Deloitte.

Information technology internal audit high impact areas of focus
Institute of Internal Auditors (IIA) Atlanta chapter meeting

February 18, 2022

Today’s objective

To provide insights into what we are seeing as important information technology (IT) risks and high impact areas of focus for internal audit (IA) functions for delivering strategic and value-added services to their organizations.

The business opportunity and risk associated with technology continues to grow:

- IT risk continues to increase in importance to organizations
  - Corporate reliance on technology increases
  - Compliance requirements increase
  - Strategic value of technology as enablers of business strategy/change increases
- Deficiencies in IT controls can have a significant impact on the organization

The modern IT IA function should wear multiple hats to add strategic value

As a trusted business advisor, an IT IA function should go beyond controls and compliance by offering actionable insights to **build resilience** and **create measurable value**. By combining the "Three A's" – **Assure, Advise, and Anticipate**, IT IA's role can evolve in the organization and deliver more strategic value.

Assure

Confidence

IA continues to provide risk-based assurance on internal controls of the organization, and leverage tools and technology to do it better, faster, and more cost effective

Advise

Insight

IA is proactive, transparent, relevant, and valuable to the organization by advising on the ability to effectively manage risk broadly

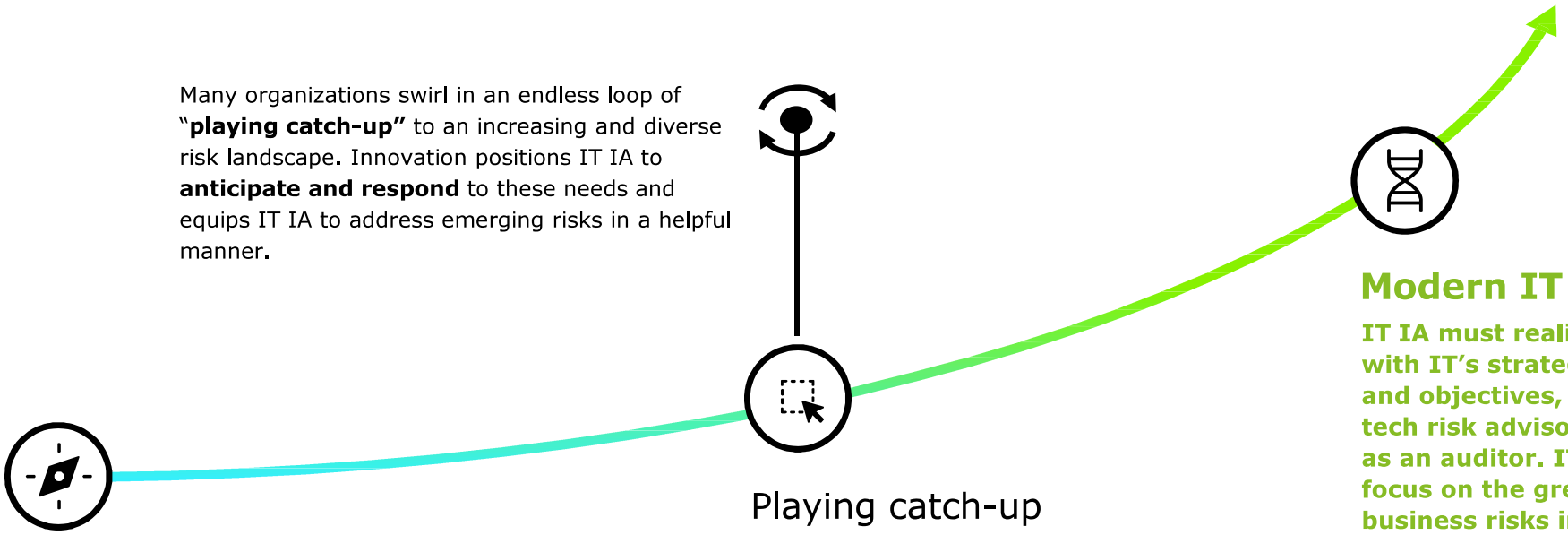
Anticipate

Foresight

IA anticipates and aligns efforts to emerging risks, strategies, and operational objectives of the organization

The evolution of IT IA is underway

As boards shift their attention to a broader set of technology risks and opportunities, IA is being **challenged** to do the same. This is an opportunity for IA to **add more value** and for audit committees and senior executives to **gain greater business and technology insights** from the IA organization



Many organizations swirl in an endless loop of "**playing catch-up"** to an increasing and diverse risk landscape. Innovation positions IT IA to **anticipate and respond** to these needs and equips IT IA to address emerging risks in a helpful manner.

Traditional IT IA

IT IA is a **supporting enabler** to the business strategy and focuses on auditing IT areas which outline omissions and vulnerabilities in various IT controls

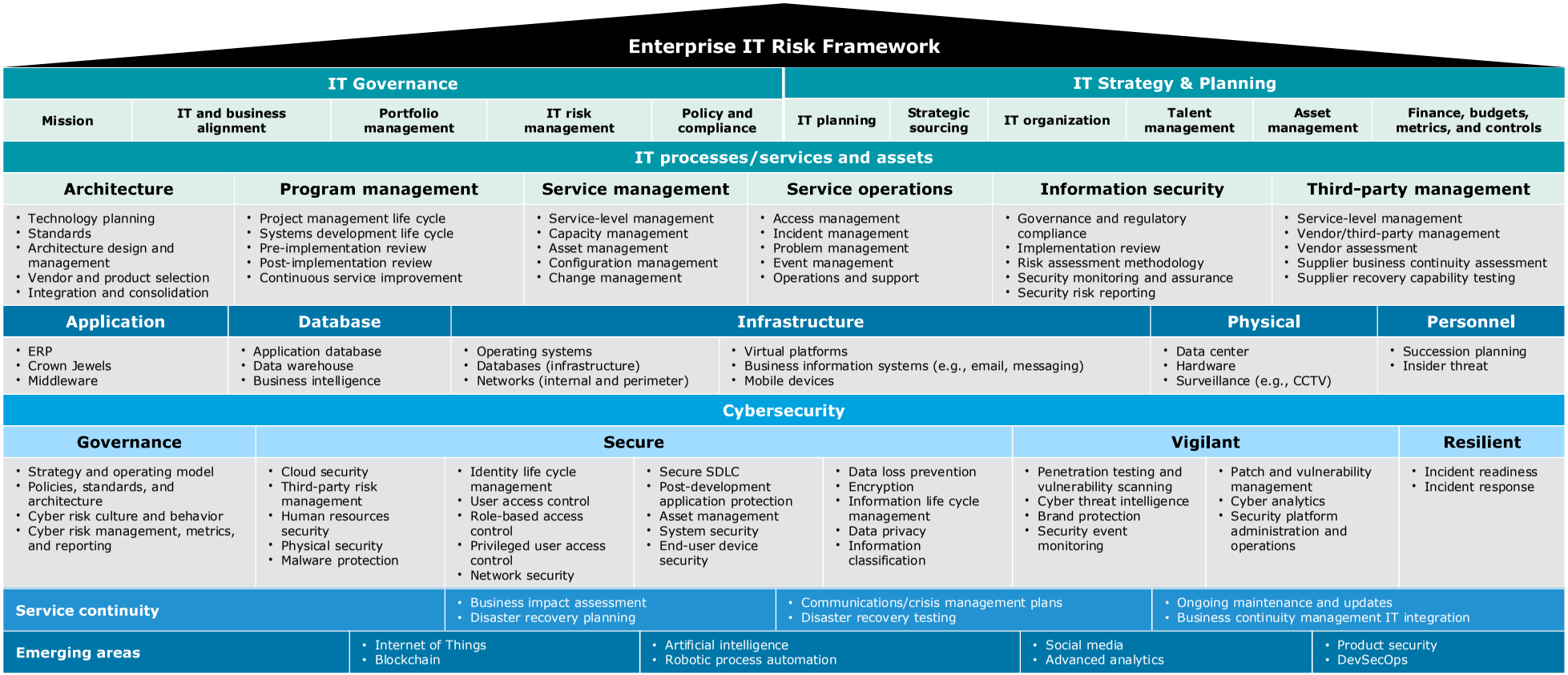
Playing catch-up

IT IA demands innovation to keep up with organizations and business environments changing faster than ever and in ways that are less predictable

Modern IT IA

IT IA must realign itself with IT's strategic role and objectives, acting as a tech risk advisor, not just as an auditor. IT IA must focus on the greatest business risks in strategic areas such as cloud, cyber, resiliency, etc.

A broad-based and end-to-end approach for assessing IT and cyber risk is needed



Deloitte's top 10 list of emerging and high impact risk areas for IT internal audit

DevSecOps risk & controls reliance

"Continuous everything" calls for a new approach to mitigating IT risks and will prompt auditors to rethink historic risks and controls for SOX and operational risks in a DevSecOps world.

Cloud governance & security optimization

A shared controls and governance model is critical for the rapid adoption of cloud-enabled models for both organizational IT needs and strategic delivery of services.

IT assurance by design during transformation

Investing time up front to design controls as part of a system implementation or transformation can save time and prevent the need for back-end remediation.

Digital risks of cognitive technologies

Robotic process automation (RPA) is gaining momentum for automating routine business tasks, but many companies have not thought through the increased security and privacy risks and increased cyber hack susceptibility.

Enterprise data privacy

Data management failures or breaches have drawn significant regulator and public scrutiny and resulted in increased pressure to improve data governance procedures and policies.

IT IA is focused on the greatest risks to the organization, the strategic board level issues, and the risk areas most impactful to company's business strategy.

Data risk, classification & protection

Many organizations struggle to successfully implement and enforce data governance frameworks, as they rely on new types of data and fragmented storage systems.

Cyber identity & access management

With the shift to a remote workforce, many IT departments are unable to keep up with increased need for access rights to support a remote workforce.

Cyber network & endpoint protection

Security of endpoints and networks with focus on the technology and current cybersecurity market trends presents an opportunity for IA to bridge the gap between the CISO and the CFO.

Enterprise business & technology resiliency

The scale of global and organizational change, compounded by shortcomings in business continuity management, is increasing organizations' exposure to risks of operational disruption.

Extended enterprise IT & cyber risk

As the extended enterprise becomes even more extended with the use of subcontractors and cloud, there needs to be a clear alignment on shared risk for cyber security and controls.

Polling question #1

Does your organization have a plan to address emerging IT risks?

a. Yes, we have a plan for all risks.

b. Yes, we have a plan for some risks.

c. Not yet.

d. Unsure/don’t know

Cloud governance and security optimization

Risks

- Shared risk responsibilities not always clear between clients and third-party providers
- Vendor governance becomes more critical as cloud risk increases

Questions to ask

- What is the organization's cloud roadmap?
- What is the brand and reputational risk due to security and privacy breaches?
- How is vendor governance approach evaluated?
- Who has shared risk responsibilities between clients and providers?
- What are the SLAs related to security and control?
- How are risk approaches altered around security, identification, data management, business resiliency, IT operations, etc.?

IA focus / actions

- Engage stakeholders on their cloud services and resulting risks profile
- Assess the organization's cloud governance, risk and controls framework

Polling question #2

Do you have cloud in your current audit plan?

a. Yes

b. No

c. N/A – We don’t have cloud systems

d. Unsure/don’t know

IT assurance by design during transformation

Risks

- Potential costly delays, defects, or breakdowns in the system of internal controls

Questions to ask

- Is control design part of a system implementation or transformation?
- What is the scope of significant control areas (e.g., system development lifecycle (SDLC), privacy, cyber)?
- Who has ownership and responsibility of governance vs. testing vs. advising in each control area (e.g., Internal Audit, SOX team, Compliance)?
- Is the testing environment reflective of the production environment?

IA focus / actions

- Get involved and be a risk advisor and partner during the pre-implementation planning phase
- Perform design review of automated controls/ITGC (IT General Controls) during implementations

Cyber identity and access management (IAM)

Risks

- Inappropriate access rights increases the risk of data breaches, financial losses and regulatory fines
- Risks related to implementation of IAM solution

Questions to ask

- Does the IAM solution automate certain specific General IT controls?
- What governance is in place for IAM solutions from an overall security perspective?
- Is centralized provisioning implemented by leveraging the IAM solution to reduce deficiencies related to access rights?
- Is Segregation of Duties conflicts related to access rights evaluated?

IA focus / actions

- Review access management policies and controls
- Deliver advice and recommendations related to IAM system implementations and transformations

Cyber network and endpoint protection

Risks

- Network security device deployment and configuration risks
- Operational risk due to reliance on IT infrastructure

Questions to ask

- Have you considered impact to brand and reputation if breaches or incidents occur?
- Are there sufficient controls in place prevent loss of critical or confidential data ?
- Increased regulatory fines or sanctions are likely to result
- Who is responsible for Privacy at your organization?

IA focus / actions

- Review IT security requirements and roadmap
- Perform an assessment of endpoint security, compliance monitoring, and specific configurations

Enterprise business and technology resiliency

Risks

- Remote working has increased security risks due to increased need for VPN, dual authentication, and other access
- Operational disruption and susceptibility of global supply chains

Questions to ask

- Does the organization have a business resiliency plan?
- What select technologies and systems support resilience in the organization?
- Does the organization have policies and procedures related to business continuity, crisis preparedness, response, and recovery capabilities
- Does the organization perform a post-crisis review to identify root cause, event impacts, and response effectiveness?

IA focus / actions

- Ensure that operational resilience is established
- Provide assurance and advisory services regarding crisis preparedness, response, and recovery capabilities

Extended enterprise IT and cyber risk

Risks

- Potential reputational damage and regulatory action due to increased reliance on third parties
- Financial impact due to failure of a third party or sub-contractor

Questions to ask

- What risks do the third parties pose?
- What has the organization—or the third party—done to address those risks?
- Does the third-party regularly check user privileges, and are these based on the principle of least privilege?
- Are they willing to enact cybersecurity requirements through a formal agreement?
- Do they have an incident response plan?

IA focus / actions

- Identify critical business activities, products and services
- Review third-party risk management programs with focus on IT security
- Develop or revalidate contingency plans for the higher risk third parties

DevSecOps risk and controls reliance

Risks

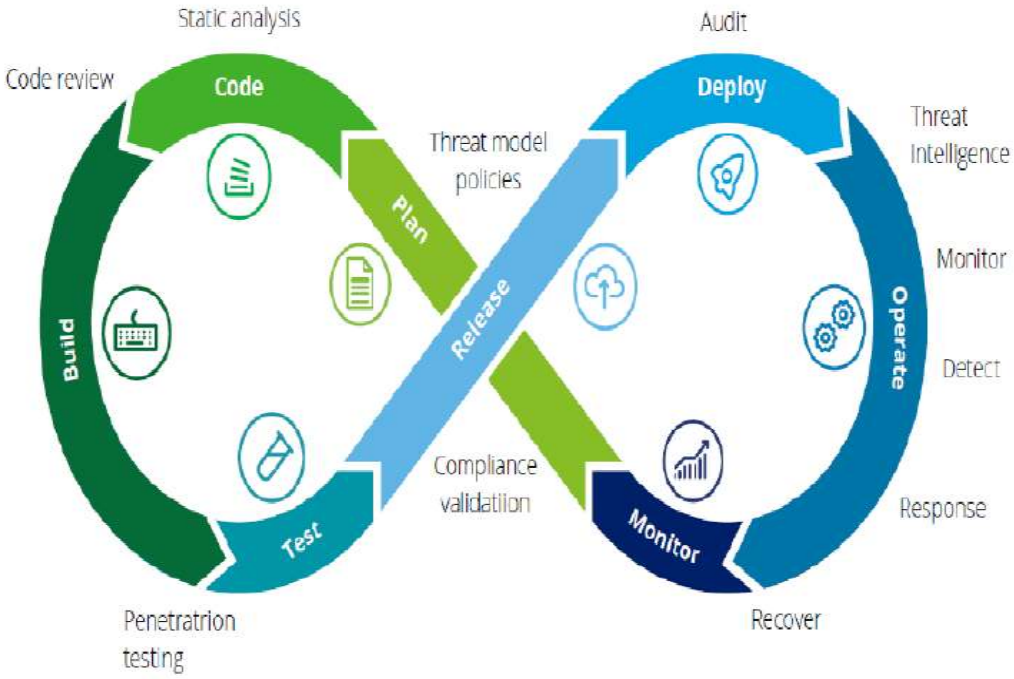
- Segregation of duties (SOD) conflicts harder to maintain
- Speed and frequency of changes/deployments much faster
- Greater reliance on automation and monitoring to gain assurance

Questions to ask

- What is the current state of the organization's DevSecOps rollout?
- Do SDLC policies/procedures address internal control requirements?
- Has IT assessed its controls framework for possible modifications?
- What application and security testing tools are being utilized?

IA focus / actions

- Shift in mindset related to IT change management risks
- Assess controls in process automation and monitoring including source data accuracy and completeness
- Understand end-to-end/continuous DevSecOps process and advise IT teams to redesign controls
- Develop strategy for Audit/Compliance integration into DevSecOps for high-risk changes vs traditional auditing



What can you do next?

- Determine which items may be relevant in your business and technical environment
- The risk assessment and audit universe should address relevant items
- Collaborate and communicate with IT, audit committee, and essential business stakeholders
- Plan for future IA resource skills and requirements
- Be careful not to underestimate the complexity and potential business impact involved
- Have frequent risk conversations with your stakeholders to get the discussion started and drive continuous risk assessment approach
- **Get creative with your IA plans combining a mix of assurance and advisory engagements to optimize IT IA's business value**

Contact information

Greg Boehmer
Senior Manager & US IT IA Leader
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
(212) 492-4269
gboehmer@deloitte.com

Deloitte.