2018 OBL TECHNOLOGY CONFERENCE

IT Regulatory Panel

Regulatory Panel Topics

- **Cybersecurity Assessment Tool Update**

  By: Steven Scott – OCC

- **Risk Assessment Reminders**

  By: Scott Kennedy – ODFI

- **Strengthening Cyber Resilience**

  By: Jay Restel – FRB

- **Importance of Change Controls**

  By: Kevin Schmidt – FDIC

Office of the Comptroller of the Currency

2018 OBL TECHNOLOGY CONFERENCE
IT REGULATOR ROUNDTABLE
CYBERSECURITY ASSESSMENT TOOL

National Bank Examiner Steve Scott

Office of the Comptroller of the Currency

CAT

- FFIEC CAT 2017 V.1 Findings: Central District
- Not Stellar- note only takes one no response to not reach baseline.
- Not sharing actual numbers due to security concerns.
- Baseline is aligned with FFIEC/OCC guidance and is minimum expectation.
- Inherent risk levels and Maturity levels.
  - -Least, minimal, moderate, significant, most.
  - - Baseline, Evolving, Intermediate, advanced, innovative .
- MRAs have increased and are high due to more in depth reviews.

- What's New?
- CAT V.2 Declarative Statement- Yes-No-YCC- Yes with compensating controls
  - The bank practice is more stringent than the statement. E.g. the statement calls for a manual process but the bank has an automated process at a higher maturity.
  - The bank practice does not meet the exact/prescriptive description of a control in the declarative statement, but the bank is able to demonstrate sustained and effective controls that achieve the control objective.

Office of the Comptroller of the Currency

CAT YCC

- YCC is <u>not</u> appropriate to use when:
  - The bank practice (control) is in development or is an immature process.
  - Bank management states that they have achieved the control objective of the declarative statement, but they are unable to provide sufficient evidence to demonstrate that they have achieved it.
  - The examiner is unsure if the bank practice achieves the control objectives of the declarative statement or is unable to find/obtain documentation to evidence a sustained/effective control to achieve the control objective.

CAT

- Regulator Expectations:

  -FFIEC CAT / OCC Bulletin 2015-31

  -Optional

  -Involve your Board- OCC Directors Workshops Ops Risk.

  -Get on the Board meeting agenda at least quarterly.

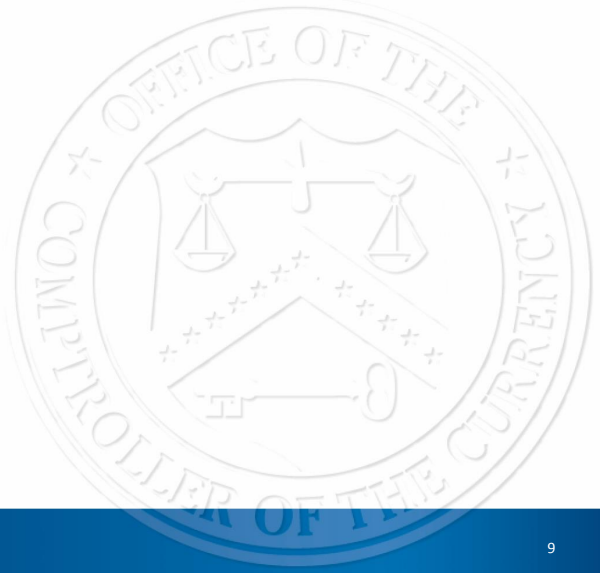
  -Appropriate strategy and budget that has contingency amounts for unplanned events.

Cybersecurity Examination Procedures for SPs

CEP v.2 Update

- Piloting the CEP v.2 at several SSP's
- Feedback incorporated 1Q 2018

Questions?



Ohio | Department of Commerce

Risk Assessment

Scott Kennedy
IT Supervisor
Division of Finance Institutions

Safe. Sound. Secure.

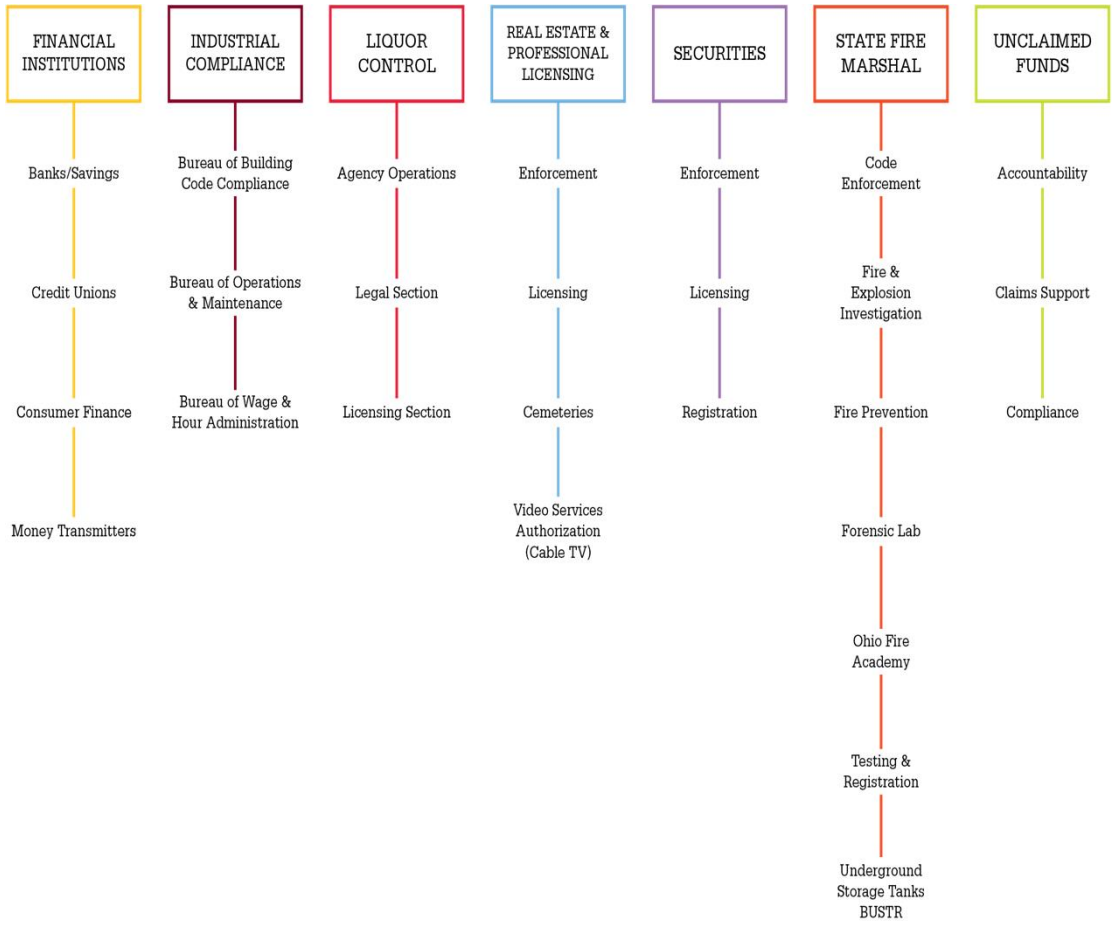
Ohio | Department of Commerce

Division of Financial Institutions

The Ohio Department of Commerce is focused on equipping businesses and protecting consumers.

Commerce has seven Divisions including (insert your Division here).

Our goal is to keep Ohioans safe, sound and secure.



Safe. Sound. Secure.

What is a risk assessment?

Risk assessment: A prioritization of potential business disruptions based on severity and likelihood of occurrence. The risk assessment includes an analysis of threats based on the impact to the institution, its customers, and financial markets, rather than the nature of the threat.

Risk Assessment Process

- All activities have a degree of risk, but the goal is to mitigate the residual risk down to an acceptable level. Start with Assets (firewalls, servers, routers, technologies, vendors, software products for loans, etc.)
- Add Inherent risk rating (High, Medium, Low – 3 or 5 position scale). This is risk before mitigation. Likelihood of loss or occurrence times Impact.

Risk Assessment Process - Continued

- Put in controls to help lower the inherent risk. (IDS/IPS, Multifactor Authentication, Access controls, Policies and Procedures, BCP, etc.)
- The result is Residual Risk. The amount of risk left over after controls are implemented. Board must accept the remaining risk, based on risk appetite.

Common Findings

- Not updating on an ongoing basis or not updating of the risk assessment promptly for new and or emerging risks,
- Not identifying all controls / assets
- Lumping assets in broad categories ï need to list them out
- Not addressing higher residual risk
- Not identifying critical service providers (Cloud)
- Not stating the frequency of testing of controls

Cyber Risk Assessment

- Additionally, management should develop, maintain, and update a repository of cybersecurity threat and vulnerability information that may be used in conducting risk assessments and provide updates to senior management and the board on cyber risk trends.
- Based on the institutionôs risk assessment, the controls should include, but may not be limited to, patch management, asset and configuration management, vulnerability scanning and penetration testing, end-point security, resilience controls, logging and monitoring, and secure software development (including third-party software development).

Risk Assessments

- Maintaining hardware and software inventories helps ensure assets are covered.
- Conducting risk assessments on systems and applications to help determine end-of-life.
- The need to encrypt data is determined by the institutionôs data classification and risk assessment.

Board Reporting

Management should provide a report to the board at least annually that describes the overall status of the program and material matters related to the program, including some of the following:

- Risk assessment process, including threat identification and assessment.
- Risk management and control decisions, including risk acceptance and avoidance.
- Results of testing.

Closing

- Remember the common findings and try to learn from other bankers.
- Remember risk assessments are your friends.

Cybersecurity Assessment Tool (CAT)

- Who uses the CAT? Other frameworks (NIST, ISO or Homeland Security)?
- ODFI is tracking the CAT. Most banks and Credit Unions are using it.
- Failure to do a gap analysis afterwards
- Not meeting baseline
- Not completing the CAT or other framework.
- Not monitoring threat information and vulnerabilities (i.e., FS-ISAC, US-CERT, InfraGard)

Guidance

- FFIEC IT Handbook
- FIL-68-99, ñRisk Assessment Tools and Practicesò(July 7, 1999)
- NIST SP 800-30, Revision 1 ï ñInformation Security: Guide for Conducting Risk Assessmentsò(September 2012)

Ohio Bankers League Roundtable

Cyber Resilience

April 2017

Jay A. Restel
Banking Supervisor – IT Operational Risk and Resiliency
Federal Reserve Bank of Cleveland

The Disclaimer…..

The views stated herein are those of the author and not necessarily those of the Federal Reserve Bank of Cleveland or of the Board of Governors of the Federal Reserve System.

FFIEC Definition of Cyber Resilience

- The FFIEC Information Security booklet defines **cyber resilience** as the ability of a system or domain to withstand cyber-attacks or failures and, in such events, to reestablish itself quickly.
- Cyber resilience can be further defined as the ability to proactively manage and minimize damage or disruptions from a cyber-event and recover and resume operations in a controlled and timely manner.
  - Ability to withstand and resist a variety of cyber-events (e.g., Ransomware, Malware, Phishing, and DDoS).
- Cyber resilience requires effective risk management and redundancy and resilience of people, processes, and technology.

Cyber Resilience Fundamentals

- Ensuring effective coordination between information security and business continuity organizations
- Designing, implementing, and maintaining resilient architecture
- Maintaining a sound cyber incident management program
- Maintaining an evolving cyber resilience testing regimen

Cyber Resilience - Key Areas

Governance

- The effectiveness and comprehensiveness of a firm's governance over cyber resilience
- The establishment of a strong and sustainable cyber resilience program in alignment with its cyber resilience strategy to address cyber events and protection of services and assets
- Program should be visible and integrated with firm enterprise risk management program and broader business continuity and incident response management programs to enable business decisions and prioritization.

Cyber Resilience - Key Areas (Continued)

Testing

- Cyber resilience capability strategies should be effectively developed, planned, tested, and maintained as part of the enterprise-wide BCP testing process.
- Conducting various cyber event scenarios, including potential issues encountered during a wide-scale disruption

Recovery and Resumption

- Development of appropriate risk management over the firm's recovery and resumption programs and processes to recover and resume operations in the event of a cyber incident

FFIEC Business Continuity Planning Booklet (BCPB)

- The BCPB recognizes table top exercises and walk-throughs as a preliminary step in the overall testing process, but they are not a preferred testing methodology.
- The BCPB indicates that testing should be viewed as a continuously evolving cycle and institutions should work towards more comprehensive testing over time.

Challenges Observed

- Ineffective integration and coordination into existing programs (e.g., Info Security, Business Continuity)
- Sensitive information sometimes not encrypted
- Solutions to address simultaneous corruption of primary and back-up data not fully implemented
- Firms currently relying solely on tabletop/walkthrough exercises. This also includes industry/street tests (e.g., FS-ISAC)
- Cyber resilience, while being tested in some form, often is not specifically integrated in traditional BC/DR program.
- Minimal cybersecurity testing with third parties

Examples of Advanced Type Testing

- Industry Tests (e.g., FS-ISAC, FBI, DHS, Treasury)
- War games – Virtual environments created for war games (sometimes multi-day)
- Red/Blue team testing:
  - Example: Red Team testing with the intent to test advanced persistent threat scenario with additional focus on the critical operating environment (wire and payments)

Summary

- Cyber threat landscape challenges firms to keep pace
- The ability to resume operations after an attack is highly reliant on the firms' capability to know which assets are compromised and how well the firm can ensure data integrity.
- Alignment of cyber incident response to the broader enterprise incident management program
- Continue to increase the complexity and robustness of cyber resilience testing and further include exercises of activities that would be needed during an actual cyber incident
- Coordinate with service providers

Questions?

The Importance of Change Controls

OBL 2018 Technology Conference

Senior Risk Examiner Kevin J. Schmidt

Disclaimer

- **All opinions are the opinions of the presenter and do not necessarily reflect the positions of the FDIC.**

Worst Case Scenario

_____ Breach Caused by Lone Employee's Error, Former C.E.O. Says

- NY Times, October 3, 2017

Forbes: October 6, 2017

- ñ*The Equifax data breach, which exposed the sensitive personal information of nearly 146 million Americans, happened because of a* ***mistake by a single employee****, the credit reporting company's former chief executive told members of Congress.*ò

KrebsonSecurity 10/17/2017

- ñThe human error involved the failure to apply a software patch to a dispute portal in March 2017,òSmith said.

Purpose of Internal Controls

- Control systems should be designed to provide reasonable assurance that appropriately implemented internal controls will prevent or detect:
  - Materially inaccurate, incomplete, or unauthorized transactions;
  - Deficiencies in the safeguarding of assets;
  - Unreliable financial and regulatory reporting; and
  - Deviations from laws, regulations, and internal policies.

Financial Change Controls

- **Common controls on the financial side of the bank with a high risk transaction:**

  Example with a wire transfer -

  - One staff member initiates a transaction
  - A second staff member finalizes the transaction
  - A third staff member verifies the accuracy of the transaction

Common IT Change Controls?

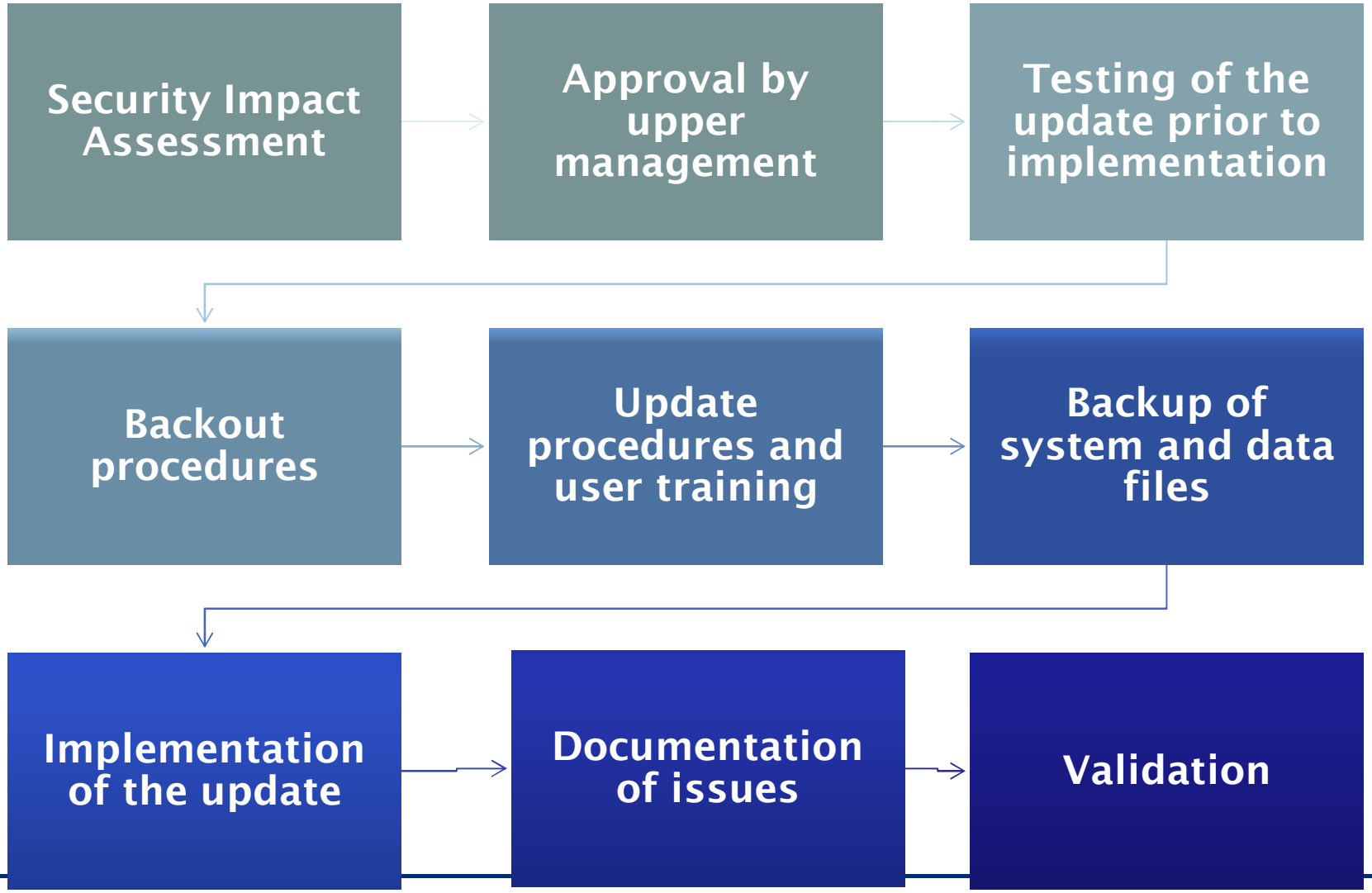
- **Common controls in many IT departments on high risk or critical changes:**
  - One IT administrator implements the change
  - Same IT administrator is responsible to verify the accuracy and validate it was done correctly.

Equifax Fatal Flaw

- **No validation or confirmation was completed on the change control request**
- **Over-reliance on scanning software**

Could the Equifax scenario occur with your institution?

Change Control Process



Change Management and Security

- **Importance of security:**

  As IT system complexity **increases**

  ⇨ Complexity in creating these systems **increases**

  ⇨ Probability of errors **increases**

  ⇨ Operational risk and the likelihood of security vulnerabilities **increases**

- **Change management is a GLBA key control, but frequently not audited or reviewed**

The Point

Validate

Validate

Validate

Questions?