Internal Audit, Risk, Business & Technology Consulting

TAKING TECHNOLOGY AUDIT TO THE NEXT LEVEL

ACUA 2023

protiviti®

Face the Future with Confidence

TODAY'S TOPICS

1. Developing a Comprehensive the Technology Audit Universe
2. Emerging IT Risk
3. Unlocking the Advisor Role

DEVELOPING A COMPREHENSIVE TECHNOLOGY AUDIT UNIVERSE

QUESTION #1

How confident are you that your Technology Audit universe includes the correct domains and controls frameworks?

A. **Have Not Developed a Technology Audit Universe**
B. **Not Confident**
C. **Moderately Confident**
D. **Very Confident**

WHERE TO START?

Have you gotten to know the IT organization?

- **Organizational Model** – Centralized, Federated, Decentralized, etc.
- **Software Development Methodology** – Waterfall, Agile, DevOps, Hybrid, etc.?
- **Software Development Quantification** – How much true development (coding and deployment) is done?
- **On-Prem versus Cloud** – Where is data hosted?
- **Cloud Footprint** – If cloud, what type of cloud hosting? (e.g., SaaS, IaaS, PaaS)
- **Third Party Reliance** – Are their critical third-party dependencies for IT to operate? Managed Services?
- **Mandatory IT Compliance Requirements** – What are the compliance related must-haves (FERPA, State, Federal, Privacy, Financial Reporting, etc.)? What are the penalties for not having these requirements in place?
- **IT Frameworks** – Does management know which frameworks they have adopted or are required to adopt?

WHAT FRAMEWORKS?

Understanding operational and compliance risk and anchoring to the right framework(s)

Secure Controls Framework "SCF" – Everything in One Place (with mapping!)

- IT Domain Capability Maturity Model "CMM" definitions (level 0-5)
- Accounting Standards – AICPA
- Internal Controls Standards – COBIT, COSO, ISO, BSI
- Cloud & Web Frameworks – CSA, OWASP
- Cybersecurity – CIS, CSC, NIST, PCI, ENISA, SWIFT, UL, C2M2, CMMC, CISA, DFARS, FedRAMP, FERPA, HIPAA, State Cybersecurity Frameworks (e.g., Texas Department of Information Resources "DIR")
- Privacy – GAPP, GDPR, State Privacy Acts (e.g., California Privacy Rights Act),
- Risk & Threat Mapping – Risk & Threat Descriptions
- Third Party Risk Management – Shared Assessments

SCF | SECURE CONTROLS FRAMEWORK

THE RIGHT VIEW FOR YOUR INSTITUTION

Define domains, assign a risk scoring, and map historical audit coverage

IT Domain	Risk Score	2021				2022				2023				2024 (Proposed)			
		#1	#2	#3	#4	#1	#2	#3	#4	#1	#2	#3	#4	#1	#2	#3	#4
Cybersecurity	Critical	✓	✓	✓	✓	✓	✓			✓	✓			✓	✓	✓	✓
IT Governance and Strategy	Critical									✓	✓	✓	✓	✓	✓	✓	✓
Contingency Planning, Business Continuity, & Disaster Recovery	Critical					✓	✓									✓	
Access Control & Identity Management	High									✓	✓	✓	✓				
Data Governance, Protection & Privacy	High							✓									
Incident Response	High	✓	✓	✓	✓					✓	✓	✓	✓				
IT Asset Management	High	✓	✓	✓	✓	✓	✓			✓	✓						
Risk / Security Assessments & Third-Party Management	High					✓	✓	✓	✓	✓	✓			✓	✓	✓	✓
IT Infrastructure, Operations, and Maintenance	High	✓	✓	✓	✓					✓	✓	✓	✓				
Physical / Environmental Control	High					✓	✓										
Change Management	Medium	✓	✓	✓	✓												
Configuration Management	Medium					✓	✓			✓	✓						
System Development Lifecycle & Acquisitions	Medium					✓	✓	✓	✓								
Awareness and Training	Low	✓	✓	✓	✓												

PUTTING IT ON THE PLAN

Does the domain need audit coverage this year?

IT Domain	Risk Score	#1	#2	#3	#4	On Audit Plan?	Engagement Name	Notes	Why Not?
Information, System, and Communication Security (Cyber)	Critical	C	C	C	C				
IT Governance and Strategy	Critical	C	C	C	C				
Contingency Planning, Business Continuity, & Disaster Recovery	Critical	C	C	C	H				
Access Control & Identity Management	High	C	H	H	M				
Incident Response	High	C	H	H	M				
IT Asset Management	High	H	H	M	N/A				
Data Governance, Protection & Privacy	High	H	H	H	M				
IT Infrastructure, Operations, and Maintenance	High	H	H	H	N/A				
IT Third-Party Management	High	H	H	M	M				
Physical / Environmental Control	High	H	M	M	N/A				
Configuration Management	Medium	M	M	M	L				
Change Management	Medium	M	M	M	N/A				
System Development Lifecycle & Acquisitions	Medium	H	M	M	L				
Awareness and Training	Low	M	L	L	L				

EMERGING IT RISK

IDENTIFYING EMERGING RISK

Are You Focused On The Right Things?

More than just IT General Controls?

Alignment with institution level goals?

Alignment with IT Organization objectives?

Mix of historical coverage and emerging risk?

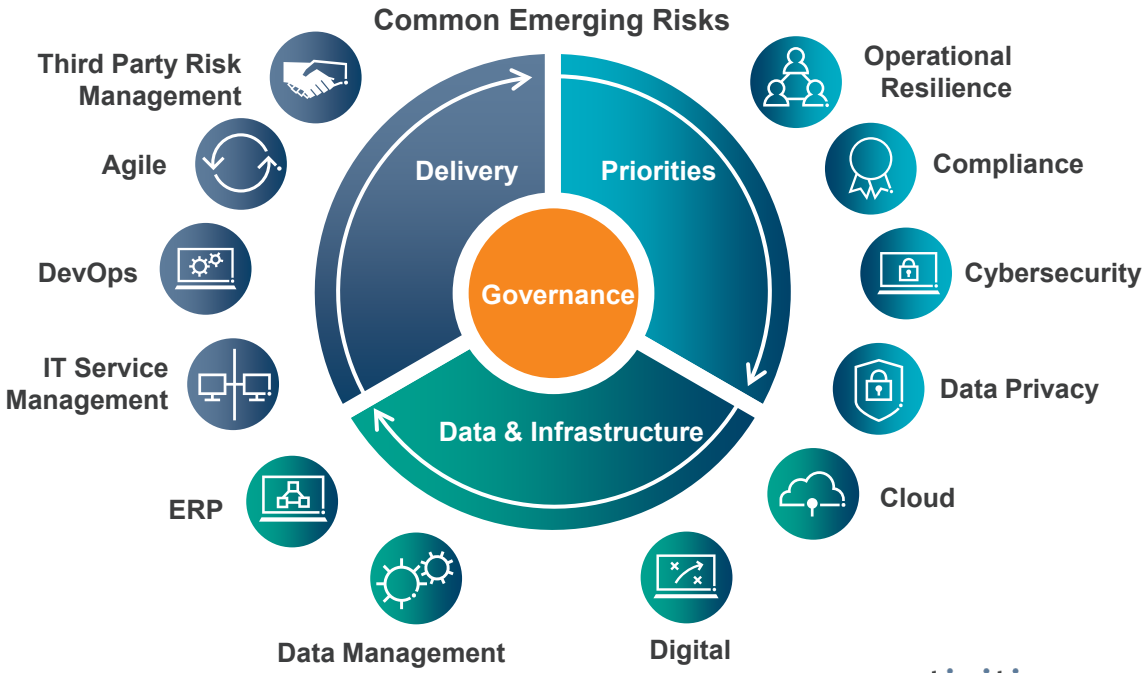
Are You Asking The Right Questions?

Before deciding on your Technology Audit Plan, consider asking yourself the following questions:

- Any technology / infrastructure modernization projects? System implementations?
- Has the impact of recent disruptions been fully evaluated?
- Is the IT Risk Assessment process performed frequently enough for the pace of change?
- Is there an understanding of insider threats and risks?
- Is RPA, Artificial Intelligence, Machine Learning, or other digital disrupters increasing?
- Is cloud adoption increasing? Are our cloud governance practices adequate?
- Are technology operations available during disruption events (resilience)?
- Are our interactions with (and reliance on) third parties sufficiently understood and governed?

Will IT Align With The Plan?

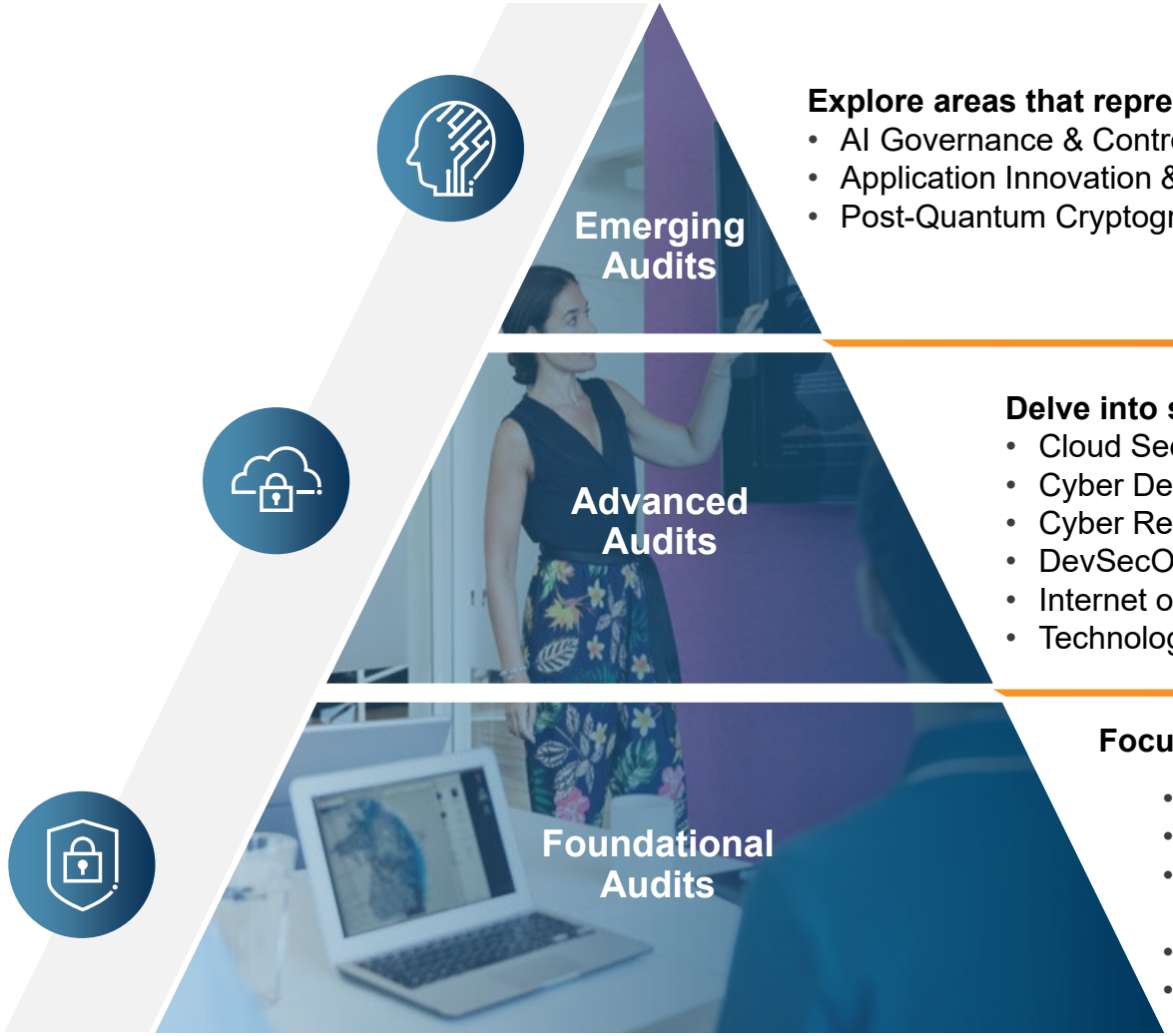
- ✓ Emerging Risk Identified
- ✓ Risk Rating Adjustments
- ✓ Mapping back to Audit Universe
- ✓ IT Organization Risk Alignment



protiviti

2023-2024 TRENDING TECH AUDITS

Protiviti identified 18 IT areas of focus with a prioritized breakdown working from the bottom tier to the top:



Explore areas that represent the future of technology

- AI Governance & Control
- Application Innovation & Modernization
- Post-Quantum Cryptography

Delve into specific technology areas that are maturing and rapidly evolving

- Cloud Security & Governance
- Cyber Defense Testing (penetration, red/blue/purple teaming, etc.)
- Cyber Response Preparedness
- DevSecOps
- Internet of Things “IoT”
- Technology Architecture

Focus on the core IT risk areas every organization needs to manage

- Cybersecurity Program
- Data Governance & Privacy
- Disaster Recovery and Business Continuity
- IT Asset Management
- IT Governance
- IT Service Management
- Patch & Vulnerability Management
- Penetration Testing
- Third-Party Risk Management

QUESTION #2

How would you assess the proficiency of your IT audit team at effectively evaluating the IT audit universe and emerging risks?

A. **Not at all proficient**
B. **Isolated proficiencies exist**
C. **Mostly proficient with only a few exceptions**
D. **Completely proficient**

QUESTION #3

What percentage of your Technology Audits are performed by third-party providers (Co-Sourcing)?

A. **0% – 25%**
B. **26% – 50%**
C. **51% – 75%**
D. **76% – 100%**

TECHNOLOGY AUDIT IN HIGHER ED – HOT TOPICS

What are the latest headlines to be aware of?

- Cyber Cyber Cyber!
    - Ransomware on the Rise – threat actors targeting “weak” higher education industry
        - 2022 and early 2023 reports from multiple sources site an increase in ransomware and other cyber attacks and that the industry overall is highly vulnerable
    - Cybersecurity Maturity Model Certification – Protection standard applicable for institutions working with confidential unclassified federal government data (primarily applicable to Research)
        - September Release Expected – when active, impacts institution's ability to perform certain research
- Crisis Management – reactive or proactive?
- Evolving Data Privacy Standards
    - Up to sixteen states with privacy laws and seven additional states that have introduced privacy bills
- Technical Debt & Talent Retention
- Artificial Intelligence – It’s here to stay, what do we need to do?

UNLOCKING THE ADVISOR ROLE

QUESTION #4

On average, what percentage of your Technology Audit plan is dedicated to Advisory engagements?

A. **0%**
B. **1% – 20%**
C. **21% – 40%**
D. **More than 40%**

A GOOD ADVISORY STARTING POINT

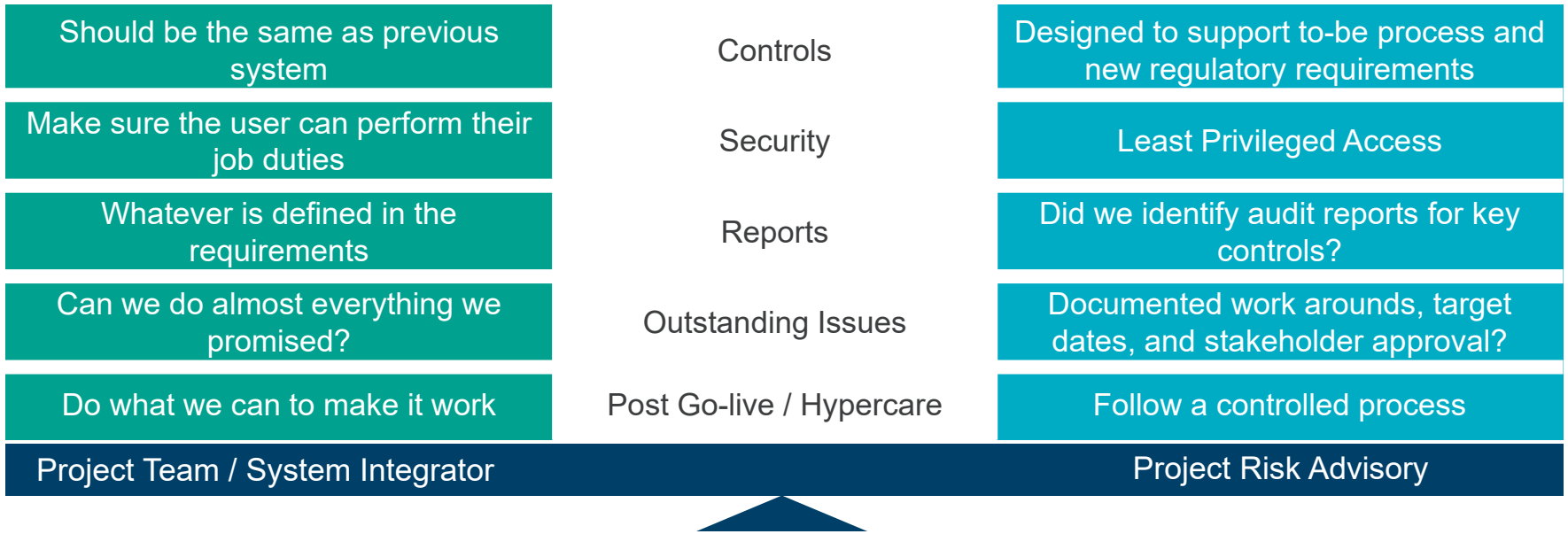
System implementations or development of strategic programs are great times to propose an advisory engagement

PROJECT RISK ADVISORY

The **Project Specialists** and / or **System Integrators** are very technical and understand all the business processes and configurations needed to make the application align with the initial requirements. They have one goal and that is to get a working version of the system implemented on-time and in budget.

The **Project Risk Advisory** team understands the risks to the organization not only from a compliance perspective, but also key risks associated with the different project phases. They have one goal and that is to make sure that all risks have been communicated and management understands the impact of any decision.

The goals and objectives of the Project Risk Advisory team do not always align with those of the project specialist and / or system implementer and it's critical that both messages are delivered to stakeholders so that management is able to make informed decisions.



THE AUDIT REPORT TRAP

But we always need a report to memorialize our findings, track formal action plans, and prepare for QARs, right?

Advisory Guidance within Methodology	Make sure your charter, policies, and procedures provide guidance on how advisory engagements should be carried out and the necessary audit artifacts to produce during the review. *Hint: Not Formal Reports*
Be Flexible	Scoping needs to be collaborative and flexible when approaching these engagements. Identify the highest risk areas and areas of highest concern with Management and tailor scope, budget, and approach accordingly.
When in Doubt, Memo	Audit methodology deviations, independence, and QAR concerns can be addressed with a memo to the audit file. Articulate how Internal Audit is engaged, what is (and is not) being performed and the results of the engagement.
Value Add Mindset	Leading Principle: How is what Internal Audit is doing driving value to business and IT teams?
Audit Committee	A comment from Management to the Audit Committee regarding the value Internal Audit provides is worth more than a good audit report

QUESTIONS?

Face the Future with Confidence

protiviti®