

Emerging Risks and the Impact on Your Audit Plan

IIA Luncheon – October 2012



Speakers

Denise McCurry
PricewaterhouseCoopers Director

Husam Brohi
PricewaterhouseCoopers Director

Agenda

Why are we here

Identification/Management of Emerging Risk

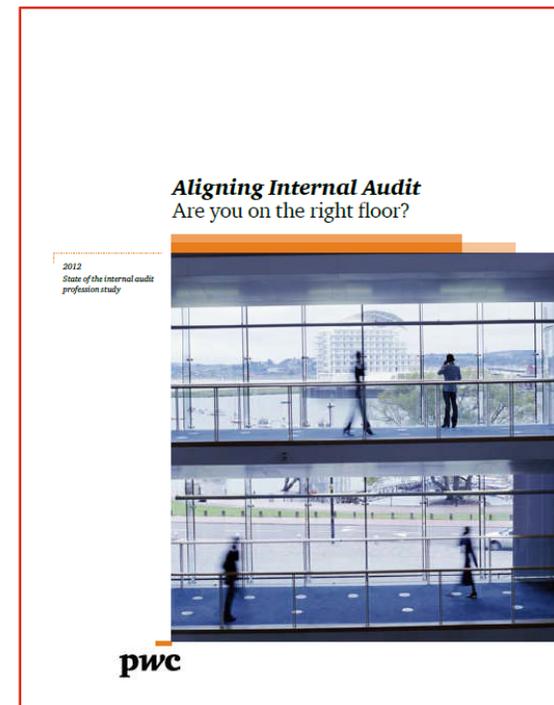
Potential Emerging Risk

Why are we here

Internal audit's role in emerging risk

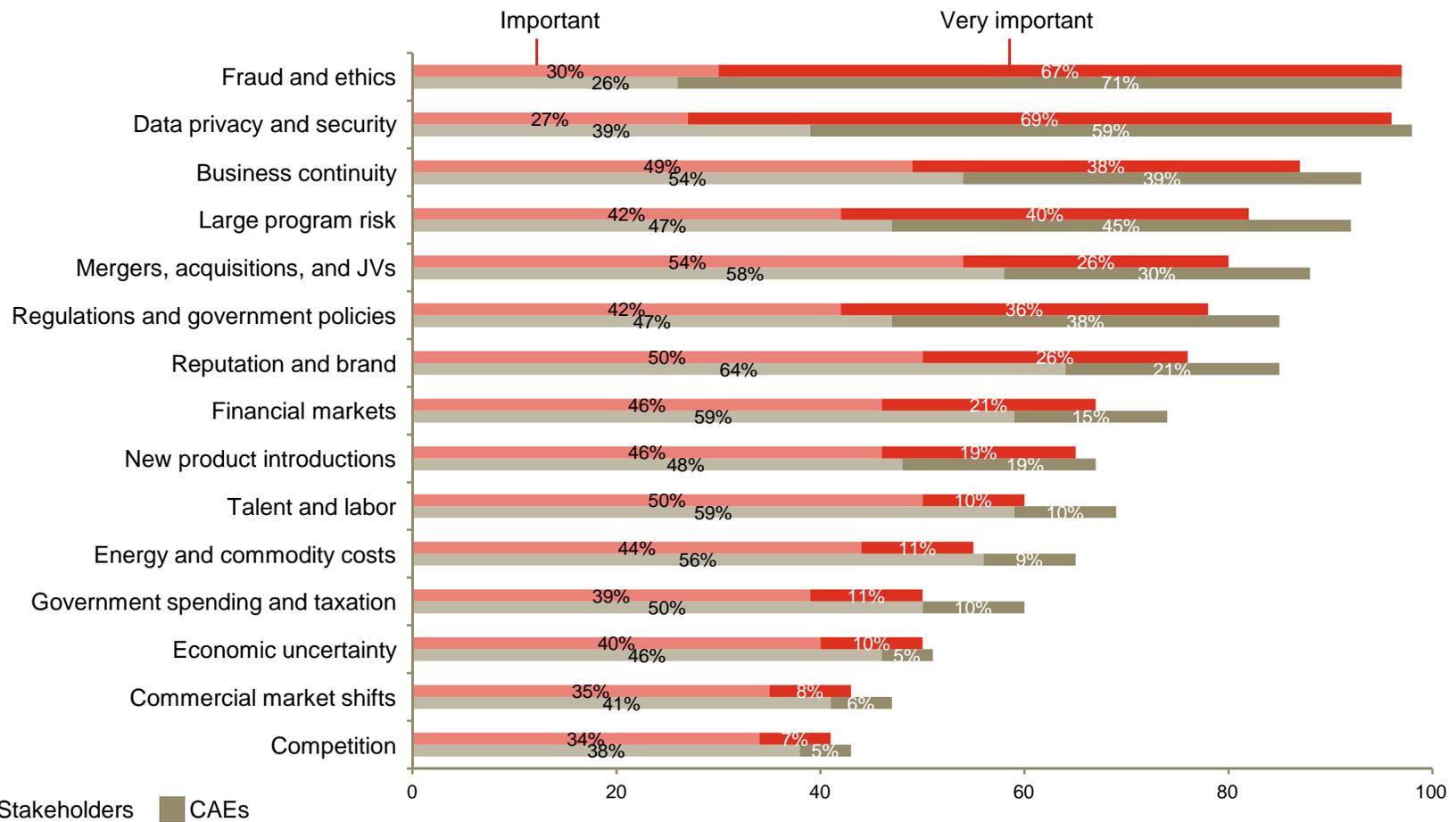
State of the internal audit profession study

- **8th** Annual State of the Internal Audit Profession Study
- Focus on the **rising importance** of risk management and the **increasing expectations** of internal audit's contribution to the effort
- **New methodology:** For the first time, an “outside-in” look at the internal audit profession through points of view of:
 - Over **660** stakeholders and **870** chief audit executives through an online survey
 - Nearly **100** stakeholders, including board members and executives in one-on-one interviews
 - **64** countries globally
 - **16** industry sectors
- Full study available at:
www.pwc.com/us/2012internalauditstudy



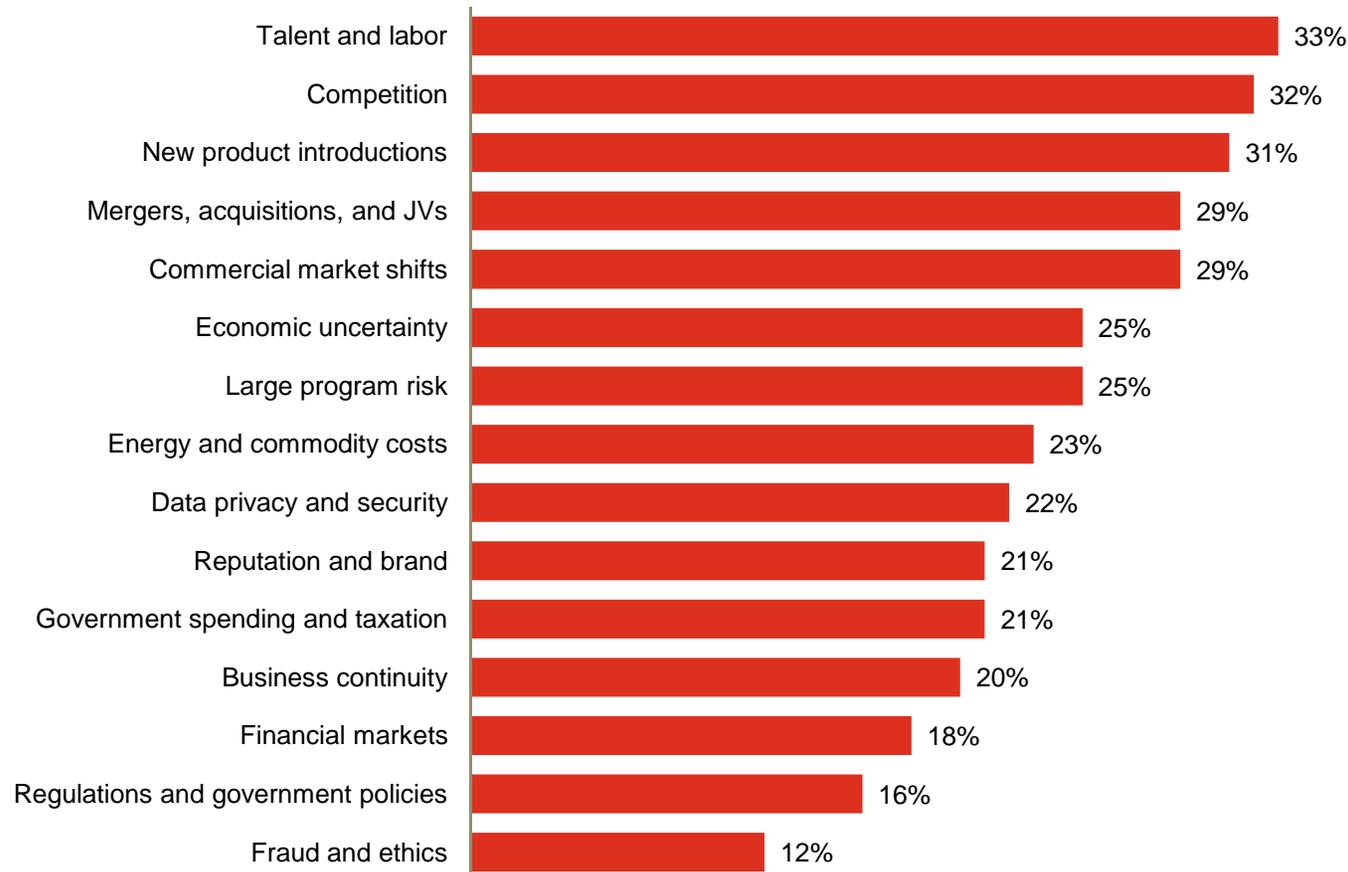
Stakeholders value internal audit's contribution...

Importance of internal audit's contribution to monitoring risks



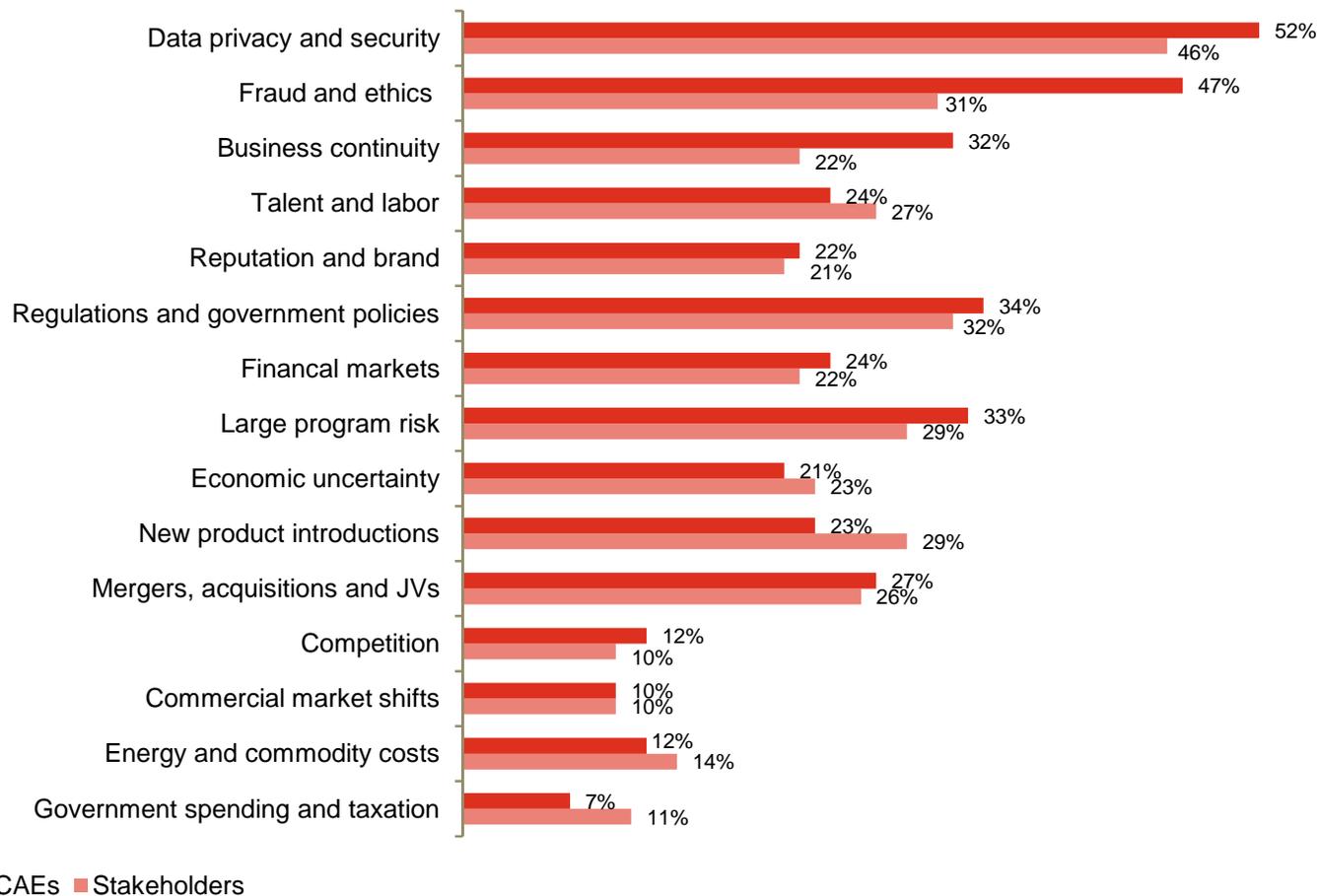
... and stakeholders want more from internal audit

Which risks are receiving too little attention from internal audit

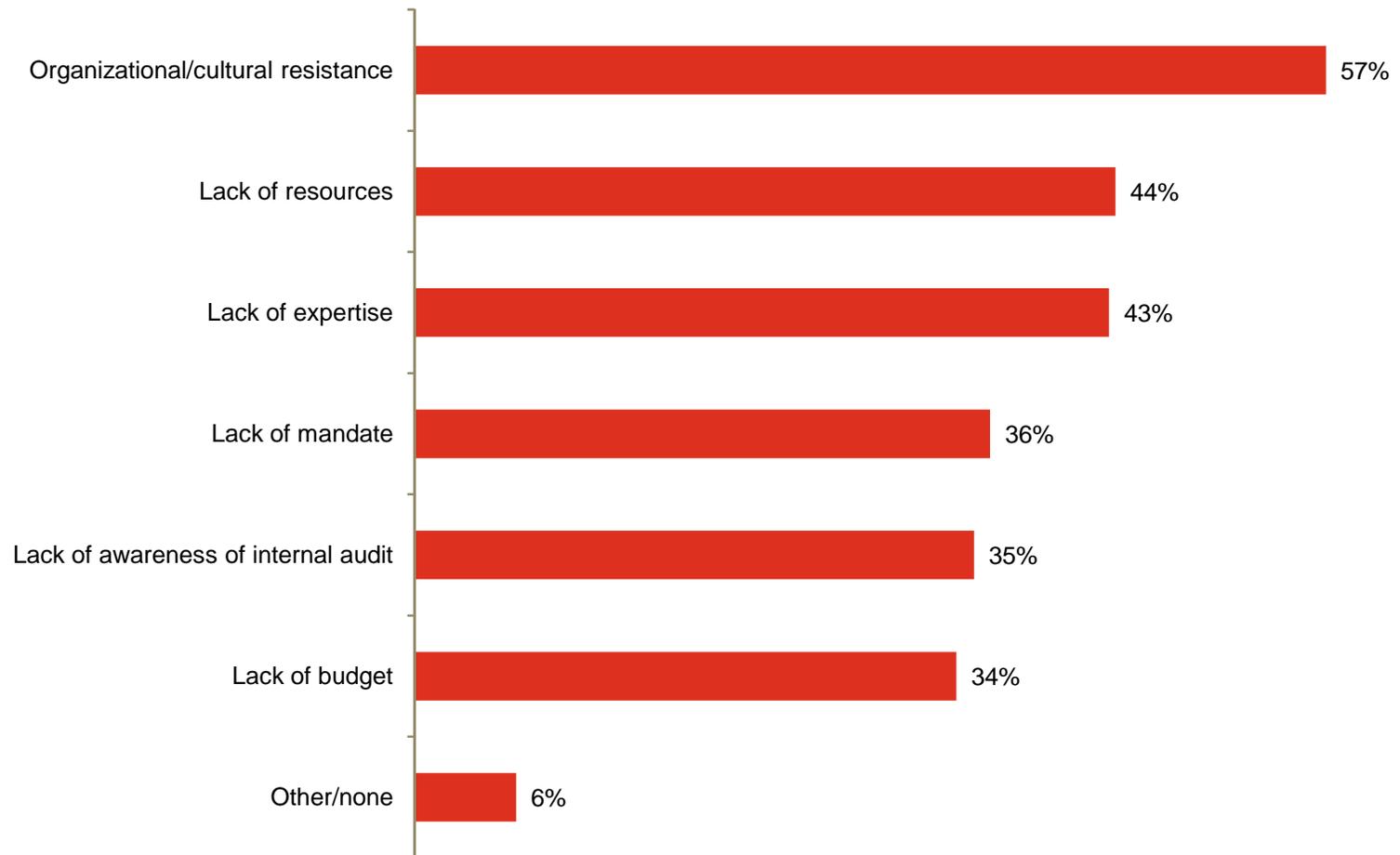


Stakeholders want focus in all critical risk areas

Risk areas in which stakeholders and CAEs want/plan to add IA capabilities



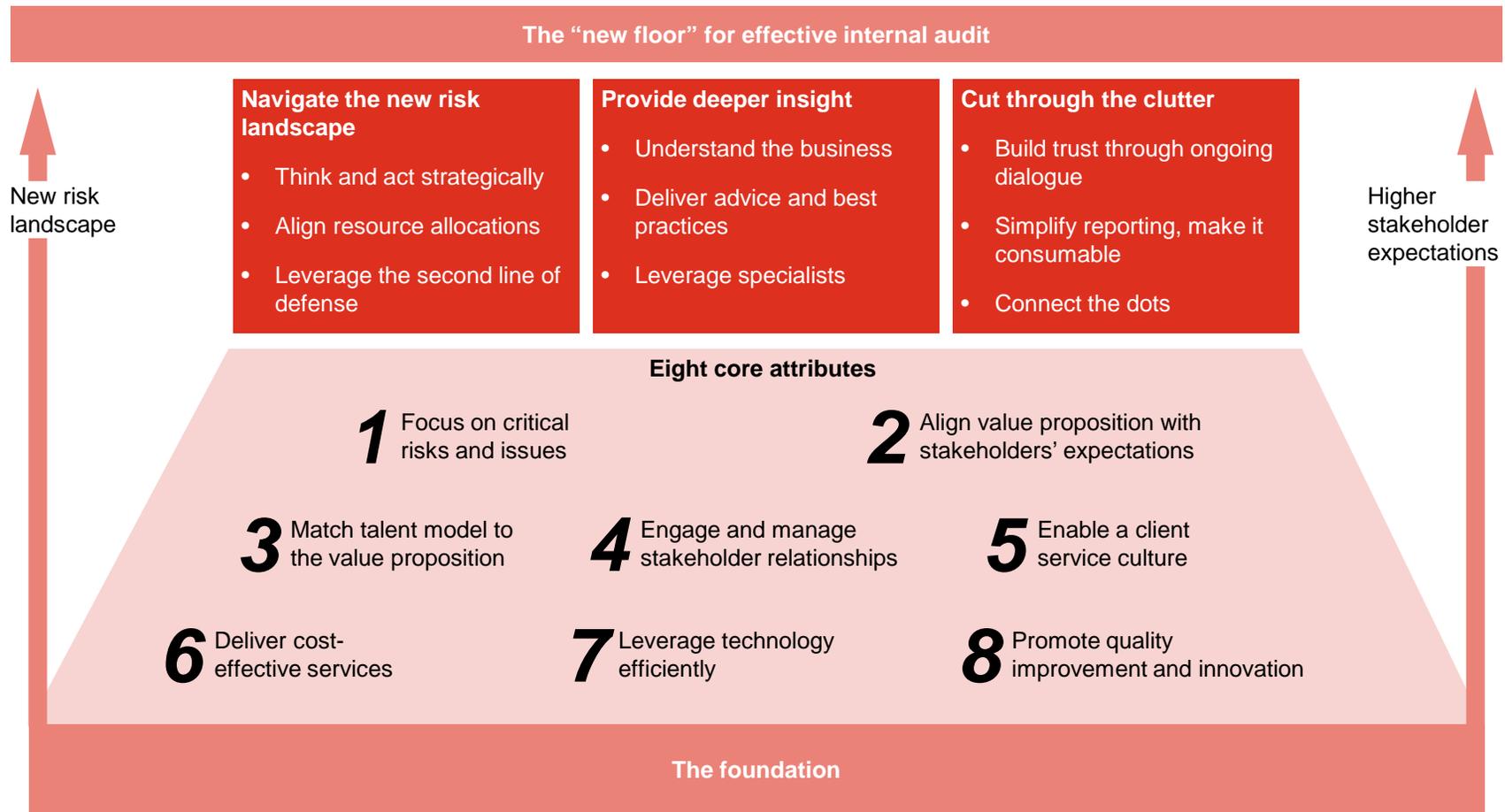
Barriers to internal audit playing a more substantive role



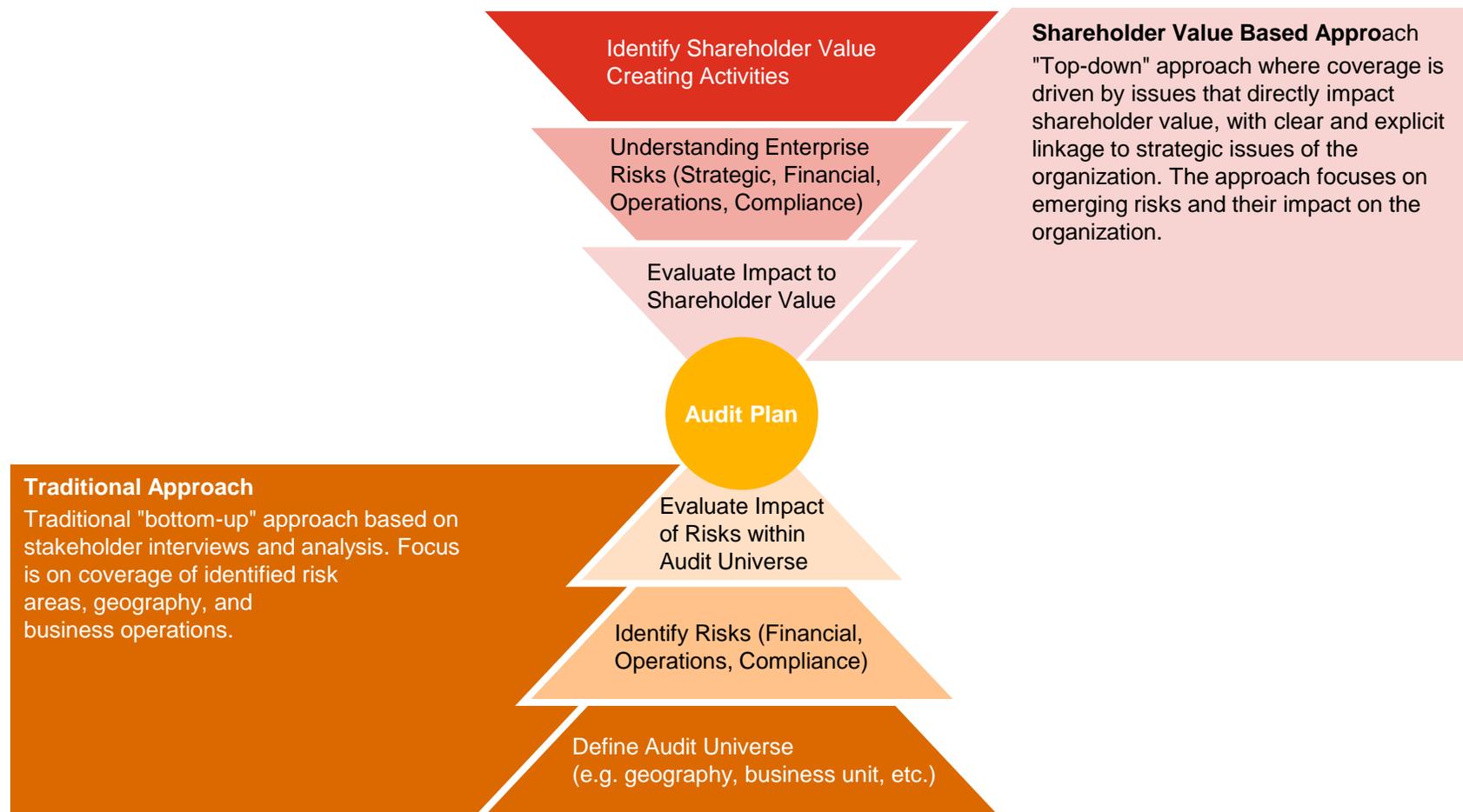
Identification & Management of emerging risk

Responding to stakeholder expectations

The new floor



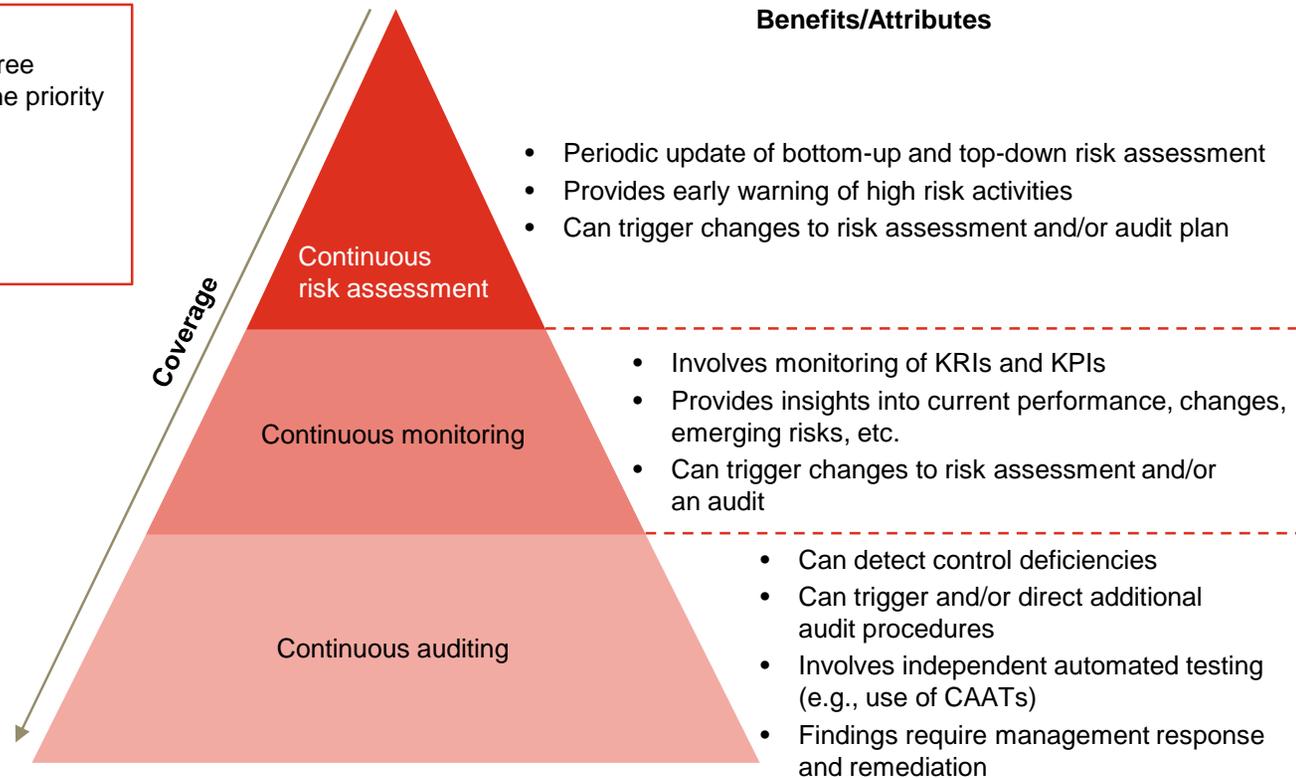
Traditional risk assessment and audit planning



A sample monitoring emerging risks

Key attributes:

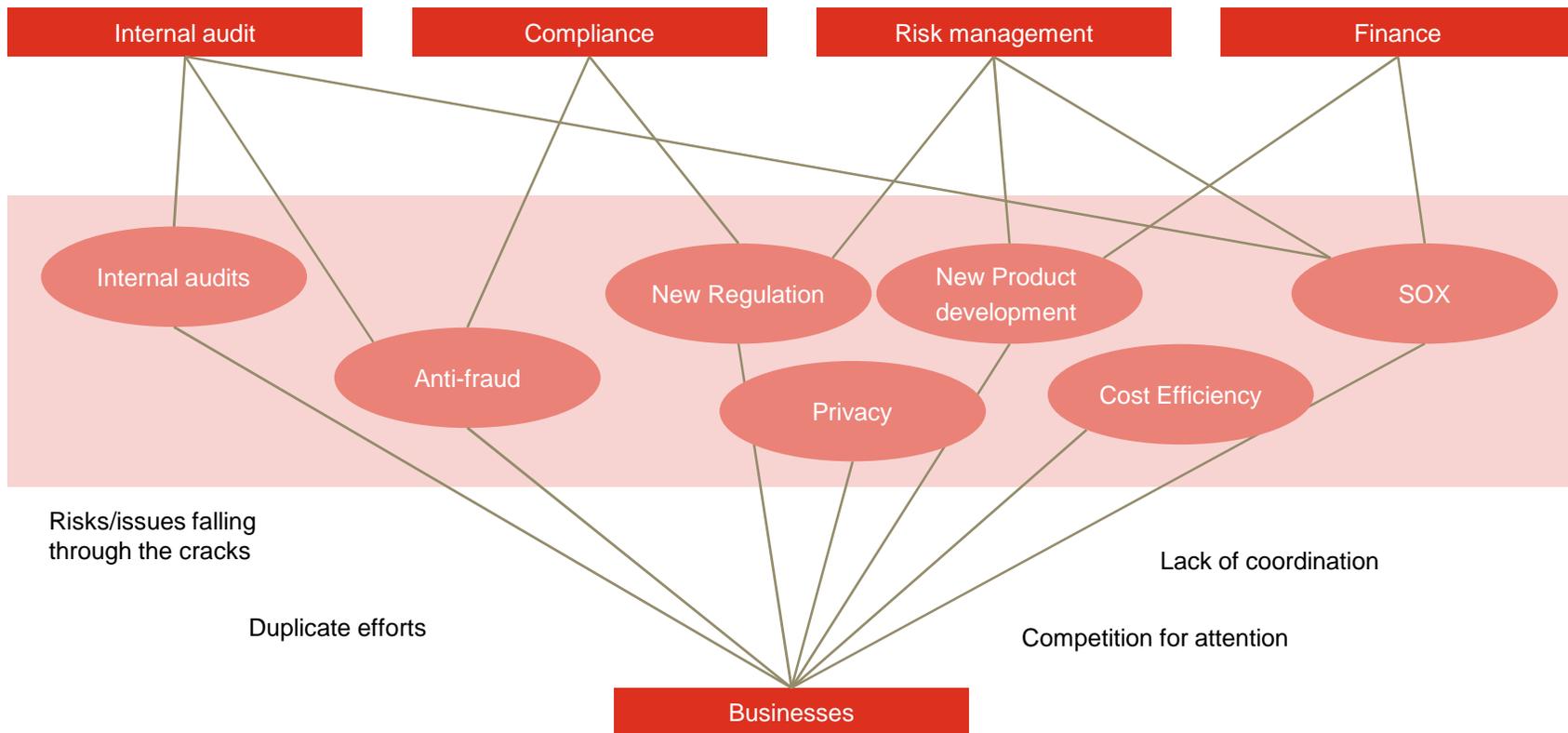
- Frequency and focus of all three processes will be based on the priority and risks identified for each risk unit.
- Formal process for elevating and reporting output from all three processes.



Linkage to audit plan - Business/risk monitoring as required in the audit frequency and intensity matrix ideally entails a well-developed continuous risk assessment and monitoring process for each risk unit

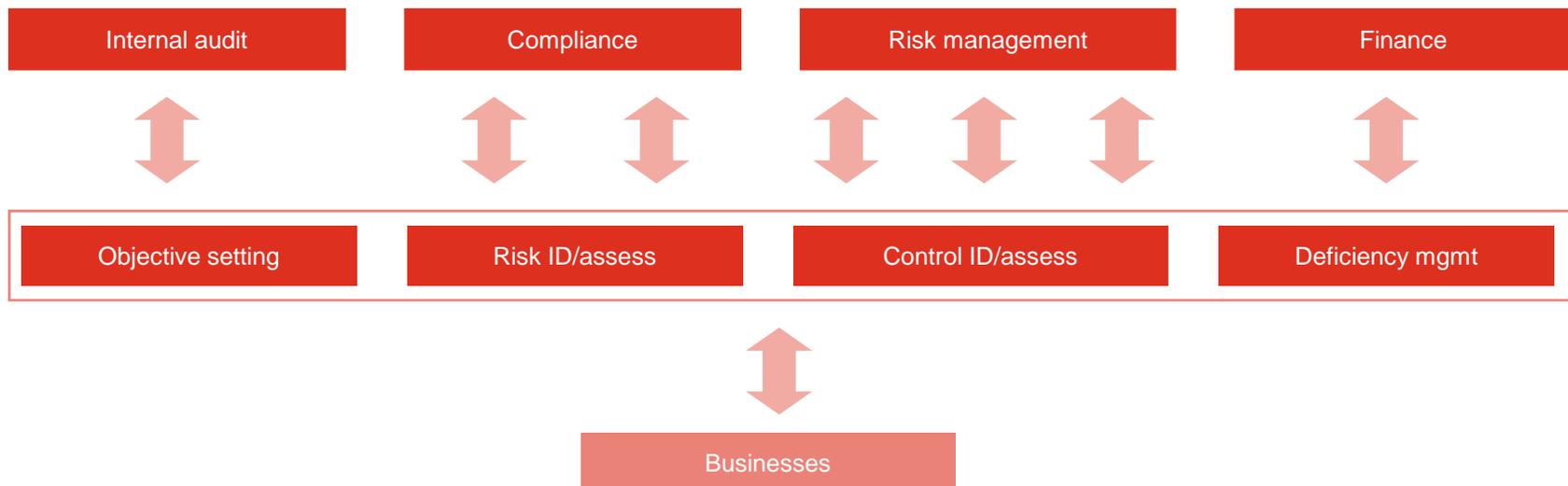
The current state of risk partner convergence

The business and regulatory environments have become increasingly complex, raising corporate risk profiles. Strategic consequences exist if companies are unable to systemically manage governance, risk and compliance requirements effectively. Most attempts to date have been ad hoc and produced limited results.



How have organizations made it work

- Utilize a standard framework
- Consider structure across/within functions, businesses and regulatory requirements
- Align with regulatory expectations
- Choose the right place to start: new and developing functions, union of similar silos, areas ripe with duplication, integrated/related environments



Potential emerging risk

Current emerging risk

- Cloud computing
- Social media
- Customs import/export
- Cyber security
- Mobile devices
- IT governance
- Software asset management
- Spreadsheet management
- ERM
- New regulations

Cyber security

CEOs/Boards are no longer ignoring cyber security

Cyber Security is an enterprise-wide issue. Specific types of Cyber Security risks organizations are facing include:

- Increase in Privacy and Security regulatory mandates in recent years, as well as expected changes in upcoming years.
- Boards are no longer willing to accept the risk that technology can pose to the business.
- Growing demand by business leaders to understand how security integrates with privacy (“what” data is sensitive to the business) and security (“how” they protect the data deemed sensitive).
- Increase in threats and vulnerabilities to sensitive data and corporate assets.
- Businesses continue to struggle to maintain accountability to their stakeholders and establish effective strategies and standards for security risk management and privacy control activities.

CEOs/Boards are no longer ignoring cyber security

Security Hot Topics: Balancing Business Enablers vs Business Risks

Privacy

Organizations looking to improve privacy management in the event of a breach "have to continually plan and prepare.

Social Media

Social media can make or break a brand and the fine line between the two must be managed.

Regulatory

Organizations in all industries are under increased scrutiny by regulatory governance bodies.

Mobile & Emerging Tech

Cloud computing, Mobile platforms and accelerated product life cycles are just the latest contributors to risk of an enterprise.

Data Loss Prevention

Company's reputation is paramount and the risk of loss of sensitive customer data threaten this fragile asset.

Threat & Vulnerability Management

A Major bank's share price dropped three percent after Wiki Leaks threatened to 'take down a major American bank and reveal an ecosystem of corruption' using documents from an executive's hard drive

3rd Parties

While risks associated with third parties continue to increase, many companies are less prepared to defend their data.

Cyber Crisis Management

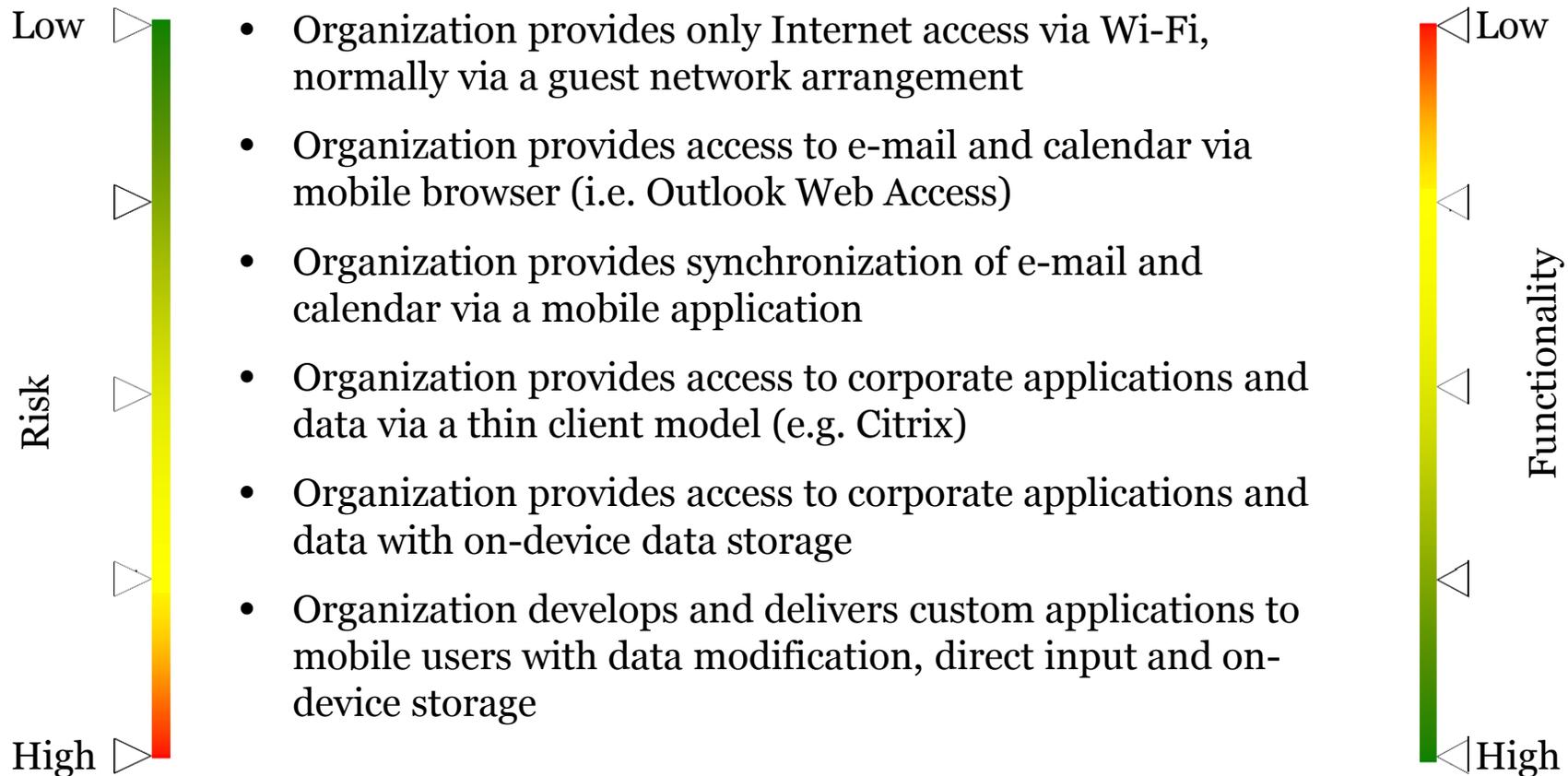
The cyber threat landscape continues to yield an increasingly sophisticated underworld of criminals. Companies need to remain prepared for such cyber crises.

Mobile security

Level Set – Basic mobile device characteristics

- Generally, “mobile devices” refers to mobile phones, smart phones, tablets and specialized mobile computing devices that primarily connect to a wireless carrier for communications. Excluded are traditional portable computing platforms such as laptops and touch screen computers running a laptop operating system (i.e. Windows).
- Mobile devices will normally include a tailored purpose operating system such as iOS, Android, Blackberry OS, Windows Phone, Symbian or a proprietary device OS
- Mobile devices generally include the option to connect to available wireless broadband services in addition to the carrier network
- Many types of mobile devices will be able to download applications from the Internet or proprietary services unless specifically blocked by the device configuration
- Generally, users will be able to synchronize their devices with enterprise applications via desktop/laptop computers and/or wirelessly

Mobile access at work – Use cases and risk profiles



Lost or stolen devices – The number one threat associated with mobility programs

- 56% of us misplace our **cell phone** or laptop each month
- 113 **cell phones** are lost or stolen every minute in the U.S.
- 120,000 **cell phones** are lost annually in Chicago taxi cabs
- 25% of Americans lose or damage their **cell phone** each year
- Major city transit authorities receive over 200 lost items per day



“Bring your own” device security considerations

- Many organizations have now opted to allow employees to procure their own devices which will ultimately connect to enterprise data and resources
- A “Bring Your Own” strategy presents additional security and privacy challenges which should be carefully considered prior to implementation
- Policies must be carefully crafted that mandate certain restrictions on the employee’s access to corporate data with a personally owned device. Policies should cover minimum device security standards, use of anti-virus or endpoint security software based on legal or compliance requirements and clear language regarding consent for the enterprise to access enterprise data on the device on a timely basis.
- The enterprise should aggressively monitor access by employees with personally owned devices and consider restricting access to the minimum level required to perform the employee’s role (e.g. e-mail and calendar)
- The enterprise should reserve the right to rapidly bar access to data and resources by employees with personally owned devices if necessary to protect enterprise data, address newly identified risks or to comply with legal or compliance requirements
- It is becoming increasingly hard to efficiently operate a BYOD program without using a Mobile Device Management (MDM) platform

Common BYOD Challenges and risks

- BYOD increasingly reopens traditional debates on use of personally owned laptops and computing equipment (i.e. Macs, external storage, printers)
- Use of personally owned devices blurs owner responsibilities regarding device support, ownership of data and how much access and control the organization may have to data on the device
- There is still frequent resistance by users to sign acknowledgements or acceptable use agreements (“It’s my device!”)
- Users want the latest smartphone, regardless of what operating system or features the organization is able to support
- Users have little incentive to report lost or stolen devices on a timely basis. In many cases the organization will only learn of a lost device when the user requests access for a new device
- If the user cancels carrier service, it is impossible to complete over the air device wiping

Mobile security – Controls

Policies and Procedures *

- Acceptable Use Policy
- Data Classification and Handling Policy
- Social Media Policy
- Information Security Policy
- Device Loss Process/Workflow
- Incident Management Plan

User Acknowledgement and Opt-In

- Signed User Acceptance Form
- Clear Instructions For Reporting Loss of Device
- Consent to Geo-Track (As Applicable)
- Potential Tax Impact (Certain States and Countries)
- Specific Security Training for Users
- Limits on Supported Devices

Risk Reduction Options

Technical Controls and Platforms

- Blackberry Enterprise Server
- Exchange ActiveSync
- Vendor Security Controls
- On Device Encryption
- Mobile Management Platform (MDM)
- Mobile Device Anti-Virus/Malware (As Warranted)

Auditing, Logging and Monitoring

- Periodic Audits of Mobile Program and Key Controls
- Integration with Log Management and SIEM Platforms
- Periodic Survey of Users to Confirm Compliance

* With Specific Content for Mobile Device Use

Social media

What is social media today

It is a channel for engagement that enables involvement, interaction, intimacy and influence between you, your customers and your employees

Outlet Type	Microblogs	Blogs	Media Sharing	Social Networks	Collaboration
Description	Content is much shorter than a blog.	Publishing platforms to post free-form User Generated Content (UGC)	Share various media types (photo, video, slides)	Online community of interest with blogging and sharing features.	Enterprise platforms to enable external or internal collaboration.
Key Characteristics	Limited amount of characters; Strong following; extensive outreach.	Un-edited user content posted; User can make money blogging.	Media often ranked by popularity based on views.	Hybrid platforms can share from other outlets.	Private/public communities for targeted objectives.
Popular Outlets	 	 	 	 	 

Social media in the news

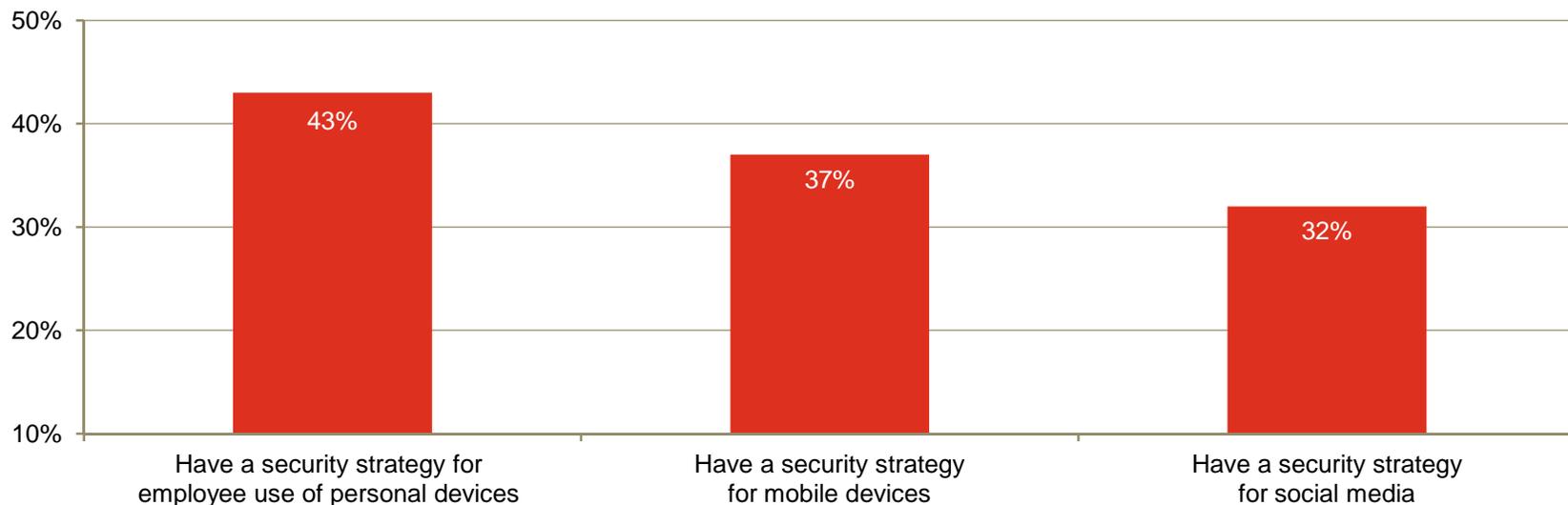
Social media opens the door to new methods of engaging customers and employees. The rapid adoption of social networking, blogs and user-created videos is revolutionizing customer expectations of how they want to interact with each other.

Unfortunately, there are also implications, including **reputational risk, regulatory requirements, intellectual property, employee relations, information security and international considerations.**

- Multi-million dollar headache for a large healthcare as a result of social media revolt over an offensive ad campaign.
- Food chain loses 10% of its value in one week, resulting in multi-million dollar losses, due to negative videos posted on YouTube.
- Several banks face severe security challenges – fake Facebook pages and phishing.

Social media: New rules and new risks

Organizations are beginning to implement strategies to keep pace with employee adoption of mobile devices and social networking, as well as use of personal technology within the enterprise. Yet much remains to be done: Less than half of respondents have implemented safeguards to protect the enterprise from the security hazards that mobile devices and social media can introduce.



Question 17: "What process information security safeguards does your organization currently have in place?" (Not all factors shown. Total does not add up to 100%.)

Typical social media risks

Information risk imperatives

Reputational & Perception

1. Reputational threat
2. Lack of Monitoring
3. Negative brand impacts
4. Crisis management
5. Insufficient employee training

Data Security and Protection

1. Identify theft
2. Malware propagation
3. Social engineering
4. Disclosure of intellectual property or other sensitive information
5. Unauthorized access and breaches through phishing, spam, and trojan horses.

Financial and Operational

1. Lack of centralized governance
2. Measuring success
3. Lack of employee productivity
4. Regulatory inquiries and possible fines

Legal & Compliance

1. Foreign and domestic privacy laws
2. Data retention
3. Regulatory compliance (PCI, FINRA, FDA)
4. Content ownership
5. Civil litigation
6. Lack of separation of personal and professional communication

Social enterprise

Social Media Governance and Executive Sponsorship

Social Media Strategy, Objectives, and Policy

Business Sponsorship

- Business objectives and KPIs
- Monitoring metrics and ROI measurement
- Information management
- Staffing

Marketing & Communications

- Social media universe and policy
- Community management
- Brand management
- Crisis management

Human Resources and Legal

- Terms of use
- Code of conduct and staff rules
- Partnership agreements
- Training and awareness

Information Security

- Authentication and authorization
- Certification & accreditation
- Monitoring & incident response
- Vulnerability scanning

Risk, Compliance, and Audit

- Risk assessments
- Risk management
- Regulatory compliance
- Internal controls
- Internal audit enforcement

Cloud computing

Introduction to cloud computing

Overview

What is cloud computing?

Cloud computing is defined by the US National Institute of Standards and Technology (NIST) as a:

Model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

- Cloud computing is often likened to utility service. Utilities, such as electricity, are available as needed and users only pay for the amount used.
- Cloud Service Providers (CSP's) have adopted the bill-for-service model, which enables companies to save money by not paying for unused or underutilized equipment, power, etc.
- Particular service offerings vary, but the largest cloud services providers (such as Amazon.com, Google, and Salesforce.com) provide computing services on what is essentially a commoditized basis – much like a utility company provides water, gas, or electricity

Threats to cloud computing

- **Compliance Complexity** – Moving data to a 3rd party cloud provider does not relieve the organization of its compliance responsibilities. A cloud based data breach can negatively impact both the organization and the cloud provider.
- **Cloud Resilience** – Moving critical data to the cloud – and then having a cloud provider go out of business or be acquired – will have some level of disruption on the organization.
- **Data Format Impact** – Some cloud providers have proprietary data formats for cloud based data. This can add complexity to change providers or terminate contracts for non-performance.
- **Security Expertise** – The level of in-house security and monitoring expertise varies widely between cloud providers. This should be a key consideration during cloud provider selection.
- **Trust But Verify** – Organizations tend to lower their guard once they outsource to a cloud provider. In reality, organizations should increase their oversight and monitoring activities.

Service delivery models and deployment models

Overview

Three Service Delivery Models:

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

Four Deployment Models:

1. Private Cloud
2. Public Cloud
3. Hybrid Cloud

Considerations for internal audit

Regulatory/Legal:

- Physical location of data storage
- Ownership of data in the cloud
- Notifications of breaches/incidents
- Responsibility for non-compliance
- Impact on SOX requirements

Due Diligence:

- Right to audit
- Assured continuity
- Security policy and process transparency
- Vendor selection/management process

Cloud computing – Controls

Policies and Procedures *

- Policy for Approval of Virtualization/Cloud
- Acceptable Use Policy
- Data Classification and Handling Policy
- Social Media Policy
- Information Security Policy
- Incident Management Plan

Contractual Controls

- Clear delineation of responsibilities between organization and cloud provider
- Standardized or generally accepted language in cloud contracts
- Service Level Agreements (SLAs) that can be measured and enforced
- Right to Audit Clause

Risk Reduction Options

Technical Controls

- Access to cloud provider's dashboards and monitoring tools
- Plug Ins to Organization's Ticketing System
- Real Time Access to Cloud Provider's Change and Issue Management platform
- Requirement for Vulnerability Scans and Attack/Penetration Testing

Other Considerations

- Exit strategy at end of contract
- Process to get data back from provider
- Contingency plan for data format conversion
- Contingency plan if cloud provider is acquired or goes out of business
- Cure provisions in the event of a data breach

* With Specific Content for Virtualization/Cloud

Questions

