

Measuring the Unmeasurable: A Balanced Scorecard for an Information Security Program



Roy L. Post
May, 2009



Public



Goal Of This Session

- / To explore how the Norton and Kaplan “Balanced Scorecard” and it’s offspring may be leveraged by an information security or information risk management program
 - for ***strategic*** planning
 - to help **present the status** of an InfoSec program to management



Agenda

- / Thought Tools – Why I Need ‘em
- / Sources of Information
- / Why Balanced Scorecard?
- / Classic & InfoSec Scorecards
- / Strategy Planning Pyramid
- / Strategy Map
- / Sample Scorecard
- / Stoplight Scorecard

Strategic Thought Tools – Why I Need ‘em

Because it's easier for me to...

- Review requests for policy exceptions
- Opine on a pen test report
- Review a partner's SAS70
- Manage a risk

But the company needs me to...

- Align our standards with company strategy
- Prepare for emerging threats
- Plan strategic investment
- Show that risks are managed

Credit Where Credit is Due

- “The Balanced Scorecard”
 - Kaplan and Norton, 1996
- “Is There Any Strategy in Your Strategic Plan?”
 - Rohm, Balanced Scorecard Institute, 2008
 - www.balancedscorecard.org
- “Creating A Balanced Scorecard For Computer Security”
 - Delooze, Proceedings of the IEEE Workshop on Information Assurance, 2006
- Corporate Executive Board – Information Risk Executive Council
 - A huge pool of shared resources from multiple companies
 - Templates, scorecards, strat plans...
 - <https://www.irec.executiveboard.com>

Public

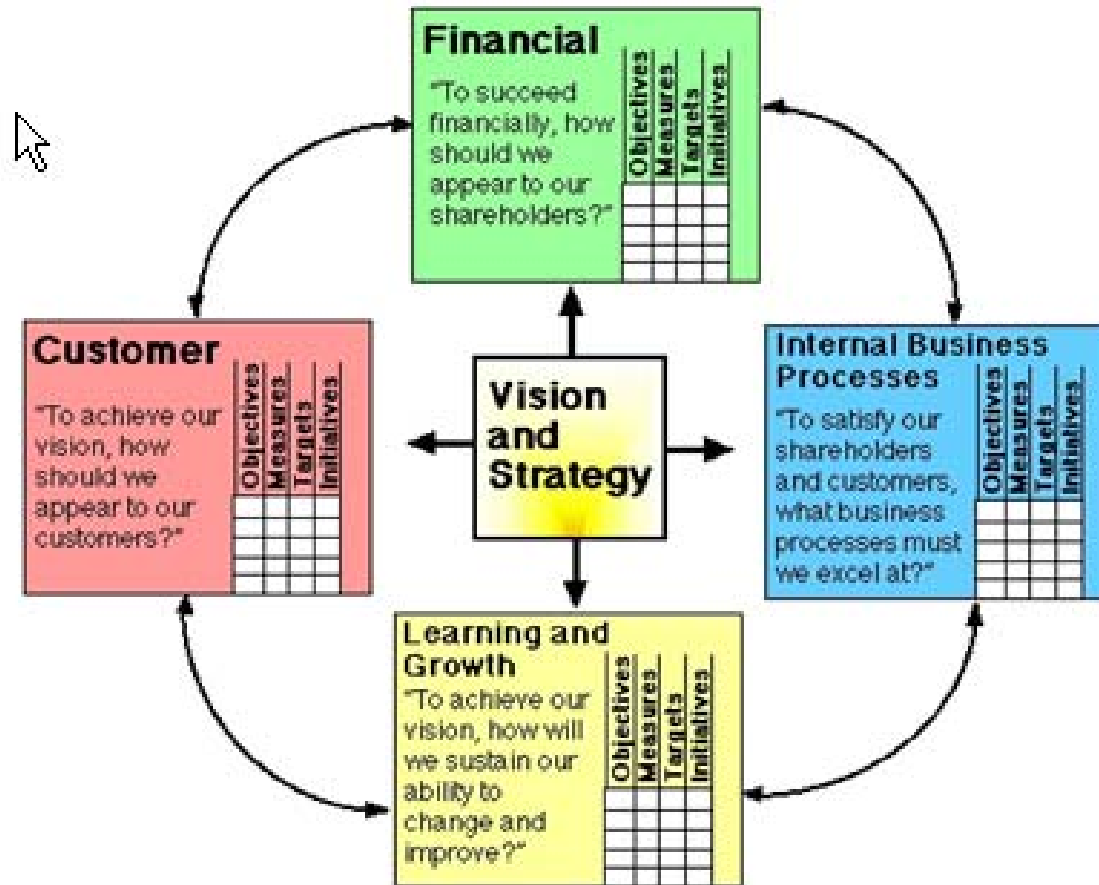


Why Balanced Scorecard?

- Where and how can InfoSec have the best impact on the business?
- So now that I know that, how am I doing?
- And what should I be doing next?
- Balanced Scorecard “Four Perspectives” Model
 - Broadens thinking beyond purely financial measures
 - If the only perspective is financial, InfoSec and risk management is viewed as a cost center, not a revenue generator

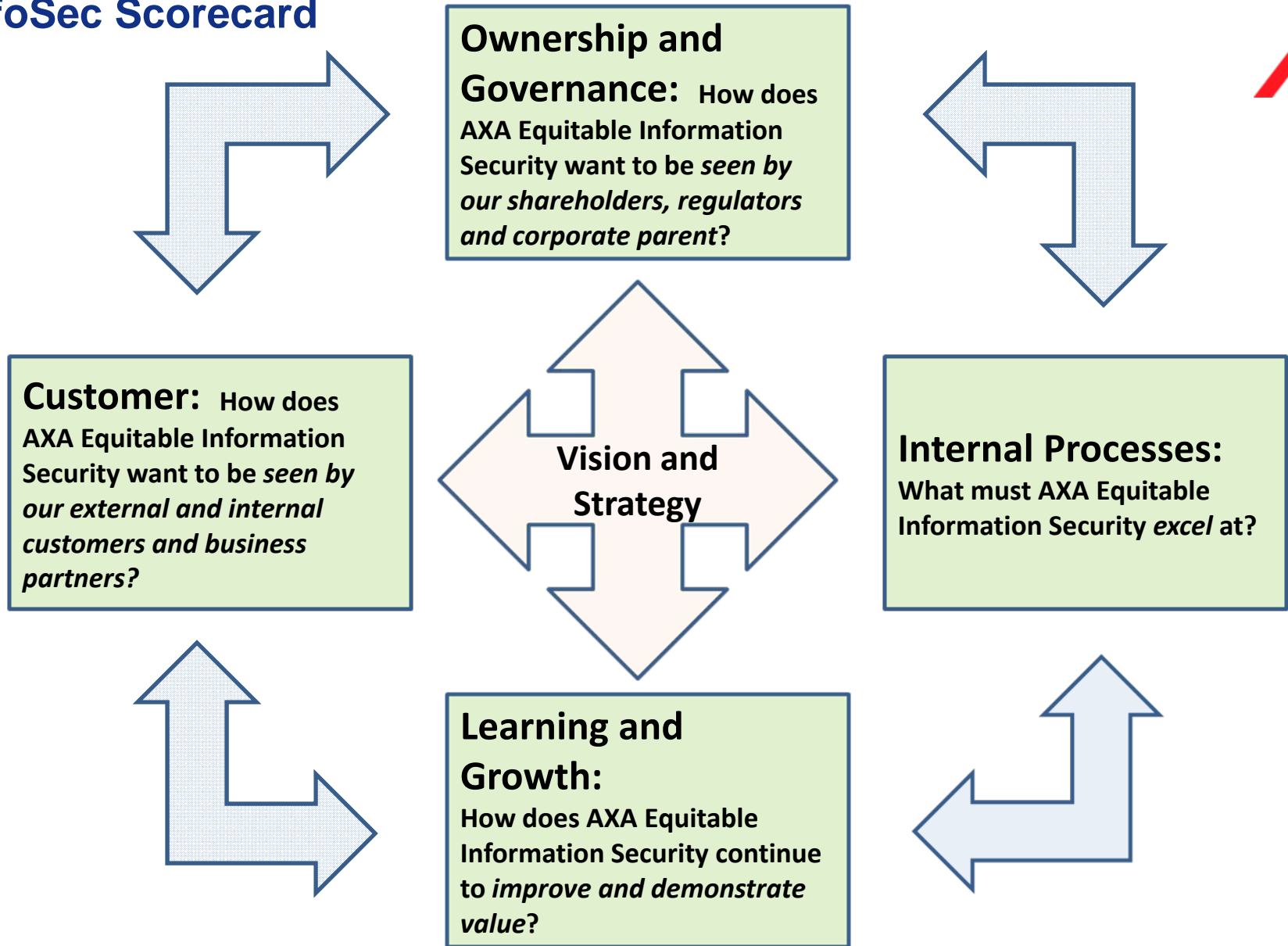


The “Classic” Balanced Scorecard



Adapted from *The Balanced Scorecard* by Kaplan & Norton

InfoSec Scorecard



Strategic Planning Layer Cake



After Rohm, 2008



Strategic Planning Layer Cake



After Rohm, 2008

Existing:
Based on
ISO 27002
Framework

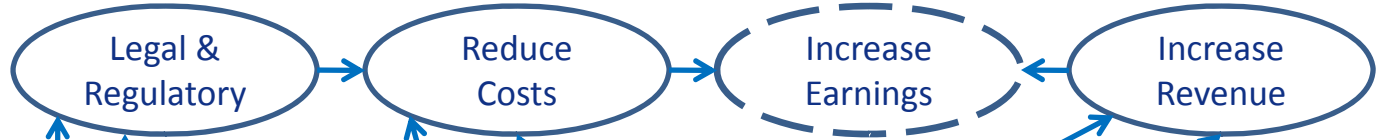
New: IAM, DLP,
VM,
Awareness, 3rd
Parties, Remote
Workers



Corporate Strategy Map – Objectives in Perspectives

Perspectives

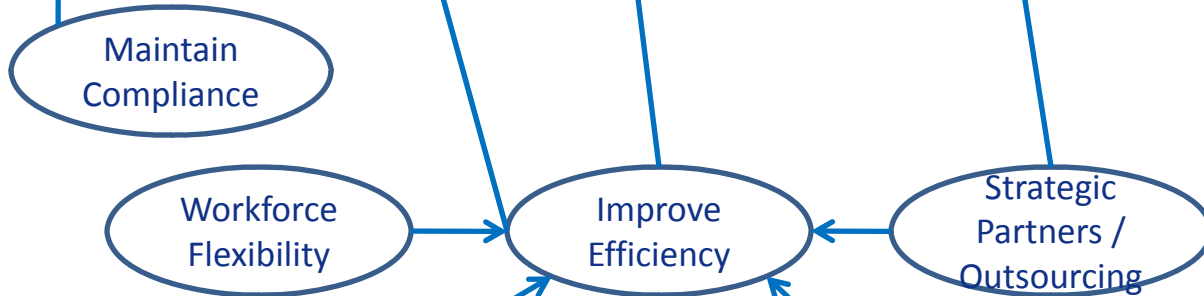
Ownership
&
Governance



Customer



Internal
Processes



Learning
&
Growth



Corporate Strategy Map – **New Initiatives**

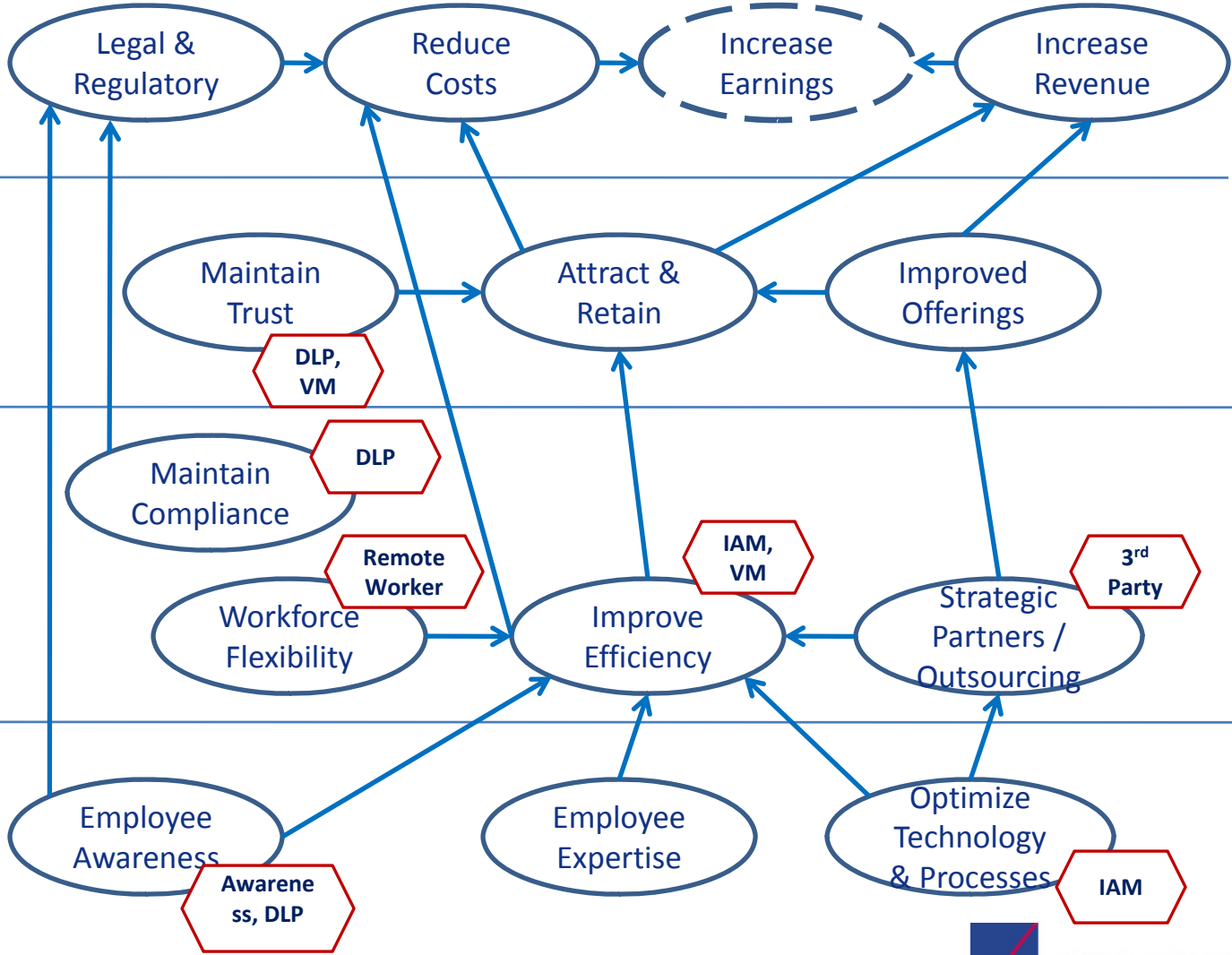
Perspectives

Ownership & Governance

Customer

Internal Processes

Learning & Growth

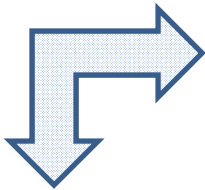


Sample Scorecard

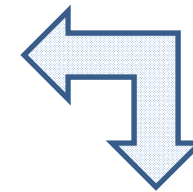


AXA Equitable Office of Information Security				
Information Security Balanced Scorecard 2009 (DRAFT)				
"Vision" statement		It is the policy of AXA Equitable to protect client, employee, financial professional, protected third-party and other corporate information from unauthorized disclosure, modification or destruction throughout the information's life cycle.		
"Strategy" statement		It is the strategy of the Office of Information Security to ALIGN security requirements and solutions with AXA Equitable strategy; craft solutions that SUSTAIN over time; and quickly ADAPT to changes in business strategy or the threat environment.		
Scorecard Dimension	Objectives	Measures	Targets	Initiatives
Internal Processes: What must AXA Equitable Information Security excel at?				
	Supporting Workforce Flexibility	# employees able to work remotely / mobile	not established	Remote Worker
	Improve Efficiency	% SLA achievement for provision/deprovision. Frequency and severity of incidents and near-misses.	not established	IAM, Vulnerability Management
	Strategic Partnerships / Outsourcing	Frequency and severity of incidents and near-misses	No incidents of significance or materiality, near-misses infrequent (?)	3rd Party / Vendor Risk Management
Learning and Growth: How does AXA Equitable Information Security continue to improve and demonstrate value?				
	Employee Awareness	Annual awareness survey	Year over year improvement	Poster campaign
	Employee Awareness	DLP reports	No incidents of significance or materiality, near-misses infrequent (?)	DLP

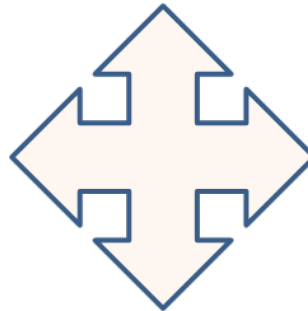
Stoplight Scorecard



Ownership and Governance			
Objective	Cost	Report State of Risk Management	Report State of L&R Compliance
Target	●	●	●
Initiative	○	●	○

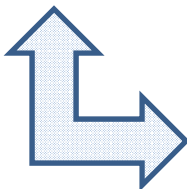


Customer			
Objective	Trust	Attract & Retain	Improved Offerings
Target	●	○	●
Initiative	●	○	●

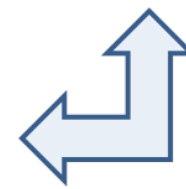


Internal Processes				
Objective	Compliance	Worker Flexibility	Efficiency	Partnerships & Outsourcing
Target	●	●	●	●
Initiative	●	●	●	●

- Hits Target. Initiative on Track.
- Short of target. Initiative recoverable.
- Failed process. Initiative not recoverable.
- Target not defined. No initiative.



Learning and Growth			
Objective	Awareness	Expertise	Optimize
Target	●	●	●
Initiative	●	○	●



Questions? Comments?



Appendix





Home | BSC Resources | About the Institute | Store | Training | Consulting | Contact Us

You are Here: [Home](#)

Search

GO

The Balanced Scorecard Institute

What is the Balanced Scorecard?

The balanced scorecard is a strategic planning and management system used to align business activities to the vision and strategy of the organization, improve internal and external communications, and monitor organizational performance against strategic goals.

[More BSC Resources >>](#)

[Print Brochure >>](#)

About the Institute

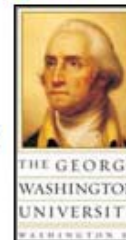
The Balanced Scorecard Institute, a Strategy Management Group company, helps organizations succeed through improved strategic focus and

Professional Certification Program

The Institute's heralded Certification Program now includes two levels of certification: *Balanced Scorecard Master Professional (BSMP)* and *Balanced Scorecard Professional (BSP)*, both of which are now achievable through public workshop participation.

[Read More >>](#)

[View Schedule >>](#)



Announcing Upcoming Events

Improve Your Performance "News"

Thanks to Facebook, Twitter and breaking news email alerts, employees know that 5 minutes ago a vague acquaintance ate corn flakes for breakfast and the stock market crashed, but they have no idea how their organization is performing strategically.

[Read More to Find Out Why >>](#)



NEW! E-Learning Overview

By popular demand! The first Institute training course streamed entirely over the internet! Cut travel expenses. Train your whole team.



Performance Measurement and Reporting

Featured Resources



Information Risk Scorecard Builder

Tools and Templates | January 2006 | XLS - 742 KB

Additional Resources



Some Company's Proactive Performance Reporting Road Map

Tools and Templates | October 2005 | PDF - 46 KB, 1 Page



Gamma Company's Information Risk Scorecard

Tools and Templates | April 2005 | DOC - 178 KB, 6 Pages

Another Company's Standardized Risk Reporting Tool



Tools and Templates | November 2005 | PDF - 65 KB, 1 Page



Sigma Company : Information Protection Scorecard

Tools and Templates | June 2005 | DOC - 180 KB, 12 Pages



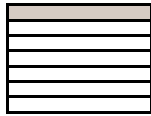
XYZ 's Risk-Based Systems Compliance Status Report

Tools and Templates | January 2005 | PDF - 85 KB, 1 Page



Yet Another Information Security Maturity Model

Tools and Templates | January 2005 | PDF - 111 KB, 1 Page



Performance Measurement and Communication: By querying members across the executive suite, IREC uncovered 20 key areas of concern to include in an Information Risk Scorecard for an executive audience. By creating a high-level composite metric for each question, members can reduce complexity and increase relevance.

Top Twenty Metrics for the Information Risk Scorecard

Twenty key questions and corresponding metrics can effectively capture the information risk profile of the enterprise

Holistic Information Risk Scorecard

Schematic

Information Protection	
Key Question	Metric
1. Are we appropriately prepared for disasters?	Disaster Recovery Readiness
2. Do IT staff members understand and follow appropriate information security practices?	IT Staff Security Awareness
3. What technical vulnerabilities jeopardize infrastructure availability and data protection?	Threat Mitigation Effectiveness
4. How many control lapses are outstanding and what are we doing to remediate them?	Control Lapse Remediation Effectiveness
5. Are there specific business units that require additional attention in the short-term?	Business Unit Risk Levels
6. How effective is the information security function at project planning and execution?	Information Security Planning and Project Execution Effectiveness
7. Does the function have the necessary skills required to meet emerging risk mandates?	Information Security Staff Readiness
8. How are our information security vendors performing?	Information Security Vendors Effectiveness
Effectiveness of Compliance and Controls	
9. How can we be sure users that have access to systems have a legitimate business need?	Information Access Control Effectiveness
10. How protected are we against information risks posed by third-parties?	Third-Party Risk Protection
11. How effectively have we protected against damage from information security incidents?	Information Security Incident Protection
12. How effectively does the company respond to incidents?	Incident Response Effectiveness
13. How compliant are we with IT areas of relevant regulations?	Regulatory Compliance Readiness
Business Risk Profile	
14. How do information risks threaten our brand and/or long-term reputation?	Brand Risk Protection
15. How effective are the IT controls of financial systems?	IT Controls of Financial Systems
16. Is there sufficient separation of duties between roles (for regulatory compliance)?	Separation of Roles Effectiveness
17. Are information security decisions based on principled risk assessments?	Risk Assessment Adoption
Internal Performance	
18. Do we pose an information risk to our customers, partners, and other third-parties?	External Information Security Acceptance
19. What organizational obstacles exist to appropriately mitigating information risks?	Degree of Business Collaboration
20. Do users understand and follow information security policies?	Awareness Effectiveness

Source: IREC research.