

Chicago Chapter



September 16, 2008

Evolving Your Information Technology Internal Audit Function

Glenn Harkabus

**Director, Audit and Enterprise Risk Services
Deloitte & Touche, LLP (Chicago, IL)**

Scott Shinnars, CISA

**Senior Manager, Audit and Enterprise Risk Services
Deloitte & Touche, LLP (Chicago, IL)**

Objectives

- ❑ **To explore and discuss the topic of evolving IT Internal Audit Beyond SOX including emerging practices and trends in the practice of modern IT Internal Auditing**
- ❑ **To explore and discuss how IT Internal Audit can get involved in mitigating risks and driving value by connecting technology to business issues:**
 - ❖ **How a robust view of organizational IT risks can support business strategy**
 - ❖ **How an understanding of future technology risks can support more informed decision-making**
 - ❖ **Adding value through IT Internal Audit**
- ❑ **Discuss current “hot topics” and key risk areas that should be considered as potential areas for the IT Internal Audit function to add value to their organizations**
- ❑ **Discuss current IT trends such as the continued globalization of IT, ongoing regulatory changes, green or eco-friendly IT, cost containment, and other trends impacting IT**

Agenda

- **Evolving IT Audit Function**
 - ❖ **Intro and Setting the Stage for How IT Audit Functions are Changing (10 min.)**
 - ❖ **A New Continuum for IT Internal Audit**
 - **Drifting Along, Getting Aloft, or Flying High: Where Do You Want to Be (5 min.)**
 - **Attributes of a New Continuum: Summary of Key Concepts (5 min.)**
- **IT Internal Audit Topics for 2009 and Beyond**
 - ❖ **IT Project Governance (10 min.)**
 - ❖ **Data Analysis (5 min.)**
 - ❖ **M&A (5 min.)**
 - ❖ **Contract Risk and Compliance (5 min.)**
 - ❖ **Software Asset Management (10 min.)**
 - ❖ **Emerging Reporting Standards: IFRS, XBRL (10 min.)**
 - ❖ **Data Leakage (15 min.)**
 - ❖ **Process Controls Systems and Embedded Processing (5 min.)**
 - ❖ **Green IT (15 min.)**

Evolving IT Audit Function

Purpose of Internal Auditing

“Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations.

It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.”

Source: *The International Standards for the Professional Practice of Internal Auditing (Standards)*; The Institute of Internal Auditors

Evolving IT Audit Function

Definition of Risk

- ❑ The objectives of the enterprise are to:
 - ❖ Protect the value of its existing assets
 - ❖ Create new or future value
- ❑ Risk is the potential for loss of *value* or opportunity cost/loss (i.e. the sub-optimization) of value growth
- ❑ Risk may be caused by an event (or series of events) that can adversely affect the achievement of an organization's objectives

Evolving IT Audit Function

One Possible Definition of Effective Risk Management

- **Generally, Risk Management is the process of measuring, or assessing risk and developing strategies to manage it. Strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk.**

Source: From Wikipedia, the free encyclopedia (en.wikipedia.org)

Evolving IT Audit Function

Feeling Bugged Down?

- Indicators of a need to change:**
 - ❖ **How many boxes will your IT IA team check this year?**
 - ❖ **How many general computer controls will they audit?**
 - ❖ **How many years have you been telling management that it needs a comprehensive business continuity plan?**
 - ❖ **How many years have they ignored that recommendation?**
- To retain relevance, IT Internal Audit needs to continue to work with the business to gain a solid understanding of the broader set of business issues facing their organizations**
- It's about forging connections between these issues and the technology that can help address them**
- It's about taking a Risk Intelligent approach that not only seeks to mitigate risks to existing assets but also encourages appropriate, calculated risk taking for reward**

Evolving IT Audit Function

❑ Internal Audit: Beyond SOX

SOX Role

- Internal auditors played a significant role in SOX compliance
- Internal audit often diverted their resources away from other critical risk areas

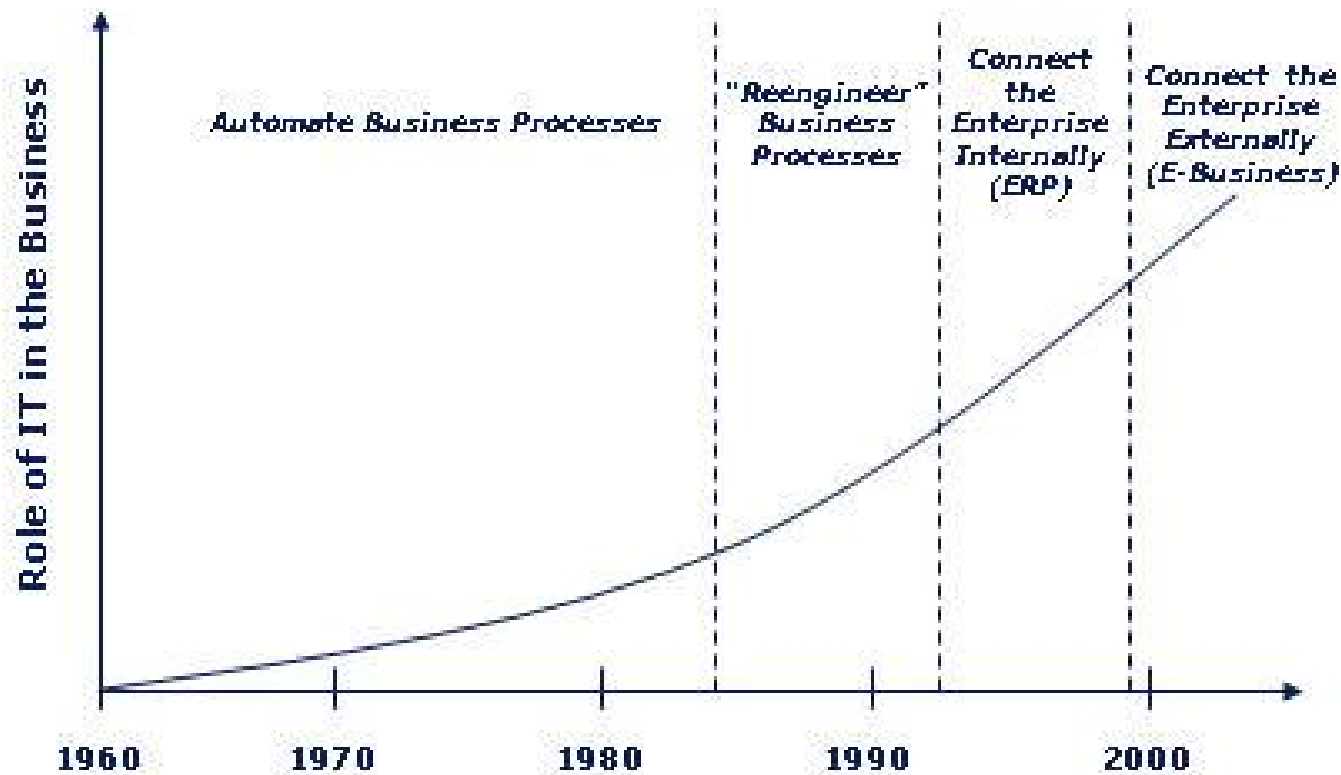
Evolving Role

- Internal audit departments are beginning to “rebalance” their activities
 - Rationalize SOX controls and processes
 - Address broader range of risks
 - Value add activities

Evolving IT Audit Function

The Role of Technology in Business

- IT has evolved from as a tool for automating business process in 1960s to a business lever



Evolving IT Audit Function

The Role of Technology in Business

		Information and Technology's Strategic Value →			
		LOW			HIGH
		Type 1: IT supports the <i>business</i>	Type 2: IT supports <i>competitive advantage</i>	Type 3: IT <i>provides</i> competitive advantage	Type 4: IT <i>is</i> the business
Role of IT	<ul style="list-style-type: none"> • Need technology to operate the business, but the company functions if IT systems fail • Timeliness and accuracy needs do not require heavy IT investment 	<ul style="list-style-type: none"> • Strategy blends technology with other capital (PP&E, supply chain, distribution, etc.) for competitive advantage • Key parts of the business depend on timely, accurate information 	<ul style="list-style-type: none"> • IT is a competitive differentiator • Timely, accurate information is often critical to business strategy 	<ul style="list-style-type: none"> • Business and IT strategies are tightly integrated • IT is explicit in the value proposition • Timely, accurate information is mission critical 	
Examples	<ul style="list-style-type: none"> • Manufacturer with "open-loop" supply chain 	<ul style="list-style-type: none"> • Manufacturer with integrated supply chain 	<ul style="list-style-type: none"> • Global express delivery service or on-line retailer 	<ul style="list-style-type: none"> • Provider of fund transfer engines or financial data products 	
		IT as commodity		IT as strategic differentiator	

Evolving IT Audit Function

We Need a New Continuum

*Where does your IT group fall along the continuum?
More important — where do you want to be?*

Type 3 – Flying High:

IT IA soars with a clear view of the future. The group is involved in value-generating work, addressing both risks and opportunities. IT IA is addressing IT risks before they become issues.

Type 2 – Getting Aloft:

IT IA has a little lift under its wings. The group helps drive current initiatives, becoming more value added and a partner with business to plan for the future.



Type 1 – Drifting Along:

IT IA floats through its audit plan, engaged in traditional GCC and systems work, diligently checking the boxes, but with no clear destination in sight.

These activities are cumulative: IT Internal Audit groups in type 3 will also engage in all the activities of types 1 and 2, addressing both the day-to-day and the longer-term issues.

Perceived Value Added

Focus (Historical → Current → Future)

Evolving IT Audit Function

Attributes of a New Continuum

- ❑ **IT Internal Audit needs to shift its focus from a historical/current orientation to a current/future orientation changing the way it works with the business:**

Type 1

- Compliance focus
- Including mostly traditional systems and IT technologies in the IT Internal Audit Universe
- Reactive to risks and changes in the environment

Type 2

- The Regulatory Present
- **IT Project Governance, Pre-Implementation**
- New Products/Services
- **Data Analysis**
- **M&A**
- **Contract Risk and Compliance**
- **Software Asset Management**
- Globalization

Type 3

- The Regulatory Future
- **Emerging Reporting Standards**
- Continuous Controls Monitoring
- **Industrial Espionage**
- **Embedded Processing Units**
- Foreign Corrupt Practices Act
- **Green IT**

IT Project Governance

Organizational Structures

- ❑ Project Leadership Team (& PMO)
 - ❖ Manages project plan, budget, issues
 - ❖ Communicates with stakeholders
 - ❖ Integrates distributed components
- ❑ Project Sponsor
 - ❖ Provides mission and funding
 - ❖ Owns success of project
- ❑ Project Steering Committee
 - ❖ Provide senior leader decisions
 - ❖ Approves significant decisions that impact project goals
 - ❖ Has appropriate power
 - ❖ Helps the Project Leadership Team achieve project goals

Governance Tools

- ❑ Project Screening Processes
 - ❖ Supports alignment with company strategies
- ❑ Standardized Methodologies and Frameworks
 - ❖ Include robust monitoring and feedback mechanisms
- ❑ Project Documentation
 - ❖ Clearly defined project charters, scope statements, and project roles

IT Project Governance

Considerations for Internal Audit

- ❑ **On which projects should Internal Audit have a role?**
 - ❖ New or unproven systems or technology development
 - ❖ Packaged software implementations (ERP)
 - ❖ Enterprise-wide scope with high business risk and impact
 - ❖ Business process reengineering and/or IT changes that impact controls
 - ❖ Processes that impact financial reporting
 - ❖ Changing job roles and responsibilities (SOD/Security)
 - ❖ Significant cost or resources allocated

- ❑ **How and what can Internal Audit contribute?**
 - ❖ **Organizationally:**
 - Part of Oversight Team or Steering Committee
 - Part of Project Management Office
 - Advisory member of sub-teams
 - Ad-hoc independent monitoring function
 - On distribution for notifications, status reports, issues lists
 - ❖ **Mechanisms:**
 - Pre-Implementation reviews
 - Post-Implementations reviews
 - Advise on planning, risk management or internal control designs

IT Project Governance

Considerations for Internal Audit

Useful Knowledge and Competencies for Project Consultation

- Understand project standards and benchmarks:**
 - ❖ Project management methodologies: PRINCE2, PMBOK, company specific
 - ❖ Data privacy standards: depends on type of data, jurisdictions
 - ❖ Software development methodologies
- Project management expertise and certification – Project Management Professional, Advance Project Management Certification, Certificate in Project Management**
- Use local resources who:**
 - ❖ Understand the ‘distance factors’
 - ❖ Will be knowledgeable of local norms
 - ❖ Will better understand how the project may affect other initiatives
- Understand how the audit can be used as a tool for integration to add value**
 - ❖ Can findings be leveraged for the planning of other projects?
- Where else can internal audit add value?**
 - ❖ Who is looking at project expenses, contract risk and vendor compliance?
 - ❖ Help with culture change management and integration?

IT Project Governance

Considerations for Internal Audit

Key Takeaways and Next Steps

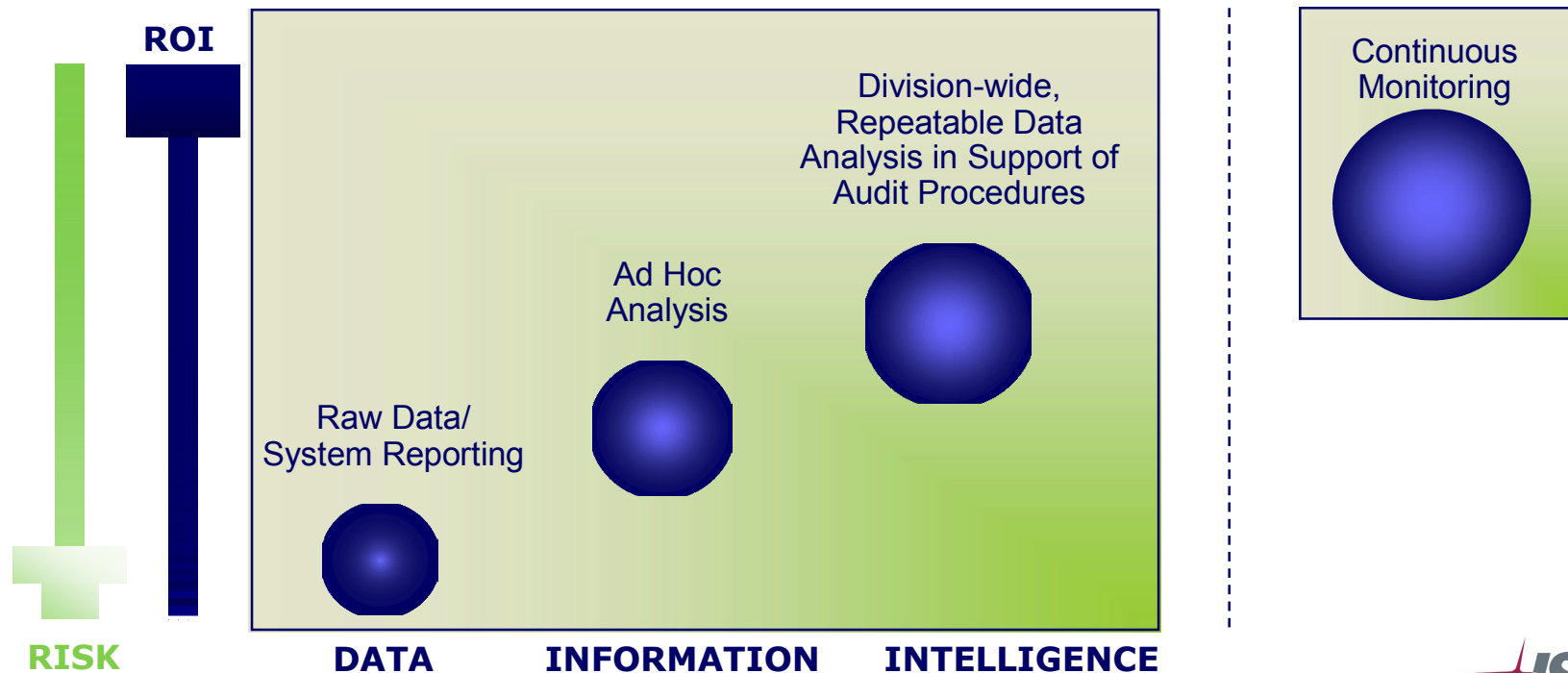
- ❑ **As an IT Internal Audit professional we need to ask if:**
 - ❖ **We are speaking the language of management? Are you assessing risk to future growth (value creation) or are you solely focused on the protection of existing assets?**
 - ❖ **We are assessing risks in isolation or are you looking at how these risks may interact and cascade?**
 - ❖ **Existing risk assessments reliably and adequately assess inherent and residual risk exposure?**
 - ❖ **We have the means to assess whether residual exposures are within the risk appetite of the company?**

Data Analysis

The Power of Information – Internal Audit Use of Data Analysis

Effective use of data analysis in internal audits provides the opportunity to turn data into meaningful information, which assists in gaining valuable insights. This capability helps to facilitate a more complete audit and an opportunity to increase return on investment (ROI) while decreasing risk.

Currently the data analysis performed across the Internal Audit groups ranges from no data analysis being performed in support of audit procedures to standardized data analysis procedures already implemented in one or more teams.



M&A

At what stage of the M&A process is IT Internal Audit consulted?

- ❑ Unlike any other group, IT Internal Audit understands the inherent — and often substantial — risks in attempting to integrate technology environments and controls
- ❑ IT Internal Audit can assist management think through the following areas of risk and reward:
 - ❖ What effect would it have on deal valuation if IT Internal Audit was called on to assess the IT environment and controls integration risks?
 - ❖ In some cases, maybe deal valuation is not even the proper measure. How about deal viability?
- ❑ Risk Intelligent IT Internal Audit Functions are those that address not just protection of existing assets but also strategic risk taking for reward

Contract Risk and Compliance

- ❑ **The Conference Executive Boards' Audit Director Roundtable names third-party relationships as one of the top hotspots for audit risk plans**
- ❑ **Stopping financial leakage is the goal ... and IT Internal Audit should be the virtual plumbers**
 - ❖ **Sophisticated data analysis routines can be built by IT internal audit as part of a contract risk and compliance program to verify accuracy and completeness**
- ❑ **If you are concerned that IT Internal Audit is perceived as a cost center rather than a revenue generator, then tackle CRC (big money could be at stake)**
 1. Many companies require some form of reporting from their business partners, but historically they have “trusted” that the information is correct
 2. Even in the most respected organizations, in spite of trust: 1) Contracts can be misunderstood, 2) Data can be misstated or manipulated, 3) activities can be misrepresented or inaccurate

Example Audits IA can perform:

- Contract Management System Audit
- Payment Analysis
- Vendor Analysis

Software Asset Management

- ❑ Gartner estimates that effective management of IT assets can save up to 30% off the lifecycle cost of software assets¹
- ❑ IT Internal Audit is uniquely positioned to add value to the organization through software asset management audits
- ❑ Benefits include:
 - ❖ Managing Risks
 - Controlling legal and financial exposure
 - Unexpected problems with acquisitions/ mergers/ divestitures
 - ❖ Controlling Costs
 - Recapture of cost from software under-deployment
 - Ability to use information for future negotiations with vendors
 - Prevention of software over-deployment, and related costs/penalties
 - ❖ Education and awareness
 - Increased level of understanding of software license agreements within the organization
 - How software licenses work within virtual environments

- Possible Internal Audits:
- Asset Management
 - Process Assessment
 - Software Usage Baseline
 - Software License Optimization

Taken from Gartner, Patricia Adams, *Management Update: IT Asset Management Stages Form the Stairway to Success*, 10 September 2003.

Software Asset Management

☐ Scoping Questions

1. How often do you contact your software vendors for support?
2. How often do you upgrade your software products?
3. Is your development in-house or outsourced? If in house, how many developers are there?
4. What Software Asset Management (SAM) and/or discovery tools do you have in place?
5. Is your IT function centralized or distributed within your organization?
6. Approximately how many servers are in your IT environment?
7. Approximately how many desktops/workstations/laptops are in your IT environment?
8. Is IT aware of and able to track every IT asset in your environment?
9. What is the operating system breakdown (%) of the above equipment?
10. Do you utilize virtual machine or partitioning technologies in your environment?
11. How do you purchase your software (direct, reseller, retail)?
12. Is your purchasing centralized or do business units have the authority to purchase independently of IT/corporate?
13. Do you have any ELA agreements in place?
14. Have you been subject to license reviews in the past?
15. Have you identified inappropriate copyrighted material in your environment?

Emerging Reporting Standards: IFRS, XBRL

- ❑ **IFRS will require significant changes in application configurations within your organization**
- ❑ **XBRL may not be far behind. Although it may not be as significant, there are IT risks related to the flow of financial information from systems using that format that should be considered**
- ❑ **Smart IT IA shops will use the lead time to help their organizations understand the issues and risks, to help drive decision-making, and to help determine the migration path and timing of the change-overs**
- ❑ **Have you begun to address these areas of risk?**
 - ❖ **Have you done a readiness assessment of your systems' ability to adapt to evolving reporting requirements?**
 - ❖ **Is it on this year's risk assessment?**

Emerging Reporting Standards: IFRS, XBRL

❑ IT Internal Audit's role in IFRS Conversion

- ❖ Understand IFRS requirements and impact on technology
- ❖ Identify technology components impacted by IFRS conversion and associated risks
- ❖ Involved as early as possible, preferably in project planning phase
- ❖ Stay involved in the remaining of the project life cycle

❑ In order to add value to IFRS conversion, IT Internal Audit should

- ❖ Maintain regular communication with the IFRS conversion project team and business owners
- ❖ Be “bilingual” in both business and technology

Data Leakage

❑ What is Data Leakage?

- ❖ The movement of a data asset from an intended state to an unintended, inappropriate or unauthorized state, representing a risk or a potentially negative impact to the organization

❑ Why is Data Protection and Security so Complex?

- ❖ Data from multiple sources is utilized by business processes and applications, and is stored in many data repositories
- ❖ Expanding Digital Universe
 - The risk of data leakage is expected to grow accordingly, along with regulatory pressure and user expectations for data protection.
 - Approximately 70% of the digital universe is created by individuals, but enterprises are responsible for the security, privacy, reliability, and compliance of 85%.*

* Source: IDC Forecast of Worldwide Information Growth Through 2011

Data Leakage

Data: Asset & Liability

- ❑ Data is both an asset and a liability. As organizations grow, the volume and complexity of data increase to support the business. Certain types of data within the enterprise data must be protected against theft, loss, and misuse.
- ❑ This data includes:

-  **PII**
-  **Patent or trade secret**
-  **Customer information**
-  **Corporate information**
-  **Medical information**

Without an effective method to:

- **Discover** data, it is difficult to apply the appropriate security controls to it
- **Classify** data, it is difficult to understand the importance and sensitivity of the data
- **Control** data, it is difficult to restrict access to data, prevent misuse of it, and secure it at rest and in transit
- **Audit** data and its usage, it is difficult to enforce the security controls

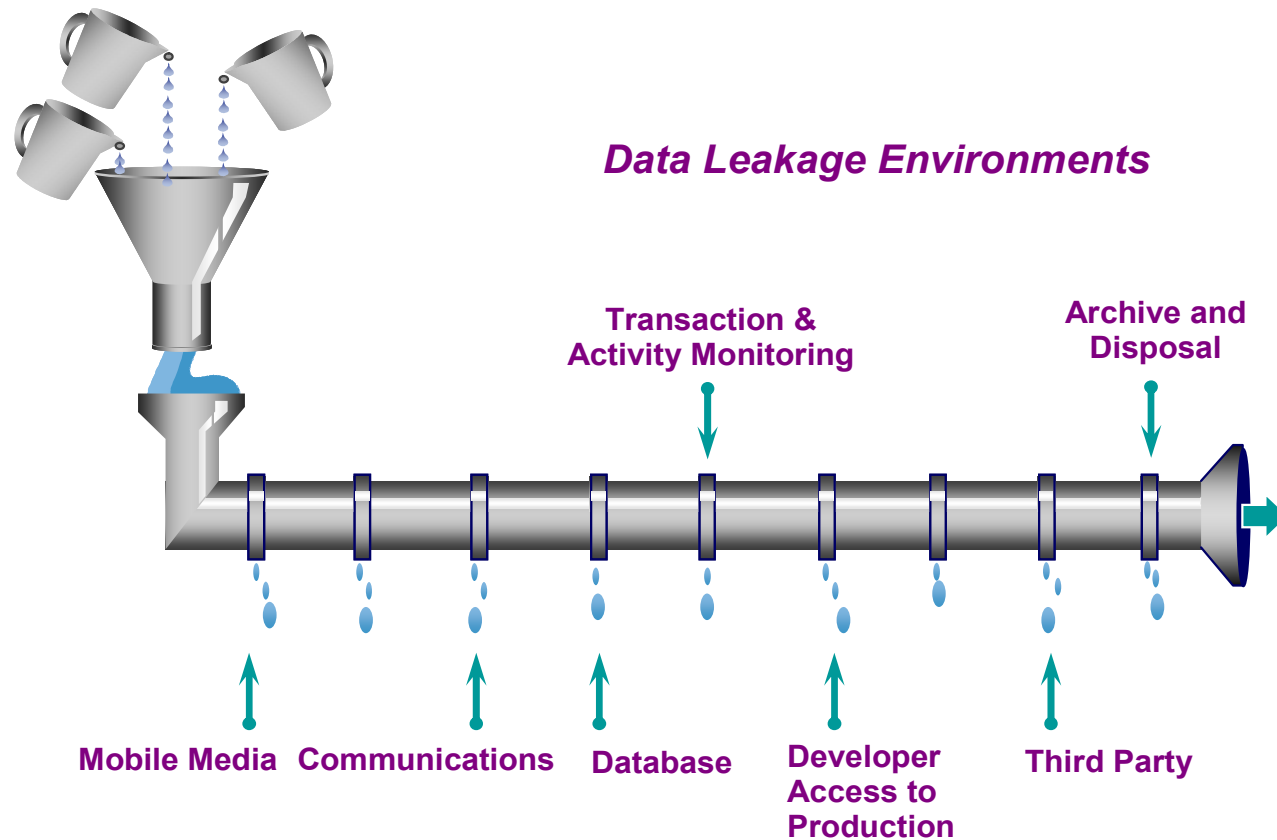
As a result, it is difficult to adequately **protect** data throughout its life cycle across the enterprise

Most organizations have not adequately protected their sensitive data because of the magnitude and diversity of the problem...a single enterprise “silver bullet” does not exist.

Data Leakage

Data Leakage Happens

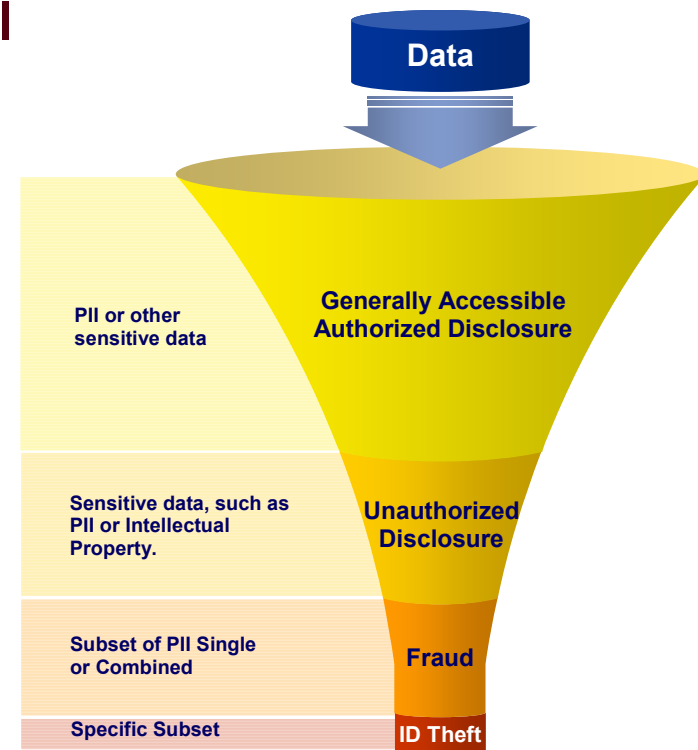
- ❑ In business, well-intentioned employees simply getting their jobs done may inadvertently put information at risk, sometimes resulting in data leakage:



Data Leakage

Anatomy of Data Leakage

- Although ID Theft has the most severe impact, other forms of enterprise data leakage are far more likely and require management attention. The majority of data losses – internal or external – are accidental
 - **Personally Identifiable Information (PII)** – Leakage of generally accessible PII and IT data occur most commonly
 - **Sensitive** – Data such as intellectual property and/or PII with a higher contextual value
 - **Fraud** – Internal or external use of PII for fraudulent gain
 - **ID Theft** – The assuming of one's identity to obtain credit for purchases. Specific subset of PII or combination



Data Leakage

❑ Business Recommendations

- ❖ Delivering Data Protection Solutions (DPS) requires engaging the business to define sensitive data, updating risk management policies, tuning business processes, raising user awareness, and integrating key DP technologies to provide policy enforcement throughout the data life cycle and the seven control environments
- ❖ Extend the risk-rationalized approach to map data flows through the relevant control environments and develop leakage controls
- ❖ Recommendation: Implement environment-specific controls in order to reduce the likelihood and impact of data transfer from an intended to unintended state

Data Leakage

- **Recommendations for IT Internal Audit for assisting the business moving forward with DP solutions:**
 - ❖ **Assess the process management has implemented to define the sensitive data to protect, as this will drive the requirements for content-detection mechanisms. Where management has not done so, recommend a process be implemented**
 - ❖ **Assist management develop rationalized requirements, including external mandates to be supported that are tied to your organizations other IT security goals**
 - ❖ **Map specific detection requirements into each of these mandates by the sensitive data definition**
 - ❖ **Define location and response requirements, including which control environments to address and the business scenarios for detecting sensitive data**
 - ❖ **Assess your organization's incident response procedures for how well they address data leakage (monitor, block, encrypt and forward)**
 - ❖ **Assist management develop the appropriate level of controls in connection with their implementation of a DLP solution in stages aligned with prioritized business risk areas**
 - ❖ **Assist management assess various technology options and software tools available in the market to address these risks**

Process Controls Systems and Embedded Processing Units

- ❑ Kiosks have become as ubiquitous as the phone booths of yesteryear. Supermarket self-checkout stations. Airport ticketing machines. Standalone ATMs.
- ❑ EPUs have smart manufacturing and programming logic built in, along with autonomous functions, operating system, and software. Like HAL of “2001,” they almost qualify as independent life forms. And like that rogue computer, they can cause problems if not properly managed. For example ...
 - ❖ How do you update the OS and software?
 - ❖ How do you secure the units?
 - ❖ Do you know what networks they are attached to?
 - ❖ How do you know if they are compromised?
 - ❖ What safeguards are in place?
 - ❖ Or maybe the questions are more basic:
 - Do you even have an accurate inventory of EPU installs?
 - Determine what embedded systems are in place or planned?
 - Evaluate the risk around these?

Green IT

What is Corporate Responsibility and Sustainability (CR&S)?

- ❑ **The continual improvement of business operations to support long term resource availability through environmental, socially sensitive, and transparent performance as it relates to consumers, business partners and the community**

Environmental

- Energy Conservation
- Water Conservation & Quality
- Emissions Reduction
- Recycling
- Re-use of Materials
- Biodiversity
- Land Use Management
- Greenhouse Gas Management

Social

- Fair Trade
- Working Conditions
- Health & Wellness
- Diversity
- Anti-Corruption and Bribery
- Safety

Financial

- Ethics
- Corporate Governance

Green IT

What is Green IT?

- ❑ **Green IT primary objectives:**
 - ❖ **Create ROI by pursuing Green IT initiatives**
 - ❖ **Create competitive advantage by pursuing Green IT initiatives**
 - ❖ **Managing IT's growing power requirements to support the increasing reliance on technology to support business applications**
 - ❖ **Complying with regulations at the Federal, State, and Local levels**
 - ❖ **Mitigating the risk of bad publicity arising from manufacturing pollution**

- ❑ **What Does Green IT Include?**
 - ❖ **Green Strategy**
 - ❖ **Infrastructure Optimization**
 - ❖ **Data Center transformation**
 - ❖ **Cost Reduction**
 - ❖ **Green Sourcing & Procurement**
 - ❖ **Capacity Management & Provisioning**
 - ❖ **Green Audit & Due Diligence**
 - ❖ **Asset Management**

Green IT

Why Are We Not Greening IT?

- Lack of stakeholder and/or executive support
- IT buyers are simply unaware of the problems
- IT is often not the focus of a company's green activities
- IT's goals of reliability and performance might be compromised
- Payback from green IT initiatives is uncertain or long term
- Customers see green IT as vendor marketing hype or "greenwash"
- Approach to greening IT is haphazard or piecemeal
- Green IT "plate" may be too full from trying to achieve too much at once, thereby neglecting other vital IT programs
- Waiting until federal regulations are mandated, then spend vast sums of capital and face implementation risks just to play "follow the leader"

Green IT – What Can Be Done?

❑ Green Data Center

- ❖ Data Center Consolidations
- ❖ Cooling Redesign & Upgrade
- ❖ Server Architecture Consolidation / Optimization
- ❖ Server and Storage Virtualization
- ❖ Application Rationalization
- ❖ Emissions Tracking and Monitoring
- ❖ DC Layout Redesign
- ❖ Energy Cost Reduction
- ❖ Equipment Lifecycle & Waste Management
- ❖ Alternative Energy Sources
- ❖ Application Hosting Green Server Farms

❑ Green IT Workforce

- ❖ EPEAT and ENERGY STAR Equipment Migration (PCs, printers, fax/copier)
- ❖ Telecommuting friendly companies (“Green Networks”)
- ❖ Equipment Lifecycle, Recycling and Waste Management
- ❖ Green IT Workplace Practices & Culture
- ❖ Green Workplace & IT Design (e.g. fewer powered Ethernet ports, wireless LANs, optimized AC)
- ❖ Thin Clients, Thin Provisioning / Storage Management
- ❖ PC Power Management

Green IT Internal Audit

❑ Role of IT Internal Audit

- ❖ Depends on where the organization is WRT CSR and Green IT initiatives
- ❖ IT Internal Audit can broaden their role and increase their value by:
 - Facilitating identification and evaluation of relevant risks/opportunities regarding CR&S initiatives, including Green IT, across the enterprise
 - Guiding management to take appropriate actions
 - Taking initiatives to help manage risks and demonstrate efficiency
 - Reporting on the consolidated CR&S and Green IT strategy and the company's progress against the plan
 - Championing the establishment of CR&S and Green IT and its reporting practices

❑ Specific Actions:

- ❖ Conducting independent and objective assessments of the organization's system of internal controls for CS&R and Green IT
- ❖ Implementing appropriate information disclosure and proactive support to improve control procedures
- ❖ Ensuring strict compliance with laws and internal regulations
- ❖ Conducting independent investigations into allegations of fraud and violations of the organization's CS&R and Green IT practices
- ❖ Reporting as necessary on the corporate CS&R and Green IT strategy and activities

Green IT Internal Audit

Possible Actions for Internal Audit

- ❑ **How can internal audit add value?**
 - ❖ **Identifying significant / critical CS&R and Green IT issues within the organization's risk universe**
 - ❖ **Auditing non-financial CS&R and Green IT performance indicators and associated targets / objectives**
 - Reviewing processes to collect data, test accuracy of information, evaluating plausibility of information that cannot be tested
 - Verifying that objectives and targets are reviewed periodically, adjusted as needed and communicated
 - ❖ **Developing / creating audit frameworks for testing CSR and Green IT activities and data**
 - GRI, ISO 14001, OHSAS 18001, SA 8000, COSO, etc.
 - ❖ **Evaluating (effectiveness/efficiency) of CSR and Green IT management system and programs**

Green IT Internal Audit

Possible Actions for Internal Audit

- ❑ **How can internal audit add value?**
 - ❖ **Bringing a degree of rigor to conducting CSR and Green IT audits - performing limited scope, supply chain, and compliance audits**
 - ❖ **Coordinate audit activities by external assurance providers**
 - ❖ **Reporting on CSR and Green IT progress, performance and issues in a language familiar to the Board and Audit Committee**

Open Discussion



Deloitte.

Member of
Deloitte Touche Tohmatsu