9.03 USING A CONTROL FRAMEWORK FOR IT AUDITS

Patrick Sickels, CISA, CRISC
CU*Answers
800.327.3478 x335
psickels@cuanswers.com
October 30, 2012

WHAT IS A CONTROL FRAMEWORK?

Examiners use control frameworks to help review the security and effectiveness of IT controls. Using a framework at the credit union can help build confidence in the examiner that the credit union is well run and does not present a security risk to member data.

Frameworks also ensure a consistent risk management and audit methodology.

ISACA: EVIDENCE

ISACA sets forth standards and guidelines that an organization can use. For example, with respect to evidence supporting a finding, ISACA provides the following guidance:

When planning the IS audit work, the IS auditor should take into account the type of audit evidence to be gathered, its use as audit evidence to meet audit objectives and its varying levels of reliability. Amongst the things to be considered are the independence and qualifications of the provider of the audit evidence. For example, corroborative audit evidence from an independent third party can be more reliable than audit evidence from the organization being audited.

Physical audit evidence is generally more reliable than the representations of an individual.

ISACA: SAMPLING

Random sampling: Ensures that all combinations of sampling units in the populatio have an equal chance of selection

Systematic sampling: Involves selecting sampling units using a fixed interval betwee selections, the first interval having a random start. Examples include Monetary Un Sampling or Value Weighted selection where each individual monetary value (e.g., $1) i the population is given an equal chance of selection. As the individual monetary un cannot ordinarily be examined separately, the item which includes that monetary unit selected for examination.

Haphazard sampling: The IS auditor selects the sample without following a structure technique, while avoiding any conscious bias or predictability. However, analysis of haphazard sample should not be relied upon to form a conclusion on the population

Judgmental sampling: The IS auditor places a bias on the sample (e.g., all samplin units over a certain value, all for a specific type of exception, all negatives, all new users It should be noted that a judgmental sample is not statistically based and results shoul not be extrapolated over the population as the sample is unlikely to be representative o the population.

ISACA: REPORTING

Reporting criteria are the standards and benchmarks used to measure and present the subject matter and against which the IT audit and assurance professional evaluates the subject matter. Criteria should be:

Objective—Free from bias

Measurable—Provide for consistent measurement

Complete—Include all relevant factors to reach a conclusion

Relevant—Relate to the subject matter

ISACA: IS AUDIT

Physical and environmental review—This includes physical security, power supply, air conditioning, humidity control and other environmental factors.

System administration review—This includes security review of the operating systems, database management systems, all system administration procedures and compliance.

Application software review—The business application could be payroll, invoicing, a web-based customer order processing system or an enterprise resource planning system that actually runs the business. Review of such application software includes access control and authorizations, validations, error and exception handling, busines process flows within the application software and complementary manual controls and procedures. Additionally, a review of the system development lifecycle should be completed.

Network security review—Review of internal and external connections to the system, perimeter security, firewall review, router access control lists, port scanning and intrusion detection are some typical areas of coverage.

Business continuity review—This includes existence and maintenance of fault tolerant and redundant hardware, backup procedures and storage, and documented and tested disaster recovery/business continuity plan.

Data integrity review—The purpose of this is scrutiny of live data to verify adequacy of controls and impact of weaknesses, as noticed from any of the above reviews. Such substantive testing can be done using generalized audit software (e.g., computer assisted audit techniques).

ISACA: CHANGE MANAGEMENT

AI6.3 *Emergency changes*

Control objective—Establish a process for defining, raising, testing documenting, assessing and authorizing emergency changes that do not follow the established change process.

Value drivers:

An agreed-upon and standardized approach for managing changes in an efficient and effective manner

Formally defined emergency change expectations and performance measurement

Consistent procedure for emergency changes

Risk drivers:

Inability to respond effectively to emergency change needs

Additional access authorization not terminated properly

Unauthorized changes applied, resulting in compromised security and unauthorized access to corporate information

ISACA: FRAMEWORK

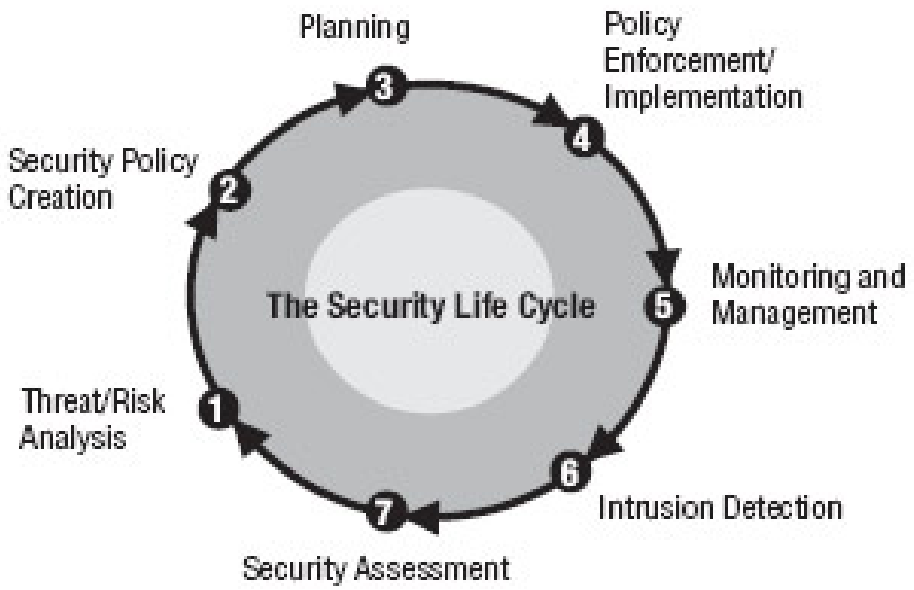
6.2 Control: Emergency changes are adequately tested before being placed into production.
6.2.1 Through interviews, observation and review of documentation, determine the process used to review testing procedures before an emergency change is accepted into production.
6.2.2 Determine if a list of authorized requesters for emergency changes exists.
6.2.3 Test objective: To verify that emergency change authorization was approved prior to the introduction of the change into the production environment
6.2.3.1 Select emergency changes from several sources.
6.2.3.1.1 Review the existence of test results and management review.
6.3 Control: Emergency changes are authorized by an appropriate member of management before being placed into production.
6.3.1 Through interviews, observation and review of documentation, determine the process used to authorize emergency moves to production. Differentiate between minor and major enhancements, operating system, configuration files and source programs.
6.3.2 Test objective: To verify that change authorizations were documented prior to the introduction of the change into the production environment
6.3.2.1 Select a representative sample of emergency changes.
6.3.2.2 Determine if the move into production was properly authorized.

ISACA: FRAMEWORK

IT RISK MANAGEMENT FRAMEWORK
Audit/Assurance Objective: The IT risk management framework is aligned with the ERM framework.
IT Risk Management Framework Definition
Control: The IT risk management framework utilizes a methodology and definitions that align with the ERM framework.
Obtain the IT risk management framework and the ERM framework.
Compare the two approaches and, if available, review documents and procedures.
Verify that the risk management processes are aligned and integrated with the ERM framework and related operational procedures.
Verify that the risk classifications are uniform and address strategic, program, project and operational activities.
Identify the scales used to classify risk: **Probability** **Expected losses/costs** **Materiality levels** **Nonfinancial factors**
Assess whether the IT risk scales align with the enterprise risk scales.
Identify gaps and misalignments between the two processes.

ISACA: DIAGRAMS

Figure 1—The Security Life Cycle



Source: Van Der Walt, Charles; "Assessing Internet Security Risk, Part One: What Is Risk Assessment?," *www.securityfocus.com/infocus/1591*

ISO: 27001

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF (Target of evaluation Security Functionality) shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

ISO: ADVANTAGES

ISO (International Organization of Standards) is well known, sounds impressive, and if actually certified (big $$$) then the examiners have much less opportunity to challenge the standards deployed by the organization (although they may still gripe about individual aspects of the security program.

IAA: GAIT

Guide of Assessment of IT General Controls

Phase 1: Identify (and validate if necessary) the critical IT functionality.

Phase 2: Identify the [significant] applications where ITGC need to be tested.

Phase 3: Identify ITGC process risks and related control objectives. This is the core of the GAIT methodology.

Phase 4: Identify the ITGC to test that meet control objectives.

Phase 5: Perform a "reasonable person" review.

IAA: GAIT

Category Description
Significant interfaces and the manual controls over them. You might need to add these to the list of key automated controls if they are not included as key controls, their failure would not be detected by the normal operation of key controls that have been identified, and they could lead to a material error.

The network infrastructure and its potential points of failure (e.g., the application and its key automated controls might be reliant on transmissions across the network, where a network failure or network security breach could reasonably likely result in an undetected material error in the financial statements).

Risk indicators
Certain indicators could signal a higher level of risk in IT processes. These should be considered when assessing risk:
How many and which key controls failed during prior period testing for §404 or during internal audits?
What is the age of the application, and how often is it modified?
Are there known problems with the processing or data?
Are there known problems with any important application functionality?
How extensively has a purchased application been modified, customized, and configured?
What is the backlog of high-priority change requests?
How often do processing problems occur?
How often are emergency changes made?
What is the level of staff turnover in key positions?
How experienced are the staff and have they received sufficient training?

COSO

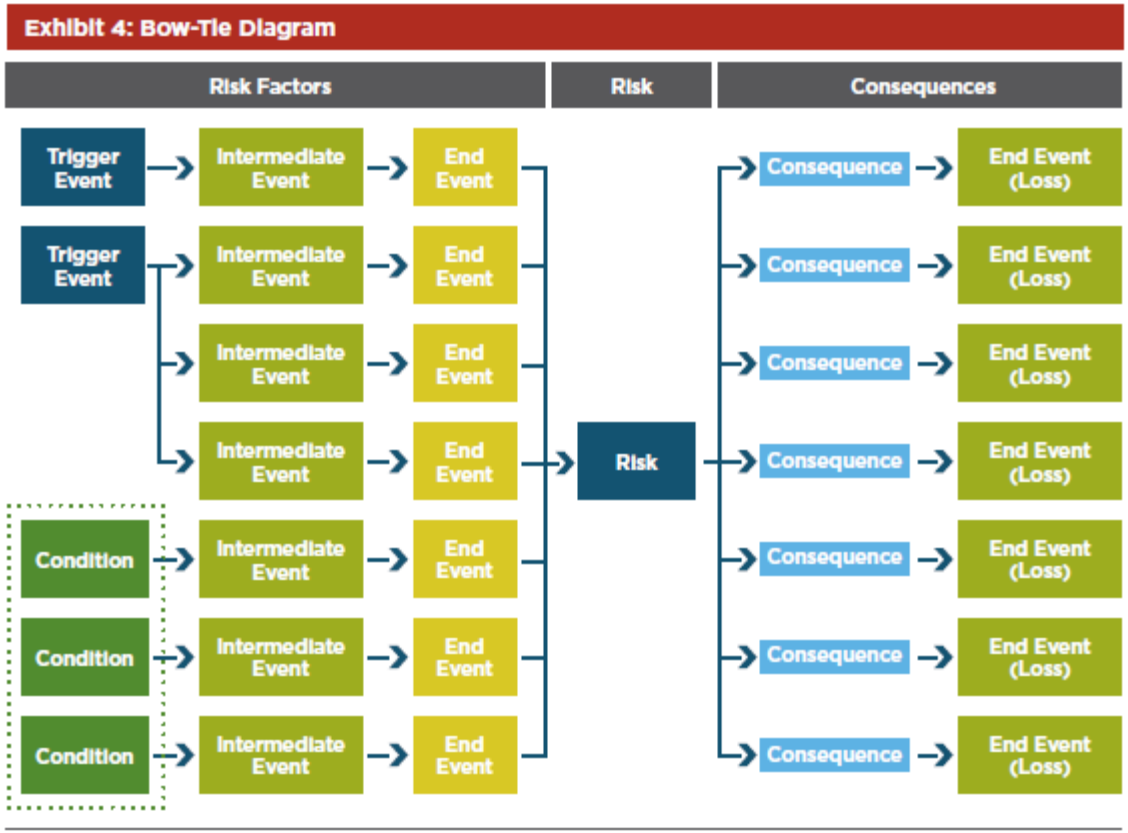


Exhibit 4: Bow-Tie Diagram
Risk Factors
Risk
Consequences
Trigger Event
Trigger Event
Condition
Condition
Condition
Intermediate Event
End Event
Risk
Consequence
End Event (Loss)

CONCLUSION

No framework is perfect

Scale to the size of your organization

Many times just important to sound good