Key Risk
  - Unauthorized or excessive access
  - Segregation of duties issues exist
- Potential Impact
  - Fraud
  - Lack of reliance on system controls and need for manual controls
  - Compliance issues
- Recommended Control Activities
  - Performance of segregation of duty analysis before granting additional access to an account
  - Implement process for periodic review of access rights
  - Implementation of role based security
  - Multiple factor authentication – tokens, key fobs, digital certificates, biometrics
  - Centralized provisioning of users and the rights they have been granted.



5) Identity and Access Management

- 48% of all breaches in 2010 were caused by internal sources:
  - 50% of the breaches caused by insiders revolved around misuse of system privileges.
  - In 2009, 90% of all internal data breaches were deliberate.

Regular employee/end-user	51%
Finance/Accounting	12%
Network Administrator	12%
Executive/upper management	7%
Helpdesk staff	4%
Software Developer	3%
Auditor	1%
Other (Third parties)	9%

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



6) Physical Security

- Key Risk
  - Servers that house core business applications are not protected from unauthorized access and environmental hazards
- Potential Impact
  - Data loss
  - Data theft
  - Business interruption
  - Damage to critical equipment
- Recommended Control Activities
  - Maintain an accurate server and application inventory listing
  - Control access to server room
  - Uninterruptable power supply
  - Environmental controls (temperature/humidity controls, fire alarms/suppression, raised floors)

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE

6) Physical Security

- In 2011, over 10 million records were breached due to 114 incidents where backup media was lost or stolen.
- If backup tapes or other media is encrypted and stolen or lost, then the data on the device is not considered breached.



7) Business Continuity

- Key Risks
  - Failure to provide products or services
  - Failure to meet contractual service level requirements
  - Survival of organization
- Potential Impact
  - Loss of customers/clients
  - Decrease in value of organization (stock)
  - Cash flow problems
- Recommended Control Activities
  - Awareness of senior management and BOD responsibilities for risk management
  - Business impact assessment process (Maximum Tolerable Outage)
  - Development of a Business Continuity Plan – Utilize internal resources as much as possible
  - Periodic testing of plan

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE

7) Business Continuity

- For Companies that are directly affected by disasters and do not have a plan in place:
  - Only 8% survive long term
  - 40% fail within 18 months
  - 12% fail within five years
  - 40% never re-open
- Out of 330 companies surveyed by CIO magazine, 43% have no contingency plan.
- Of the 187 companies with a plan, only 18% have tested their plan.

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



8) Backup and Recovery

- Key Risk
  - Critical business information is lost and cannot be recovered
- Potential Impact
  - Data loss
  - Financial misstatement
  - Business interruption
- Recommended Control Activities
  - Create a data retention and backup schedule that is aligned with the business requirements
  - Daily backups of key business applications and data
  - Monitoring of backups
  - Backup restoration testing to ensure recoverability
  - Off-site storage of backup media

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



9) Third Party Vendors

- Key Risks
  - Loss of data confidentiality and integrity
  - Unauthorized use and tampering with customer data
  - Failure to meet service level requirements
- Potential Impact
  - Benefits and efficiencies not recognized
  - Theft of critical information
  - Compromised internal control environment
  - Business processes become less effective
- Recommended Control Activities
  - Require a SSAE 16, SOC 2 or “right to audit” clause in all contracts
  - Definition and monitoring of specific service-level targets, which must be achieved as part of the outsourced service’s delivery
  - Evaluation of controls, risks and financial solvency of vendor
  - Web banking applications are OWASP compliant



10) Industry Issues – Commercial Banking

- Commercial Banking – the ability to provide your customers with an array of services via the internet
  - Cyber criminals are targeting commercial accounts.
  - Business accounts are not afforded the same legal protections that consumers are given.
  - Cyber criminal's tool box consist of; viruses, spybots, key loggers and malicious emails - all are used to steal user credentials
  - Due to the increase in criminal activities the FFIEC has enact the Supplemental Guidance on Internet Banking Authentication

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



10) Industry Issues – Anomaly Detection

- What is Anomaly Detection?
  - It is the process of detecting something unusual.
  - In the online banking world if means detecting unusual online banking behavior in order to identify possible fraudulent activity.
  - Three types
    - Individual Account Holder Activity – preferred by FFIEC
    - General/population based
    - Based on Website traffic



10) Industry Issues – Anomaly Detection (continued)

- Why did the FFIEC mandate Anomaly Detection Systems?
  - All the tools in the hackers tool box have one thing in common- they require interaction with the online banking system.
  - Because of this, this is where the financial institutions have the best opportunity to stop the fraudulent attacks by looking for unusual online banking activity.
  - It defeats the widest range of threats
  - Has no impact on the customer's experience
  - Does not require the account holder to install or maintain any tools or software
  - Is transparent to the criminals

10) Industry Issues – Anomaly Detection (continued)

- How does it work?
  - Create and continually update a model of behavior for each account holder
  - Monitor every online banking transaction from start to finish
  - Capture and analyze the various components of each transaction and compare to the profile developed for the account holder.
  - Components consist of items such as: payees, time of day, frequency and type of transactions, how they access the account, amounts and other types of information



10) Industry Issues (continued)

- Mobile Banking Fraud – allowing customer to access financial services using a mobile smart phone.
  - Mobile malware increased 155% in 2011. Most of the increase is tied to the android app market.
  - SMS Trojans and spyware makes up 98% of the mobile malware
  - Mobile banking is really internet banking – different type of device with additional vulnerabilities.

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE



10) Industry Issues (continued)

- Mobile Banking Controls
  - Strong Device Passwords
  - Malware Protection
  - Firewall Protection
  - Remote wipe capabilities
  - Encryption for data storage and transmission
  - Education and awareness
  - Out of Band authentication
  - Layered Security framework

SCHNEIDER DOWNS

INSIGHT ▪ INNOVATION ▪ EXPERIENCE

Questions