IT for IA Fundamentals
A. Welcome and Introduction
Agenda

A. Welcome and Introduction

B. Intro to Technology Audit

C. Technology Frameworks, Standards and Regulations

D. Technology Risk Assessment and Scoping

G. Wrap Up and Conclusion
B. Introduction to Technology Audit
Learning objectives

After this module, you will be able to:

• Understand current technology trends, challenges and what this means for Internal Audit
• Understand the heightened expectations of Internal Audit
• Introduction to Internal Technology Audit domain model
Technology Disruption - Video

https://youtu.be/gyI1wekNB_Y
Technology disruption is resulting in increased expectations of Internal Audit

Key Trends
- Cybersecurity & Privacy Risk
  - Theft of customer data and intellectual property
  - Organized crime activity
  - Global ecosystem
- Digital Disruption
  - Social
  - Mobile
  - Analytics
  - Cloud
- Business & Technology Transformation
  - Consumerization of IT
  - Evolving business models
  - Massive transformation of applications and infrastructure
- Big Data
  - Increased transaction volumes
  - Data quality
  - Data governance & management
- Regulatory Pressure
  - Complex regulatory environment
  - Increased pressure and audits

What this means for our Internal Audit
- Expectations
  - Higher expectations from executive management and boards
- Drive Value
  - Greater focus on quality and driving value and impact from investment in Internal Audit
- Trusted Advisor
  - Provide proactive strategic advice to the business

What this means for Internal Technology Audit
- Clarity
  - Need to clearly articulate full suite of IT Internal Audit solutions
- Leadership
  - Opportunities to grow, innovate, and drive quality
- Differentiation
  - Organic and inorganic growth through specialization

Growing expectation that Internal Audit is addressing these risks
Top 11 drivers that will create the biggest challenge for companies in the next 18 months

<table>
<thead>
<tr>
<th>Driver</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data security and privacy</td>
<td>80%</td>
</tr>
<tr>
<td>Cost pressures</td>
<td>70%</td>
</tr>
<tr>
<td>Talent availability</td>
<td>60%</td>
</tr>
<tr>
<td>Reputation risk</td>
<td>60%</td>
</tr>
<tr>
<td>Emerging technology risk</td>
<td>50%</td>
</tr>
<tr>
<td>Shifts in competition</td>
<td>40%</td>
</tr>
<tr>
<td>Growing dependence on third-party vendors</td>
<td>40%</td>
</tr>
<tr>
<td>Financial market volatility</td>
<td>40%</td>
</tr>
<tr>
<td>Changing consumer behavior</td>
<td>30%</td>
</tr>
<tr>
<td>Commodity market risks</td>
<td>30%</td>
</tr>
<tr>
<td>Velocity of business change</td>
<td>20%</td>
</tr>
</tbody>
</table>

2015 State of the Internal Audit Professional Study
Skills that are important for Internal Audit function to possess

- Financial controls
- General IT
- Specialized IT (e.g., cybersecurity)
- Data privacy
- Business continuity
- Data analysis
- Compliance (including fraud and ethics)
- Supply chain
- Engineering
- Six sigma (or other lean concepts)

2015 State of the Internal Audit Professional Study
Not your Mama’s Technology Audit
It’s much more than IT General Controls

Cybersecurity & Emerging Technology
- Cybersecurity
- Emerging Technologies (cloud, mobility, social media, etc.)
- Threat & Vulnerability Management (e.g. A&P)
- Network, Operating System, And Database Security
- Technology Regulatory Compliance (ISO, NIST, PCI)

Project Assurance
- Real-time Project Assurance
- Portfolio Optimization
- Program and Project Management
- Benefits Realization
- Controls Outcome

IT Governance & Service Delivery
- IT Governance & Strategy
- IT Asset Management
- Data Governance
- Global IT Operations
- Systems Development & IT Change Management
- Business Resiliency
- Third Party Risk Management

Business Applications
- Business Process Controls
- User Access & Segregation of Duties
- System interfaces and data quality
- ERP Optimization
- Automated Controls & Configurations
C. Technology Frameworks, Standards & Regulations
Learning objectives

After this module, you will be able to:

• Articulate the different technology related regulations that impact today’s organizations
• Discuss the impact regulations have on the Technology Internal Audit function
• Describe the different types of frameworks and standards leveraged to manage IT risks
Technology Audit – Frameworks, standards and regulations

- **Frameworks** - (e.g. COBIT 5.0, NIST CyberSecurity), ITIL
- **Standards** - NIST (e.g. 800-53), ISO, PMBOK
- **Regulations** - (e.g. SOX, PCI)
Technology regulatory environment overview

- Compliance is about more than prevention. It’s also about navigating opportunities.
- Some laws are industry-specific, such as:
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Gramm-Leach-Bliley Act (GLBA),
  - Payment Card Industry Data Security Standard (PCI DSS).

However, the lines are becoming blurred (e.g. corporate health data, pharmacies at retailers)
Role of technology Internal Audit in a changing regulatory environment

Technology Internal Audit functions must consider the following as it establishes its role in regulatory reforms:

• Technology audit function positioning
• Technology audit risk assessment and audit plan coverage
• Methodology and expertise
### Significant Technology related regulations/guidance

#### Example listing

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HIPAA</strong> - Health Insurance Portability and Accountability Act</td>
<td>The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information.</td>
</tr>
<tr>
<td><strong>HITECH</strong> - Health Information Technology for Economic and Clinical Health Act.</td>
<td>HITECH Act widens the scope of privacy and security protections available under HIPAA; it increases the potential legal liability for non-compliance; and it provides for more enforcement.</td>
</tr>
<tr>
<td><strong>PCI</strong> - Payment Card Industry Data Security Standard</td>
<td>The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.</td>
</tr>
</tbody>
</table>
# Significant Technology related regulations/standards

Example listing

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GLBA - Gramm-Leach-Bliley Act</strong></td>
<td>The Financial Privacy Rule governs the collection and disclosure of customers’ personal financial information by financial institutions. It also applies to companies, regardless of whether they are financial institutions, who receive such information.</td>
</tr>
<tr>
<td></td>
<td>The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information.</td>
</tr>
<tr>
<td><strong>SOX- Sarbanes-Oxley Act</strong></td>
<td>Established (among other things) IT control requirements to ensure the accuracy and completeness of financial statements as well as the prevention/detection of fraud.</td>
</tr>
<tr>
<td><strong>NERC-CIP – North American Reliability Corporation Critical Infrastructure Protection</strong></td>
<td>Standards for protecting the bulk power system against cybersecurity compromises that could lead to misoperation or instability.</td>
</tr>
</tbody>
</table>
Example – Regulations impact on IT outsource providers

When outsourcing an IT solution, companies face the risk that sensitive customer data may end up in the service provider’s custody. In that case data breaches could result in security and privacy violations as indicated by regulations such as HIPAA, GLBA, and the EU’s Data Protection Act, depending on the company’s type of work and country of operations.

HIPAA: HIPAA applies to U.S. organizations working in the health-care industry. The standard also addresses the security and privacy of electronic health information systems and data, including policies and procedures for:

- Securing the privacy of electronic information.
- Preventing unauthorized access to and disclosure of health-care information.
- Maintaining audit trails in computerized record systems.

Service providers that provide IT services to organizations in the health-care industry must comply with HIPAA.
GLBA: This act applies to financial institutions that provide financial products and services to consumers, such as:

- Lending, brokering, or servicing any type of consumer loan
- Transferring or safeguarding money
- Preparing individual tax returns
- Providing financial advice or credit counseling
- Offering real estate settlement services
- Collecting consumer debts.

If any IT services are outsourced by a financial institution, the service provider must comply with the act’s requirements. The service provider should ensure that:

- Prevent unauthorized access to work area and network used for processing of financial information
- Data processing and storage security measures are implemented
- Network security and controls are implemented for securing data transmissions

The security requirements to be practiced by the service provider for compliance are the same as those described above for HIPAA and GLBA.
## IT Standards & Frameworks Defined

### Frameworks vs. Standards

<table>
<thead>
<tr>
<th>Framework</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>A technical framework helps define an <strong>approach</strong> to implementing, maintaining, monitoring, and improving information technology programs. ITIL and COBIT are frameworks.</td>
<td>A technical <strong>standard</strong> is an established norm or requirement in regard to technical systems. It is usually a formal document that establishes uniform engineering or technical criteria, methods, processes and practices. ISO 27001 and NIST 800.53 are standards.</td>
</tr>
</tbody>
</table>
# Significant Technology related Frameworks & Standards

Example listing

<table>
<thead>
<tr>
<th>Framework/Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>COBIT (v. 5.0) Framework</strong></td>
<td>It's the leading framework published by ISACA for the governance and management of enterprise IT.</td>
</tr>
<tr>
<td>Control Objectives for Information and related Technology</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://cobitonline.isaca.org/">https://cobitonline.isaca.org/</a></td>
</tr>
<tr>
<td><strong>COSO 2013 Framework</strong></td>
<td>Principle 11 (of 17) of the Framework addresses IT.</td>
</tr>
<tr>
<td>The Committee of Sponsoring Organizations of the Treadway Commission</td>
<td>The organization selects and develops general control activities over technology to support the achievement of objectives.</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.coso.org">www.coso.org</a></td>
</tr>
<tr>
<td><strong>NIST Cyber Security Framework</strong></td>
<td>Guidance for critical infrastructure organizations to better manage and reduce cybersecurity risk. The framework has five domains: Identify, Protect, Detect, Respond, and Recover</td>
</tr>
<tr>
<td>National Institute of Standards and Technology</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="http://www.nist.gov/cyberframework">www.nist.gov/cyberframework</a></td>
</tr>
</tbody>
</table>
## Significant Technology related Frameworks & Standards
 Example listing

<table>
<thead>
<tr>
<th>Framework/Standard</th>
<th>Description</th>
</tr>
</thead>
</table>
| **ITIL – Information Technology Infrastructure Library** | ITIL is a widely and globally accepted set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business.  
| **NIST Information Technology** – National Institute of Standards and Technology | The development of management, administrative, technical and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.  
| **PMBOK – Project Management Body of Knowledge** | PMI (Project Management Institute) global standards provide guidelines, rules and characteristics for project, program and portfolio management.  
## Significant Technology related Frameworks & Standards

### Example listing

<table>
<thead>
<tr>
<th>Framework/Standard</th>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>27001 &amp; 27002</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CSA</strong> — Cloud Security Alliance</td>
<td>Established a set of best practices and controls related to cloud computing.</td>
<td><a href="http://www.cloudsecurityalliance.org">www.cloudsecurityalliance.org</a></td>
</tr>
</tbody>
</table>

The Institute of Internal Auditors issue supplemental detailed practice guidance for conducting Technology Internal Audit activities. These include topical areas, sector-specific issues, as well as processes and procedures, tools and techniques, programs, step-by-step approaches, and examples of deliverables.

• GTAGs (Global Technology Audit Guides):
  - GTAGs are guides to the Assessment of IT Risk (GAIT)
• GAIT Methodology:
  - GAIT for Business and IT Risk
  - GAIT for IT General Control Deficiency Assessment
Standards & guidance – International Professional Practices Framework (IPPF) (continued)

<table>
<thead>
<tr>
<th>Attribute standards *</th>
<th>Performance standards **</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practice advisories</td>
<td>Practice guides</td>
</tr>
</tbody>
</table>

### Global Technology Audit Guides (GTAG)

- **GTAG 1 – IT Controls**
- **GTAG 2 – Change and Patch Mgt**
- **GTAG 3 – Continuous Auditing**
- **GTAG 4 – Managing IT Audit**
- **GTAG 5 – Mg & Auditing Privacy Risks**
- **GTAG 6 – Mg & Auditing IT Vulnerabilities**
- **GTAG 7 – IT Outsourcing**
- **GTAG 8 – Auditing Application Controls**
- **GTAG 9 – Identity and Access Mgt**
- **GTAG 10 – Business Continuity Mgt**
- **GTAG 11 – Developing the IT Audit Plan**
- **GTAG 12 – Auditing Projects**

### Guide to the Assessment of IT Risk (GAIT)

- **GAIT Methodology**
- **GAIT for ITGCC Deficiencies**
- **GAIT for Business and IT Risk (GAIT-R)**

Link: [https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Practice-Guides.aspx](https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Practice-Guides.aspx)
Learning check

Multiple Choice Question

• Which of the following would be the “best” standard to review Information Security related control topics
  A. COBIT
  B. PMBOK
  C. COSO
  D. ISO 27001
  ◦ A
  ◦ B
  ◦ A & C
  ◦ D
D. IT Risk Assessment and Scoping
Learning objectives

After this module, you will be able to:

• Articulate that there are business consequences to IT Risk
• Discuss two different levels of IT risk assessment
Technology Risk Assessment Process

**Step 1: Develop Firm-Wide Technology Risk Profile**

- Evaluate nature and extent of technology use
- Understand level of business dependence on technology
- Quantify business impact of IT risk
- Understand the distribution of technology risk
- Understand significance of key risk drivers

**Step 2: Establish Technology Risk Universe**

- Review Application Portfolio
- Review IT Project Portfolio
- Review IT Service Management/Delivery Functions
- Review IT Infrastructure/Cyber

**Step 3: Perform Detailed IT Audit Risk Assessment**

- Understand IT Control environment
- Perform detailed IT Risk assessment
- Develop detailed technology risk coverage roadmap

Risk Identification  →  Risk Classification  →  Long-Term Coverage
Introduction to two levels of IT risk assessment

All technology is “business” technology...and supports the client’s objective of remaining a going concern. Just as all Information Technology in use at a firm exists only to support business objectives, “technology risk” is only relevant because of its business consequences.

<table>
<thead>
<tr>
<th>Technology Inherent Risk Assessment</th>
<th>Detailed Technology Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk assessment related understanding the nature and extent of technology use at an organization and the business risk technology use imputes</td>
<td>Risk assessment related to the planning and scoping of an annual or multi-year IT audit plan.</td>
</tr>
</tbody>
</table>

Assesses the stability and complexity of the technology environment, the businesses dependence upon technology, and key risk indicators to quantify the potential business consequences of IT risk.

Assesses specific IT and Business entities in the risk universe to develop an integrated technology audit plan.
**Firm-wide Technology Inherent Risk Profile**

The likelihood of a negative technology event occurring can be assessed by an analysis of risk attributes related to business factors, the technology environment and the threat landscape help define the firm’s business/technology risk relationship. Consider the following four factors.

<table>
<thead>
<tr>
<th>Stability</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>The stability and/or degree of change in both the business and IT</td>
<td>The level of business and technology complexity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dependence</th>
<th>Exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td>The level of dependence the business has on technology</td>
<td>The vulnerability of the IT environment</td>
</tr>
</tbody>
</table>
Firm-wide Technology Inherent Risk Profile

The impact of a negative technology event can be pervasive. It can interrupt operations, erode earnings, alienate customers and arouse the interest of regulators... just to name a few. But... most technology risk has the same four basic and fundamental drivers

<table>
<thead>
<tr>
<th>Access</th>
<th>Unauthorized disclosure of information/ inappropriate access to systems, data or functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td>Insufficient accuracy, timeliness, or completeness of information and data dependent processes</td>
</tr>
<tr>
<td>Availability</td>
<td>Technology dependent business processes and associated data are not accessible within acceptable timeframes and performance thresholds</td>
</tr>
<tr>
<td>Agility</td>
<td>Enabling technologies and associated processes are not able to respond to business change with reasonable speed and cost</td>
</tr>
</tbody>
</table>

Inspired by the Westerman model, MIT Sloan - Center for Information System Research
**Firm-wide Technology Inherent Risk Profile**

By thinking about risk in this manner... and understanding the affinity between the various impact attributes and risk drivers one can begin to paint a picture of IT risk at an organization, and begin to develop a focused coverage strategy.

![IT Audit Domain/Risk Affinity](image1)

![Risk Drivers](image2)
Detailed Technology Risk assessment activities

1. Understand stakeholder objectives
2. Identify key risk areas
3. Gather information
4. Develop risk universe
5. Evaluate and prioritize risks
6. Develop audit plan
7. Operationalize the plan
8. Perform ongoing monitoring
9. Continually reassess risk
10. Report

Ongoing risk assessment
## Technology audit – Risk assessment fundamentals

### IT Risk Universe

| Business strategy | IT strategy | Strategic initiatives | IT governance | Policies & standards | Portfolio management | Manage finances | Manage human capital | Manage talent | Project management | Manage technology acquisition | System & process development | Manage change | Manage service delivery | Manage resiliency | Manage information security | Manage IT infrastructure | Manage vendors | Manage data | Manage compliance | Monitor |
|-------------------|-------------|-----------------------|---------------|---------------------|----------------------|---------------------|------------------|---------------------|----------------|-------------------|-----------------------------|-----------------------------|---------------|----------------------|----------------------|-----------------------------|----------------------|-------------|--------------|----------------------|---------|
| CEO               | CIO         | CRO                   | CMO           | AC Chair            | CAE                  | CEO                 | CFO              | CMO                 | CRO             | CIO               | CMO                         | CRO                         | CMO            | CMO                   | CMO                   | CMO                         | CMO                 | CMO          | CMO          | CMO                  | CMO     |
Technology audit – Risk assessment fundamentals
Risk profiles

INHERENT RISK

CONTROL EFFECTIVENESS

RESIDUAL RISK

Third Party Risk
Data Integrity Risk
Emerging Tech Risk
Digital Disruption Risk
Project Risk
Cyber Security Risk
Privacy Risk
Technology audit – Risk assessment
Strategy & profile

- Technology Audit
- Risk Universe
- Service Quality
- Architecture Complexity
- Data Integrity
- Volume of Program Changes
- Cyber Threats / Privacy
- Availability
- Volume of Users
- Governance

Business Strategy

Stakeholder Input

Technology Audit - Risk Assessment

High Risk Entities – Continuous?
   Medium Risk Entities
   Low Risk Entities

IT Internal Audit Plan
Bio

Eric C. Lovell

Director, Carolinas Internal Technology Audit Solutions Leader

Eric is a Director and has more than 15 years of experience in Information Technology Internal Audit, Technology Architecture, IT Management, Cybersecurity, IT Governance, Risk and Compliance.

He has worked with a variety of internal audit functions assessing, designing, and implementing technology audit solutions to meet the needs of changing business and technology environments, and subsequent increases in board and regulatory expectations. Eric specializes in providing technology and information security audit services for large multinational organizations across a wide array of industries. His experience spans leading risk based information security program assessments; system development/pre-implementation audits, security & privacy focused third party vendor reviews and performing technology audits over IT infrastructure, e-commerce/e-banking solutions and emerging technologies, such as cloud services.

Eric has significant experience designing and implementing cybersecurity and system implementation audit and assurance programs and has performed numerous IT governance and Information Security governance assessments. Recent assessments have included deep dives into Information Security program effectiveness, management oversight, framework selection, and cybermetrics.

Eric’s primary area of focus today is the strategic program development for internal technology audit, cybersecurity, and IT Risk. His experience gives him a unique perspective in solving those tough challenges facing today’s technology audit functions.

Prior to joining PWC, Eric was Director of IT Internal Audit at Ally in Charlotte, NC.

He serves on the Board of the Charlotte, NC chapter of InfraGard and is responsible for coordinating member symposia and special events.

Education and certifications

• B.S. Criminal Justice - Appalachian State University
• M.A. International Politics – Appalachian State University
• MBA – McColl School of Business; Queens University
• Certified Information Systems Auditor (CISA)
• Certified Green Belt, Six Sigma
• Certified Help Desk Director