

IT Regulatory Hot Buttons

Answer by: [Jimmy Sawyers](#), BOL Guru

Question: As it relates to IT examinations, what are the top "hot buttons" for regulators?

Answer: Never in the history of financial institution IT examinations has there been more IT to examine or greater regulatory scrutiny of the IT area. Your next IT examination will be like no other that you have ever experienced before. Y2K focused more attention on IT, but that attention had a shelf life. On January 1, 2000, financial institution management could breathe a sigh of relief. Not anymore. IT examinations are here to stay and they are not getting any easier.

It is almost ironic that IT is treated separately in examinations. The whole financial institution is basically a communications network. IT is pervasive and extends to every area of the financial institution. Accordingly, the scope of IT examinations is being extended, and examiners are learning more about IT.

Every person is influenced by his or her background and recent experiences. Regulators are no different. Certain hot topics become top of mind with IT examiners due to recent training they received, new regulations, new technologies and what is being discussed in the media. This is not to say that regulators have blinders on when it comes to IT examinations, but it might behoove you to pay attention to the latest regulator "hot buttons." You will be better prepared for your next IT examination.

While not an all-inclusive list, here are six hot buttons of recent note:

1. **Business continuity planning**

The effects of the 9/11 terrorist attack are far-reaching and will be felt for generations to come. The immediate effect as it relates to IT examinations is an increased emphasis on business continuity planning. Many tragic, yet valuable lessons were learned by financial institutions located near Ground Zero. While your next disaster is not likely to be one of such magnitude, 9/11 has thrust the topic of business continuity back to the forefront.

2. **The Gramm-Leach Bliley Act and Information Security**

In 2001, financial institutions management dealt with the privacy issues surrounding The Gramm-Leach Bliley Act (GLBA) and many thought their job was done. Not so fast. Section 501(b) of the GLBA has management hopping again to comply with the Guidelines Establishing Standards for Safeguarding Customer Information. The old saying, "There is no privacy without security" rings true once again.

IT examiners are also using the GLBA to enforce old recommendations like review and control over user access to new recommendations like reviewing firewall logs. The GLBA has given examiners more ammunition to make financial institution management take notice of IT exam recommendations.

3. **IT Risk Management**

A big part of GLBA is the risk assessment process. Examiners want to see how the institution assesses IT risk as it relates to customer information systems and non-public customer information. Institutions should be taking steps to identify foreseeable threats and assess the likelihood and potential impact of such threats.

4. **User Access Controls**

Controls over user access is nothing new to IT examinations, but greater scrutiny is now placed on how users are granted access, how often that access is reviewed for appropriateness, and how change management is employed. For example, if users are added to the core processing system with virtually, unlimited access to all applications and all functions, you have a problem. User access should be based on need, while observing age-old controls such as segregation of duties and dual control.

5. **Network Security**

Firewalls, intrusion detection systems, network operating system security, virus protection, remote access, network infrastructure issues, all of which did not show up on an examiner's radar just a few short years ago, are now hot topics. Be prepared for ambiguous questions about specific systems. Do you review firewall logs? If so, how do you respond to known attacks? How is remote access granted to users, including vendors? Do you have a complete, detailed schematic of your network? When was your last vulnerability scan? Have you engaged an outside firm to perform a vulnerability assessment or penetration test? All serious questions. Be prepared to articulate your position and efforts.

Know the difference in a vulnerability scan and a penetration test. Network security technology is still fairly new so much of the terminology has double meaning based on the context of the question or answer. Perhaps you have a monthly vulnerability scan of your firewall complete with a detailed report showing detected vulnerabilities, their related risk and the ease of fix. Perhaps you have engaged consultants to perform a penetration test that includes physical attempts to enter restricted areas of your financial institution.

Get to know your network, document it thoroughly and be prepared to verbally describe your network infrastructure during interviews with the examiner.

6. **Directorate Awareness of IT Activities**

Most Board of Directors meetings are dominated with discussion of financial issues, typically lending, capital expenditures and investments. While vitally important to the safety and soundness of the institution, IT is not always discussed. Some boards are very attune to technology and devote a significant amount of time and effort to understanding the financial institution's IT environment. More often, any discussion of IT at board meetings is met with glazed looks and glances at watches.

With the current regulatory environment and the push for more corporate responsibility, board members are learning that some aspects of technology can be outsourced, but their responsibility for oversight cannot. At a minimum, the Directorate should understand the impact of IT controls on the integrity of the financial statements. One of the best methods to maintain directorate awareness of IT activities is to reference the Information Systems Steering Committee, or similar committee, minutes in the Board of Directors' meeting minutes.

Good luck on your next examination.

Note: This information appeared originally in Jimmy's book, [IT Auditing for Financial Institutions](#), available in the BOL Banker Store.

Surviving Your IT Exam

Answer by: [Jimmy Sawyers](#), BOL Guru

Question: I've heard that IT examinations are much more rigorous these days. What are some general tips for surviving our next IT examination?

Answer: Formerly a blip on the regulators' radar, information technology has become the subject of intensive examinations in recent years. An army of former safety and soundness examiners now has their IT examiner stripes and they are ready for battle. Regulators now devote more resources to the IT examination than ever before. Accordingly, the IT examination rating your financial institution receives has become much more significant than in years past.

To help you survive your next IT examination, we have the following tips:

1. **Avoid repeat findings.** Nothing will bring your rating down like repeat findings. Ignore past findings at your own risk. It is a good idea to review the previous report of examination prior to your next examination. This will allow you to blitz any outstanding items and avoid this costly mistake.
2. **Don't overpromise.** The easiest thing to do when responding to examination findings is to say that you will correct every finding right away. Unless you are in violation of the law, keep in mind that there are some IT risks that you might be willing to accept. Articulate your response carefully and follow through on your commitments.
3. **Be aware of regulatory hot buttons.** Don't be blindsided by being unaware of what is foremost in the minds of examiners (e.g., Section 501b of the GLBA). Review the regulators' work programs which are available online, seek the advice of your external IT auditors and consultants, read industry publications, attend conferences on IT issues, and network with your peers.
4. **Be prepared.** It's not just the Boy Scout motto, it's a good practice to complete your examination successfully. When you receive the examiner's "request for information," tackle it immediately, gather the information requested, index it to the examiner's documentation, and have it ready when the examiner arrives.
5. **Use the exit conference wisely.** The exit conference is an excellent forum to clear up any miscommunication or misunderstanding, on either the examiner's part or your part. Don't rush through the conference, thinking ahead to the report. Instead, take copious notes, ask the examiner to explain his or her findings in great detail, and include the appropriate people in the conference so certain items can be addressed immediately. While it should go without saying, this is also the time to turn off cell phones, hold all calls and devote your management team's full attention to the exit conference.

Being on the receiving end of an IT examination is never easy. By properly preparing for the examination, communicating effectively during the examination, and responding promptly and thoughtfully to examination findings and recommendations, you can help your financial institution not only survive the examination but emerge with a better, more secure IT environment that will contribute to the safety and soundness of the entire institution.

Note: These tips appeared originally in Jimmy's book, [IT Auditing for Financial Institutions](#), available in the BOL Bookstore.

Tips For Developing IT/InfoSec/GLBA Policies

Answer by Andy Zavoina, BOL Guru

[BIO AND CONTACT INFO](#)

Question: We are in the process of developing a more comprehensive IT/Information Security policy for our growing institution. What recommendations can you make regarding content that will insure compliance with regulators? Are you aware of any sample policies that meet regulatory criteria that we can refer to for guidance? We are most interested in successful ways of incorporating GLBA requirements.

Answer: Because systems and requirements change, a solid "one size fits all" template would be difficult. Review your examination materials and try to answer as many questions as possible to your satisfaction, and hopefully to your examiners as well.

<http://www.ffiec.gov/guides.htm>

You can also look at this [guidance](#) from Bonnie Mizrahi.

First published on BankersOnline.com 3/17/03

Verification Of Source Documents For Master File Changes

by John Burnett, BOL Guru

[BIO AND CONTACT INFO](#)

Question: Are we required to verify source documents for master file changes (file maintenance)? Our system produces a daily report listing what was changed (the from and to) and who changed it. Do we really have to compare the source document to the report produced by our system?

Answer: Verification of source documents on a sample basis will provide a control over errors and potential misdealing by staff. One of the easiest ways to "mess with" a customer's accounts is to change an address and have statements routed elsewhere.

While it may not be feasible to do a 100% verification of all source documents, I think that verifying a random sample on a regular basis helps keep your staff honest and your auditors satisfied concerning your controls.

First published on BankersOnline.com 05/5/03

Internet and/or Technology Incident Response Sample Policies & Procedures

Answer by Mary Beth Guard, BOL Guru

[BIO AND CONTACT INFO](#)

Question: Does anyone have some sample policies and procedures regarding Incident Response relating to Internet and/or Technology or any suggestions as to what points should be included?

Answer: In an incident response plan, you want to cover the following topics, at a minimum:

Identify possible "incidents" before you do anything else. This can be done in a brainstorming session, and you can get additional ideas from the Net.

1. Figure out how you can spot critical incidents. Who will be monitoring what?
2. Determine who should get notice of various types of incidents. For example, if your Web site goes down, who should be notified and how. If there is an unfriendly employee termination, who needs to know about it. If a laptop is stolen, or a password is compromised, who do you tell.
3. Decide if you can streamline some types of reports by developing report forms and/or checklists.

4. Mitigate damage. Act immediately to control the possible negative consequences of the incident. For example, if a disgruntled employee has just been fired, remove their permissions from the network and any special software they can access. If you use secure modems, remove their IP address and user name/password from the set of permissible accessors. Do not allow them to access their computer or any others within the organization. Try to determine whether it's possible they had access to anyone else's passwords or access rights. If so, force a change of those passwords. If your network has been infected with a Worm that propagates via email, take your email server down until the worm has been cleaned off your system in order to avoid further spreading it.
5. Bring in outside experts, if necessary, to troubleshoot and contain the problem. You may need computer forensics experts, for example, or you may wish to notify the FBI. If someone has hacked into your customer files, you need to marshal your PR resources.
6. If it fits the definition of "computer intrusion", file a SAR. Identify the systems that have been compromised.
7. Protect the evidence. The Secret Service Web site has excellent guidance on preserving electronic evidence.
8. Restore data from backups, if necessary.
9. Schedule a post-mortem review. Determine what you need to do differently and what you learned from the experience. Make whatever changes need to be made as a result.

First published on BankersOnline.com 04/07/03

Conducting An Information Technology Risk Assessment

Answer by Trent Fleming and Jimmy Sawyers, BOL Gurus

Question: I would welcome any suggestions regarding how to conduct an information technology risk assessment.

Answer by Trent Fleming:

[BIO AND CONTACT INFO](#)

There are a number of regulatory bulletins and privately produced guides for this.

Basically, you want to identify all operational systems, and their inputs and outputs. Then, take a look at your exposure to loss, unauthorized access, excessive downtime, etc.

Then, begin to assess the risk to your bank's operations if one or more of your considered risk scenarios plays out.

Answer by Jimmy Sawyers:

[BIO AND CONTACT INFO](#)

Measuring IT risk calls for different approaches based on the situation. You can take a qualitative or quantitative approach. For example, if you are referring to performing the risk assessment for the GLBA, you could take a qualitative approach and write a narrative of the assessment, assigning risk categories (e.g., high, medium, low) to each area. Or, you could take a quantitative approach, assigning values based on: 1. The Threat Likelihood/Probability of Occurrence, and; 2. The Magnitude of Impact. These values can be multiplied to obtain a risk ranking.

Each individual area can then be categorized into a risk summary. Then, you can identify which risk areas you plan to mitigate through your Risk Mitigation Action Plan. This also serves as an excellent tool for board reporting and monitoring the plan's progress.

We prefer the quantitative approach because you can establish very granular ratings for baselines and benchmarks, plus you can more easily involve several people in the exercise,

gaining a consensus and avoiding one person setting the institution's overall risk management program.

Another approach to IT risk assessment involves considering the bank's complete IT environment and related sections to be included in the risk assessment. This approach allows a more comprehensive, yet general view of IT risk.

A Significance Ranking can be assigned (i.e., How significant is this area as it relates to the bank's overall IT environment? Consider recent developments within the industry, regulatory issuances and the importance of this area to the bank). Then, you can assign a second value, a Risk Factor, measuring the related risk in this particular bank. The two values can be multiplied to ascertain the Risk Rating for this item.

We cover both of these practical approaches to measuring IT-related risk in our book, [IT Auditing for Financial Institutions](#), available in the BankersOnline Banker Store.

First published on BankersOnline.com 2/3/03