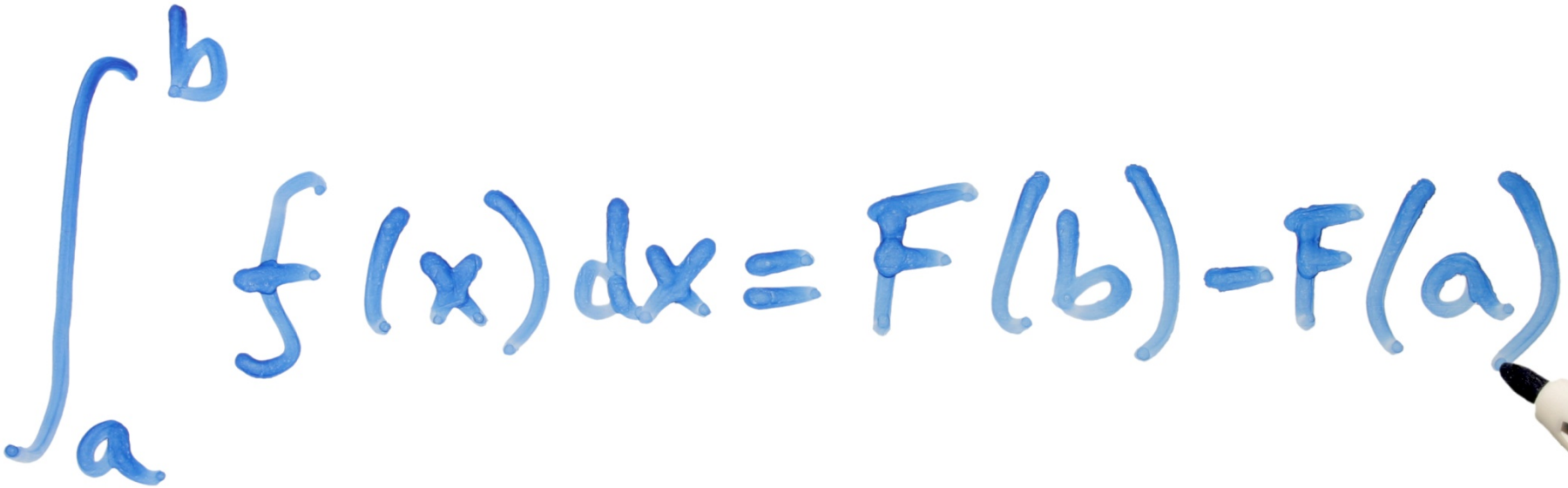


9.01 IT Risk Management: A Quantitative Approach

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

Quantitative Approach

Quantitative Approach to risk management asks the organization to track costs and ROI as part of the overall IT risk management process.

Use of numbers can help your credit unions during regulatory exams.

URSIT

- **Uniform Rating System for Information Security**

- Financial institutions and service providers rated composite “1” exhibit strong performance in every respect and generally have components rated 1 or 2.

- Financial institutions and service providers rated composite “2” exhibit safe and sound performance but may demonstrate modest weaknesses in operating performance, monitoring, management processes or system development.

- Financial institutions and service providers rated composite “3” exhibit some degree of supervisory concern due to a combination of weaknesses that may range from moderate to severe. If weaknesses persist, further deterioration in the condition and performance of the institution or service provider is likely.

- Financial institutions and service providers rated composite “4” operate in an unsafe and unsound environment that may impair the future viability of the entity.

- Financial institutions and service providers rated composite “5” exhibit critically deficient operating performance and are in need of immediate remedial action.

COMPONENTS: AUDIT

Financial institutions and service providers are expected to provide independent assessments of their exposure to risks and the quality of internal controls associated with the acquisition, implementation and use of information technology

External Vulnerability Assessment (Report to Supervisory Committee)

1. Penetration Testing
2. Assessment of IT department general controls
3. IT Risk Assessment to include Part 748, Appendix A
4. Security Assessment

Audit Plan

1. The risk assessment process
2. Employee & vendor access levels to critical systems
3. Employee compliance to IT & computer use policies
4. The vendor management process
5. Service auditor's reports and test whether "Client control considerations" are properly implemented by the applicable departments

CALCULATING AUDIT ROI

Audit Type	Cost	Notes
Penetration Test	$18,000	Competitively bid?

Network Security
Network Surveying
Port Scanning
System Identification
Services Identification
Vulnerability Research & Verification
Application Testing & Code Review
Router Testing
Firewall Testing
Intrusion Detection System Testing
Trusted Systems Testing
Password Cracking
Denial of Service Testing

Wireless Security
Wireless Networks Testing
Infrared Systems Testing
Communications Security
Voicemail Testing
Modem Testing

Physical Security
Access Controls Testing
Perimeter Review
Monitoring Review
Alarm Response Testing
Location Review
Environment Review

CALCULATING AUDIT ROI

Finding	Risk Level	Cost to Implement	Hours to Implement	Recommend
Finding 1	High	$1000	30 hours	Yes
Finding 2	Medium	$1500	15 hours	Yes
Finding 3	Low	$1000	30 hours	No

Other Considerations

1. Do external audit findings reflect examination findings?
2. Was credit given by examiners for remediating past findings?
3. What is the hourly cost of the engagement (total/hours)?
4. What are the yearly costs of remediation?

Use this information to determine ROI and what risks are acceptable based on the costs associated. Acceptable risks can be managed by showing this cost-benefit analysis.

COMPONENTS: MANAGEMENT

This rating reflects the abilities of the board and management as they apply to all aspects of IT acquisition, development, and operations ... Generally, directors need not be actively involved in day-to-day operations; however, they must provide clear guidance regarding acceptable risk exposure levels and ensure that appropriate policies, procedures, and practices have been established.

Policy Requirements

1. Information security program (risk assessments, tests of controls, training, board reports)
2. Designated security officer responsible for ensuring compliance (Appendix A, RR 748)
3. Physical access controls and environmental controls for the data center
4. System, network, e-mail, and database administration
5. Firewall, router, and server security management
6. Monitoring and backup of firewall and intrusion detection logs
7. Wireless communication
8. System access levels and administrative authorities granted by duty position
9. Password administration for critical systems (network & EDP system logon, home banking)
10. Use of encryption to protect sensitive data
11. Use of modems (these can undermine firewall protection if not properly managed)
12. Remote access for vendors and employees, if applicable
13. Frequency of system patches and updates, logs maintained
14. Virus protection and updates
15. Vulnerability scanning and penetration tests
16. Regulatory compliance of website content, e-forms, e-statements, applications, etc.
17. Vendor management (Procurement, Contract Reviews, Service Level Agreements, Due Diligence Reviews, Vulnerability Scans, SSAE-18, Business Continuity Tests, etc.)
18. Problem resolution and member service
19. Backup & recovery procedures
20. Testing of business continuity and disaster recovery plans

CALCULATING GOVERNANCE ROI

Project	Estimated Cost	Actual Cost	Variance	Estimated Completion	Actual Completion	Variance
Project A	$9,000	$13,000	$4000 (30%)	30 hours	40 hours	10 hours (25%)

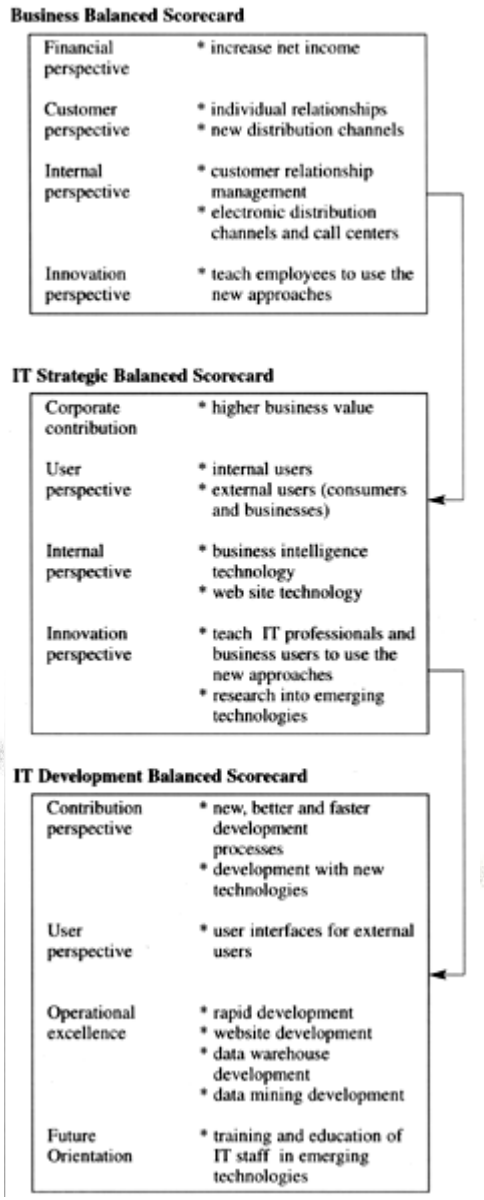
Executive managers and the board should have:
One page benefit analysis of the dollars spent on the project

Expected costs, dates and milestones (long term projects can be tracked on a quarterly or monthly basis)

Review project variances and make adjustments – are people overestimating or underestimating costs and project timelines?

GOVERNANCE SCORECARD

Figure 4 — Bank example of a cascade of scorecoards



Establish a scorecard for the organization:

- Did the project finish on time and on budget?
- Are variance times increasing or decreasing? Good reasons for delays or cost increases?
- Did the project meet its goals?

IT governance has to provide the organizational structures to enable the creation of business value through IT and the assurance that IT investments in bad projects is limited or (preferably) nonexistent.

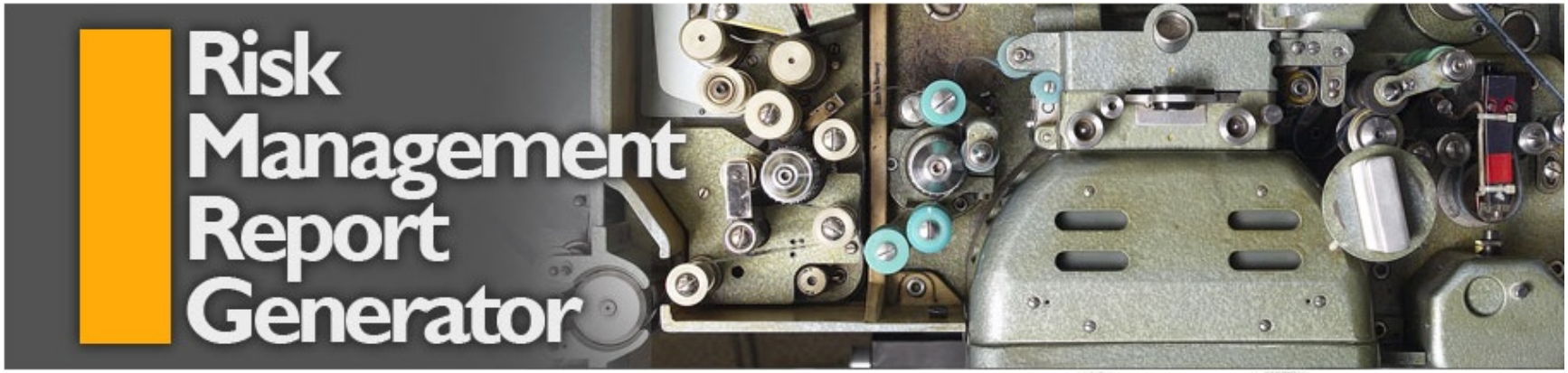
COMPONENTS: DEVELOPMENT AND ACQUISITION

This rating reflects an organization's ability to identify, acquire, install, and maintain appropriate information technology solutions. For most credit unions, this means vendor oversight.

Vendor Management

1. Has the board of directors approved a Vendor Oversight Policy?
2. For the critical service providers, did the credit union contact references and user groups to evaluate the service provider's reputation and performance?
3. Did the credit union determine if the third party vendor is using subcontractors (other third parties) to supplement the services provided to the credit union?
4. Did the credit union determine if the third party vendor or their subcontractors are foreign subsidiaries of U.S. Companies or Foreign Companies?
5. Did the credit union request and evaluate the service provider's financial condition initially and then annually, thereafter?
6. Did the credit union obtain and review audit reports/ SAS 70 reviews, initially and annually thereafter?
7. Has the credit union reviewed the Client Considerations (controls) contained in SAS 70 Reports?
8. Has the credit union implemented the Client Considerations (controls) contained in SAS 70 Reports?
9. Did the credit union obtain and review regulatory examination reports initially and annually thereafter?
10. Did the credit union obtain adequate information detailing the security measures in place to protect the facility, member data, etc.?
11. Did the credit union secure a high level schematic of the third party vendors system?
12. Did the credit union determine if the third party vendor has appropriate insurance coverage and receive confirmation of the coverage?
13. Does the credit union regularly review reports documenting the service provider's performance?
14. Does the credit union participate in user groups?
15. Did the credit union review the service provider's business resumption contingency plans to ensure that any services considered mission critical for the institution can be restored within an acceptable timeframe?
16. Does the contract specify confidentiality requirements for member information? (Gramm Leach Bliley Act)
17. Does the contract document the ownership of data and processes by each party entering into the contract?
18. Does the contract outline the responsibilities, duties, and liability of each party?
19. Does the contract address software details such as source code agreements, escrowing software, etc?
20. Do contracts identify the roles, responsibilities, and controls for exchange of information between external parties?
21. Does the contract address minimum service levels for each service provided by the vendor?
22. Does the contract identify the monthly, quarterly, and annual reports which will be provided to the credit union to evaluate the vendor's adherence to service levels identified in the contract?
23. Does the contract address minimum security procedures to protect member and credit union information?
24. Does the contract address encryption for sensitive data on backup tapes and storage facilities?
25. Does the contract identify services to be performed by the service provider including duties such a software support and maintenance, training of employees, etc.?
26. Does the contract outline the obligations of the credit union?
27. Does the contract address parties rights in modifying existing services performed under contract?
28. Does the contract provide guidelines for contract re-negotiation?
29. Did the credit union submit the contract to legal counsel for review prior to signing the contract?

CU*ANSWERS D&A TOOLS



These questions can be answered at rmrg.cuanswers.com – **this tool is free**. In some cases, other credit unions will have their risk report that can be reviewed.

It is still important for the credit union to show examiners that the work of reviewing the vendor has been done.

CALCULATING D&A RISK

Vendor	Criteria	Metric	Other Alternatives	Metric	Cost Differential
ISP 1	Speed	1.54 mbps	ISP 2	32.4 mbps	+$10,000/yr
ISP 1	Reliability	99% uptime	ISP 2	95% uptime	+$10,000/yr

The examiners should gain assurance that when a third-party provider is purchased, the vendor selection process leads to effective vendors and services and an appropriate mitigation of any risks that the applicable IT service presents to the financial reports.

Important Note: It is far less important as to which vendor is ultimately selected; what matters is the process. For example, here the decision would be - is it too risky to have slower speed or longer downtime? Either provider is the right answer; the key is documenting how you arrived there. In other words, there is no wrong answer with the right documentation and decision process.

COMPONENTS: SUPPORT AND DELIVERY

This rating reflects an organization's ability to provide technology services in a secure environment. It reflects not only the condition of IT operations but also factors such as reliability, security, and integrity, which may affect the quality of the information delivery system.

This is all about developing benchmarks for your IT services and then determining if those benchmarks are improving, staying the same, or declining.

CALCULATING S&D RISK

ITIL Process		Examples of ITIL Metrics	
		Cost	Time
Service Support	Configuration Management	Number of licenses not used Cost associated with breaches in SLAs caused by accurate CMDB	Duration that the CMDB has been consistently up-to-date
	Change Management	Cost to recover failed changes Cost incurred by outage during changes	Time to complete change
	Release Management	Cost of release Cost of meeting urgent releases Cost of conducting end-user training sessions for new releases	Time to complete investigation of reported bugs Service time lost due to release activity
	Incident Management	Savings from incidents resolved right first time	Call time with no escalation Mean time to resolve incident
	Problem Management	Cost associated with user downtime Cost to overcome missed target resolution time	Time to close a problem
	Service Desk	Cost of meeting SLAs that require changes Cost of SLA breaches caused by 3rd party support contracts	Duration of calls Time spent calling back customer for more information or to give a solution

CALCULATING S&D RISK

Service Delivery	Service Level Management	Service Delivery costs Cost associated with SLA breaches caused by third party support contracts	Elapsed time to follow up and resolve issues
	Financial Management	Actual costs against budgeted costs Software license fees vs. available licenses Percentage of unaccounted total IT costs	Staff time spent on costing activities
	Capacity Management	Cost arising from SLA breaches due to poor service performance	On-line response time
	Continuity Management	Cost to rectify wrong entries in crisis control team directory Cost of changes that have caused major issues	Delay in IT service continuity plan completion/update
	Availability Management	Cost to repair per incident	Downtime due to unavailability of service Response time per incident

CALCULATING S&D RISK

Service	Criteria	Metric	Q3	Q2	Q1
Change Management	Configuration errors	0 errors or 0% downtime	0 errors	2 errors (2 hours downtime)	1 error (1 hour downtime)

Make note here that after Q2 a new change management program was implemented. The examiners should gain assurance that changes are made when a particular area of Support and Development is not meeting the criteria benchmarks.

RISK MANAGEMENT REPORTS

AUDIT
Risk Level of Finding + (Cost of Remediation - Cost of No Remediation) = Audit Risks

GOVERNANCE
Project costs (time and dollars) + variance = Management Risks

DEVELOPMENT AND ACQUISITION
Current cost of technology – Potential new technology = D&A Risks

SUPPORT AND DELIVERY
Cost of service currently – benchmarks = S&D Risks

Prime question – ***What is the benefit to the members?***

Standard benefits include:
- More security
- Better credit union performance
- More or improved products and services
- A healthier credit union

CONCLUSION

Quantitative analysis need not be complex to be effective. Evidence that there are good reasons for decisions based on cost/benefit analysis goes a long way to making examinations easier.