protiviti®

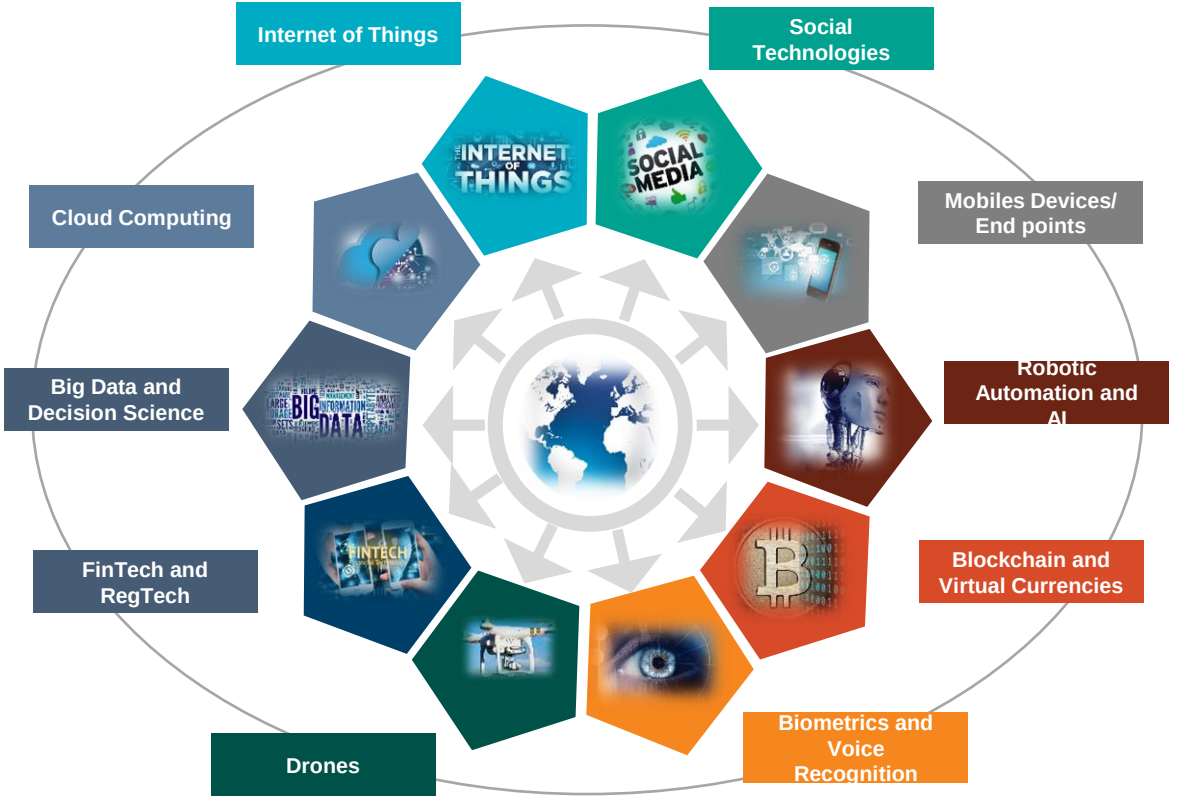
Face the Future with Confidence

CHANGING ROLE OF IA- IT AUDIT UNIVERSE & SKILLS FOR IT AUDIT

22 MAY, 2021

- Technology Landscape and Next Gen IA
- IT Audit Universe
- Cyber Audits and COVID 19 – A Reference Case
- Way forward

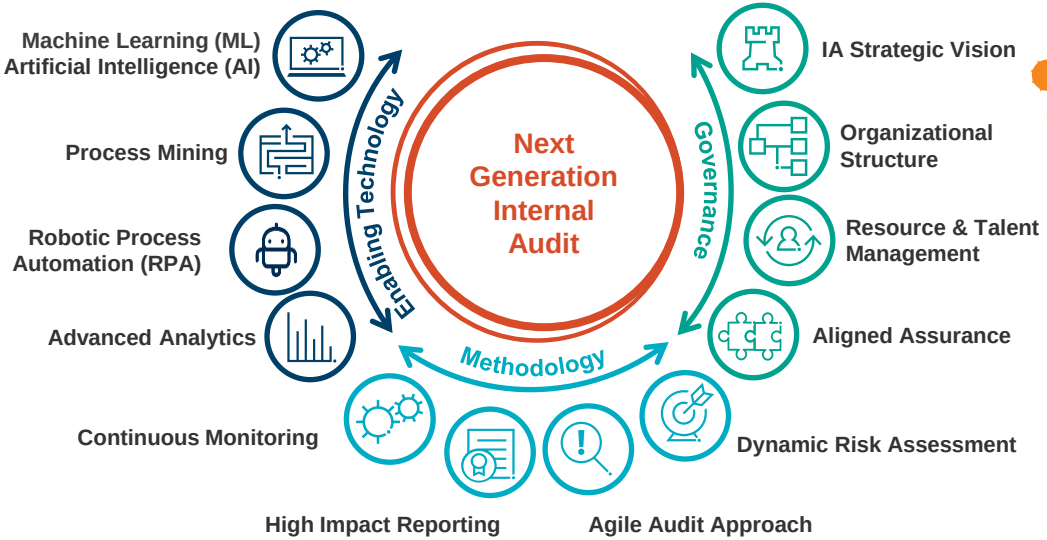
TECHNOLOGY DISRUPTION



As organizations strive to become more innovative, we (IA) must balance that with the need to manage various risks as well as data effectively, including but not limited to data quality, data governance and data protection

NEXT GENERATION INTERNAL AUDIT

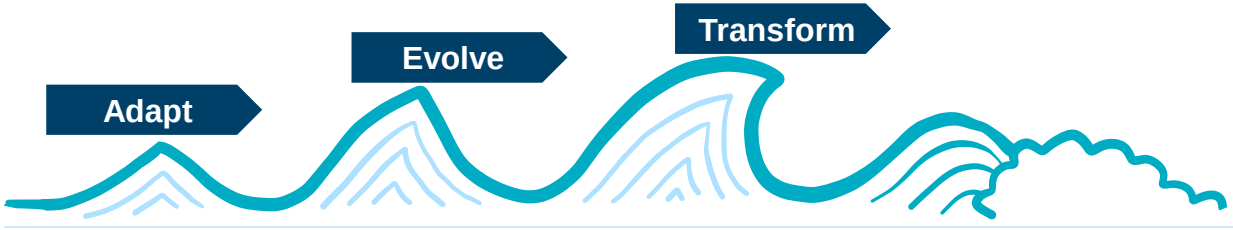
While “Next Gen” may sound like something that is far off, the reality is **every IA function should be examining their activities** (across governance, methodology, and enabling technology) **to ensure they are delivering risk assurance, advice, and insight in an efficient and effective manner**.



Three Essential Objectives

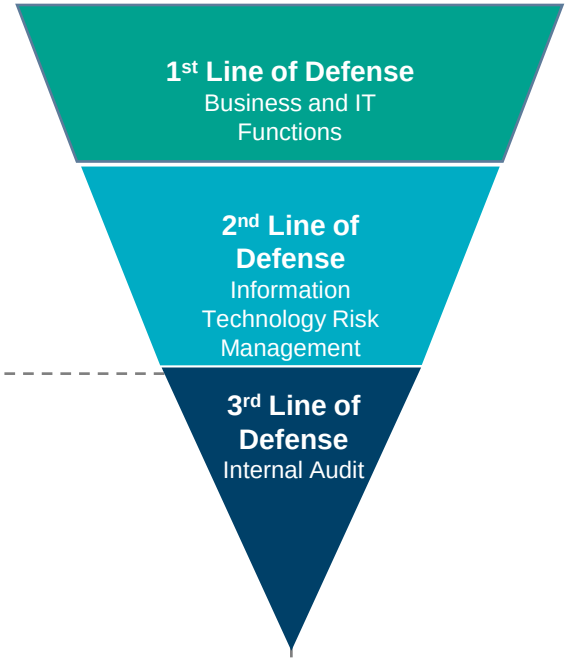
1. Improve assurance by increasing the focus on key risks
2. Make internal audit more efficient
3. Provide deeper and more valuable insights from internal audit’s activities and processes

EMBRACE NEXT GEN IA



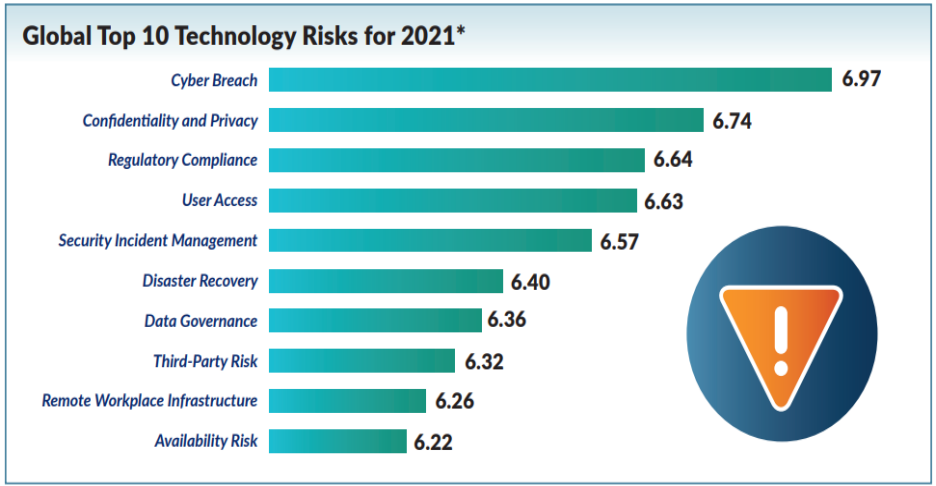
Key Questions to consider for Internal Audit Leaders in order to embrace Next Gen IA:

- Are you positioned to respond to changing key business risks associated with digital transformation initiatives?
- Are you able to leverage enterprise data efficiently to conduct risk assessments and continuous monitoring?
- Have you added resources and skill sets, to address increased expectations from internal and external stakeholders?
- Have you started to use technology to enhance the IA function along with relying on existing methodologies?
- Are you still relying primarily on point-in-time risk assessments?
- Are you still performing audits and reviews in the same way as in years past?

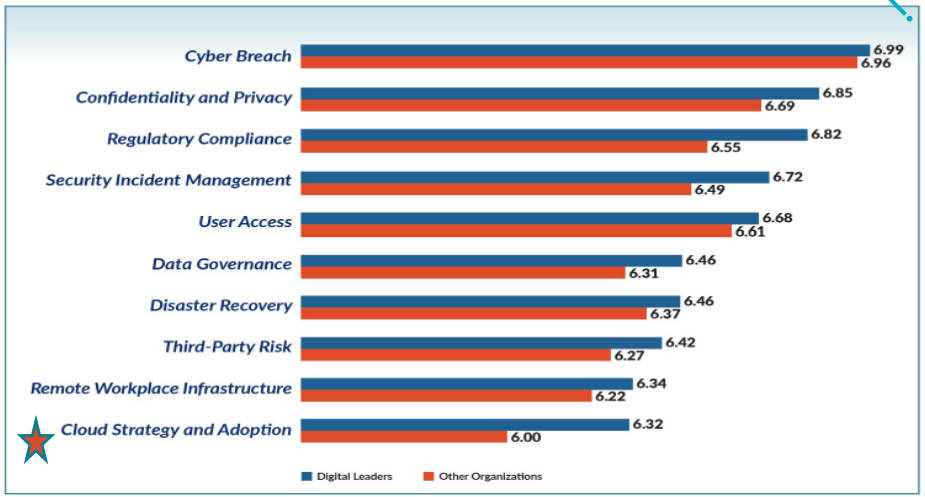


TECHNOLOGY AUDITS

TOP TECHNOLOGY RISKS 2021



IT Audit's Perspectives on the Top Technology Risks for 2021.



ISACA and Protiviti partnered to conduct the 9th Annual IT Audit Technology Risks Study in September 2020. More than 7,400 (n = 7,470) executives and professionals, including CAEs as well as IT audit vice presidents and directors, completed our online questionnaire. In the survey, respondents were asked to rate the significance of 39 technology risk issues on a scale of 1 to 10, based on their organization's technology risk assessment, with "1" representing low impact to the organization and "10" representing extensive impact to the organization.

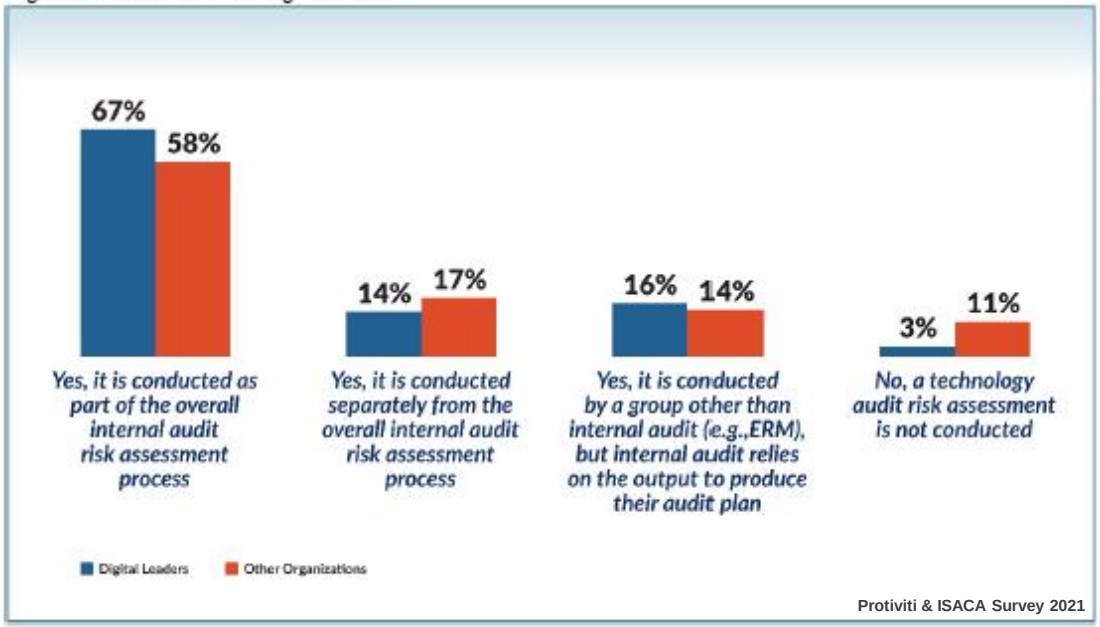
Protiviti & ISACA Survey 2021

IDENTIFY & ASSESS TECHNOLOGY RISK

	All respondents
Yes, it is conducted as part of the overall internal audit risk assessment process	61%
Yes, it is conducted separately from the overall internal audit risk assessment process	16%
Yes, it is conducted by a group other than internal audit (e.g., ERM), but internal audit relies on the output to produce their audit plan	15%
No, a technology audit risk assessment is not conducted	8%

Protiviti & ISACA Survey 2021

Digital Leaders vs. Other organisations

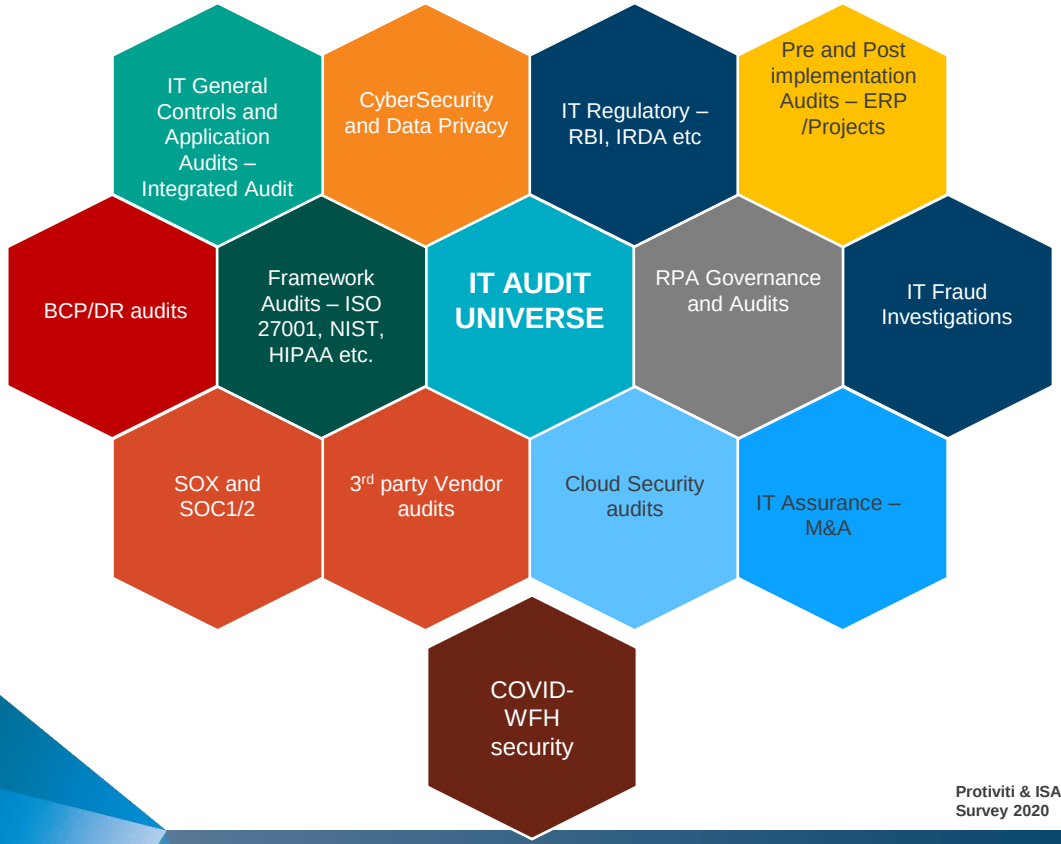


Protiviti & ISACA Survey 2021

No luxury of conducting high-level “check-the-box”

TECH AUDIT UNIVERSE

IT AUDIT UNIVERSE



	Africa	Asia	Europe	Latin America/ South America	Middle East	North America	Oceania
Conducting IT general control audits	82%	70%	81%	86%	69%	79%	78%
Conducting application audits	82%	67%	74%	85%	73%	72%	70%
Conducting IT process audits	73%	63%	76%	85%	80%	69%	78%
Conducting cybersecurity audits	65%	52%	69%	78%	73%	71%	65%
Conducting vulnerability assessments	46%	18%	22%	36%	29%	21%	20%
Supporting the organization's PCI compliance program	11%	11%	12%	14%	10%	19%	11%
Conducting penetration testing (including Red & Blue team activities)	26%	10%	15%	21%	20%	14%	15%
Conducting vendor audits (including third-party attestation reports)	30%	20%	30%	33%	15%	31%	20%
Testing for IT Sarbanes-Oxley or other related country-specific compliance	10%	11%	16%	18%	7%	45%	7%
Conducting IT assurance reviews as part of due diligence for mergers and acquisitions	33%	18%	15%	25%	15%	21%	20%
Conducting RPA audits	12%	5%	14%	7%	2%	18%	15%
Conducting social engineering audits	19%	6%	14%	11%	15%	13%	9%
Testing business continuity/disaster recovery plans	54%	27%	37%	55%	39%	46%	46%
Conducting pre- and post-implementation audits	52%	33%	41%	48%	46%	49%	43%
Conducting framework assessments (e.g., against COBIT, NIST, ISO, etc.)	47%	30%	45%	62%	44%	46%	46%
Conducting reviews of third-party cloud services via the use of the Cloud Security Alliance (CSA) framework	19%	9%	16%	16%	5%	21%	4%

Protiviti & ISACA Survey 2020

NEED FOR CYBERSECURITY AUDITS

Cybersecurity is included in the audit plan

What cyber-related audit activities have been performed? (Multiple responses permitted)

	Leaders	Non-Leaders
Security program assessment/framework gap analysis	73%	67%
Privileged access management	64%	63%
Technical assessments (vulnerability assessment, penetration testing, "red team")	52%	49%
Data loss prevention (identification of "crown jewels")	51%	44%
Security incident response — simulation/tabletop	48%	38%
Social engineering	35%	25%
Cyber breach kill chain	16%	11%

How are cybersecurity audits typically resourced? (Multiple responses permitted)

	Leaders	Non-Leaders
Exclusively with in-house (IT audit) resources	46%	47%
In-house resources with support from technical IT/information security resources	41%	31%
Co-sourced using external SMEs	32%	27%
Outsourced	16%	15%

KEY FACT

Among organizations that are not addressing cybersecurity as part of audit activities, the percentage of those that cite a lack of qualified/available resources (people or tools) as the primary reason

- Cybersecurity audits are gaining prominence across the globe.
- More than 50% of the organizations have either engaged with a third party for co-sourcing agreements for SME support or have completely outsourced such audits due to lack of qualified resources.

Protiviti & ISACA Survey 2020

MAJOR CYBERSECURITY FRAMEWORKS USED

Which of the following frameworks does the audit function use in performing assessments of the organization's cybersecurity posture/maturity? (Multiple responses permitted)

NIST Cybersecurity Framework	54%
COBIT	51%
ISO 27000	43%
NIST 800-53	20%
CIS Top 20	12%
FFIEC Cybersecurity Assessment Tool	10%
AICPA Trust Service Criteria	7%

Protiviti & ISACA Survey 2020

Framework Definitions

- **COBIT**: Created by ISACA for information technology management and IT governance.
- **ITIL**: A set of detailed practices for IT service management that focuses on aligning IT services with the needs of business.
- **COSO Internal Controls – Integrated Framework**: Provides principles-based guidance for designing and implementing effective internal controls.
- **FFIEC Cybersecurity Assessment Tool**: Helps financial institutions identify their risks and determine their cybersecurity preparedness.
- **NIST Cybersecurity Framework**: Helps organisations to better understand and improve their management of cybersecurity risk.
- **ISO 27000 Series**: Information security standards published jointly by the International Organization of Standardization (ISO) and the International Electrotechnical Commission (IEC).
- **CIS Critical Security Controls**: Prioritised set of actions to protect the organisation and data from known cyber attack vectors.
- **CSA Cloud Controls Matrix**: Cybersecurity control framework for cloud computing.
- **FAIR Cyber Risk Framework**: Provides information risk, cybersecurity and business executives with standards and best practices to measure, manage and report on information risk from the business perspective.

A PENETRATION TEST IS NOT ENOUGH !!!!

Internal audit plans frequently include a penetration test, and only a penetration test, as a cybersecurity-related audit. The increased risk environment necessitates that internal audit look beyond penetration tests and increase the number of cybersecurity audits.

Limits of Penetration Testing

A penetration test does not always provide an accurate or comprehensive assessment of cybersecurity risk. The goal of a penetration test is to simulate a single attack, not to uncover all possible attack scenarios. It is also usually very time-constrained, lasting weeks instead of the months that actual attackers have.

Internal audit departments need to rebalance their plans to cover more cybersecurity areas.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identity	ID AM	Asset management
		ID BE	Business Environment
		ID GV	Governance
		ID RA	Risk Assessment
		ID RM	Risk Management Strategy
PR	Protect	PR AC	Access Control
		PR AT	Awareness & Training
		PR DS	Data Security
		PR IP	Information Protection Processes & Procedures
		PR MA	Maintenance
		PR PT	Protective Technology
DE	Detect	DE AE	Anomalies & Events
		DE CM	Security Continuous Monitoring
		DE DP	Detection Processes
RS	Respond	RS RP	Response Planning
		RS CO	Communications
		RS AN	Analysis
		RS MI	Mitigation
		RS IM	Improvements
RC	Recover	RC RP	Recovery Planning
		RC IM	Improvements
		RC CO	Communications

SELECTING THE RIGHT SECURITY AUDITS

An internal audit plan focused on cyber risk should be based on the organization's risk profile and the external threat landscape. Security audits are generally categorized into four areas (as described below), and then specific projects can be selected based on the corresponding maturity level.

Technical Attack Assessments

Traditional and emerging attack vectors an attacker may use to access your network and information

Program/Governance

Understanding and assessing the overall security posture of the environment

Breach Detection & Response

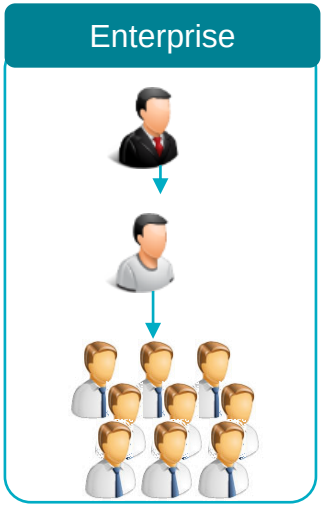
Assessing an organization's ability to identify and properly response to a security incident

Applications & Infrastructure

Focused assessments to identify and evaluate risks associated with applications, supporting infrastructure, and emerging technology such as Cloud and IoT

COVID-19: IMPACTING BUSINESS…

Enterprise



- Work from home
- Remote access & operations
- Heavy online transacting
- Virtualized meetings
- Online collaborations

Business Ecosystems

Theme of COVID-19 for Business
NEW RULES OF ENGAGEMENT IN THE JUNGLE ……

CYBER SECURITY – COVID NORM

Some CXO's are now driving strategic questions that will take enterprises to a new model of operation…..

New Normal ?

Do businesses need **physical office space?**

Why cant organizations cut cost & move to a "Bring Your Own Device" (**BYOD**) Model ?

New ways to deliver ?

Can we just transact O2C, P2P cycles electronically **using RPA** without / with minimal human intervention

New ways to host & access ?

Why not virtualize, provide **remote connectivity & Mobility based applications ?**

Why cant we just **put everything on the cloud** and do away with physical infrastructure?

3 Stage Cyber Defense Audit Scope for COVID-19

(Different organizations will be on different paths to managing their COVID-19 challenges, hence varied internal control environments and audit themes)

1 **Audit Theme :** Review current state of cyber defense

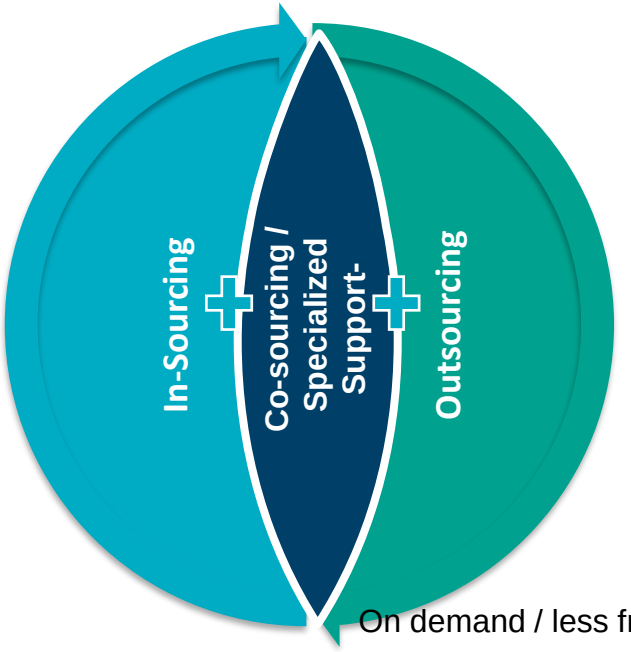
2 **Audit Theme :** Review Defense posture upon resumption

3 **Audit Theme :** Review defense strategy for the new normal

TECHNOLOGY AUDITS – DELIVERY MODEL !!

- ✓ IT Internal auditors are in demand as the need for IT Audit increases.
- ✓ IT Internal Auditor is someone that understands Business and Technology and provide meaningful support to business in achieving the goals and mitigating risk

- Largely focused on traditional audits and business focused
- Focused towards mandated audit program
- Learning curve and maturity of the IA function



- Head count limitations – Full / Partial
- Skill set Limitations
- Cost Limitations
- On demand / less frequent audits

Having a Right Balanced team structure is an Ideal combination

WHAT NEXT?

ACCELERATING IT AUDIT SKILLS

A combination of elements need to be looked upon to drive - “Successful Technology Audit program”

- Shift Focus on Risk Assessment
- Develop Knowledge Management
- Benchmarks and Surveys
- Effective Partnership- IT Org and Management
- Skills/Capability Assessment
- Involve more on Advisory support
- Training and Mentoring – HR/L&E
- Cross functional Training – BU’s
- Partnering Opportunities- Vendors
- Adopting Tools and Technology- Enablers

TECHNOLOGY RELATED CERTIFICATIONS

Face the Future with Confidence

https://www.linkedin.com/in/vijaik/
Vijai.k@protivitiglobal.in

protiviti®