PEMPAL

Internal Audit Community of Practice (IACOP)

IT AUDIT: From Theory to Practice

WEBINAR

IT Audit Resources and Planning

Professor Frank Yam

Chairman & CEO – Focus Strategic Group Inc

November 23, 2020

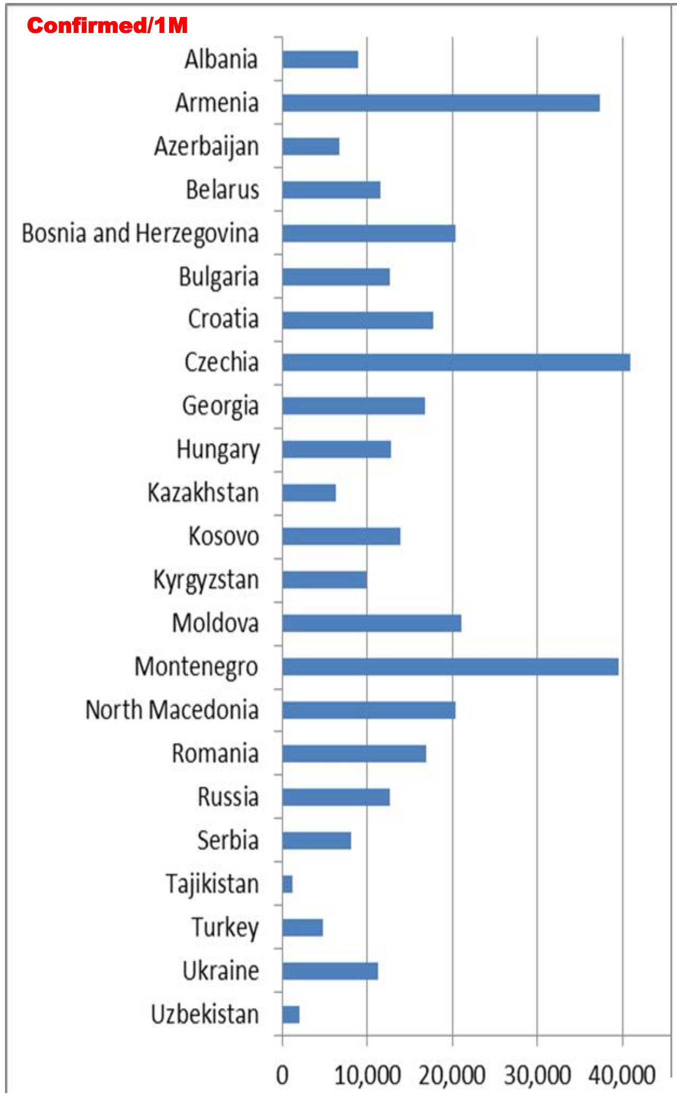
Content

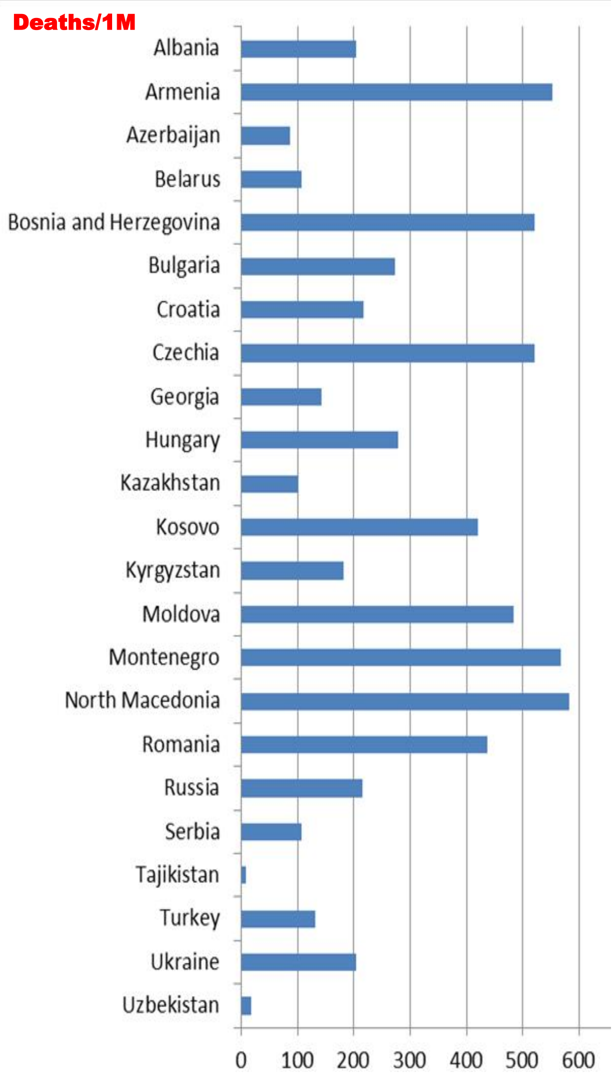
- □ **Embracing the New Normal**
  - □ COVID-19
  - □ Impact to Internal Audit Functions
  - □ Everything Digified
- □ **IT Audit Resources**
- □ **IT Audit Planning**

THE NEW NORMAL

Post COVID-19

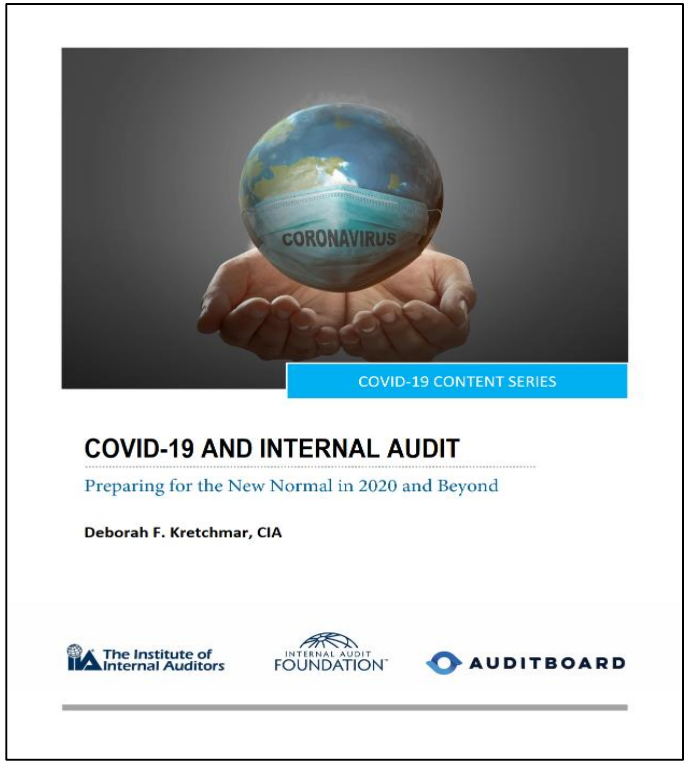
Country	Population	Confirmed/1M	Deaths/1M
Albania	2,876,641	8,969	205
Armenia	2,965,275	37,281	552
Azerbaijan	10,172,439	6,743	87
Belarus	9,448,180	11,574	108
Bosnia and Herzegovina	3,273,270	20,336	520
Bulgaria	6,929,071	12,601	274
Croatia	4,095,903	17,784	218
Czechia	10,716,269	40,948	520
Georgia	3,986,347	16,697	142
Hungary	9,651,311	12,730	279
Kazakhstan	18,858,176	6,283	101
Kosovo	1,810,366	13,934	421
Kyrgyzstan	6,563,032	9,806	181
Moldova	4,030,509	21,016	484
Montenegro	628,095	39,588	567
North Macedonia	2,083,343	20,419	582
Romania	19,190,198	16,889	437
Russia	145,957,452	12,586	216
Serbia	8,724,381	8,072	107
Tajikistan	9,614,381	1,192	9
Turkey	84,668,717	4,749	132
Ukraine	43,636,591	11,225	205
Uzbekistan	33,644,633	2,061	18
AVERAGE	19,283,677	15,369	277





THE NEW NORMAL

COVID-19’s Impact to Internal Audit Functions



COVID-19 CONTENT SERIES

COVID-19 AND INTERNAL AUDIT

Preparing for the New Normal in 2020 and Beyond

Deborah F. Kretchmar, CIA

The Institute of Internal Auditors

INTERNAL AUDIT FOUNDATION

AUDITBOARD

Top concerns, but under-represented in annual audit plans:

1) Cybersecurity
   - Organizations have allowed staff to work from anywhere, placing reliance on processes and controls over cyber risks that may not be adequately assessed.

2) Information Technology
   - Almost 60% have added new technology and data security

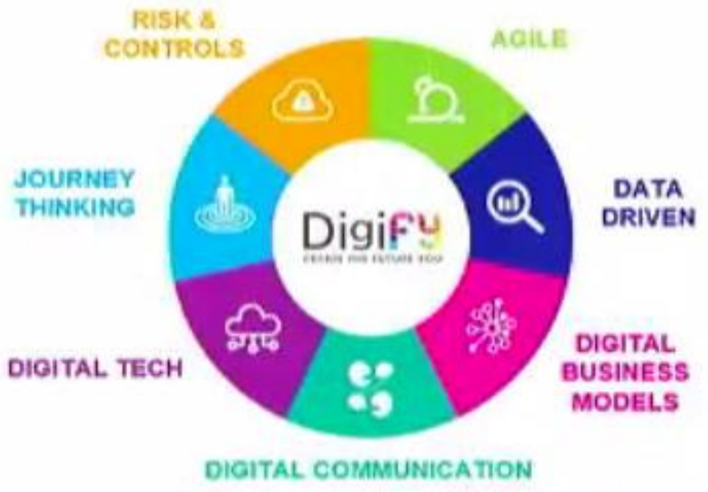
3) Third-party Relationships
   - Less than half (48%) have devoted IA resources to cover third-party relationships

BUT IT IS NOT JUST ABOUT COVID-19

THE NEW NORMAL
Everything Digified

For Organisations:

- □ Staff work from anywhere
- □ Flexible working hours
- □ Staggering Schedules
- □ Provide PPE to staff (and even customers & guests)
- □ Priority on (1) Keeping everyone safe, and (2) CEM and BCP
- □ New strategies and initiatives (including technology-related)
- □ Potential layoffs



For Internal Auditors:

- □ Remote Auditing (teleconferencing, screen sharing, video conferencing, file sharing)
- □ Change in skills required as a result of digital transformation
- □ Unemployment and economic downturn will increase fraud risks (hence, audit focus needs to change)

IT Audit Resources

Who should we be looking for?

ETHICAL
PROBLEM SOLVER
NEGOTIATOR
VALUER
ECONOMIST

AUDITOR QUALITIES
WATCHDOG
PROFESSIONALLY SCEPTICAL
BOOKKEEPER
INDEPENDENT
ANALYTICAL THINKER
MATHEMATICIAN

COMPUTATIONAL THINKER
IT LITERATE
DATA ANALYST
CONTROLS EXPERT
BIG DATA
BIG DATA

The KEY to success = building teams that can thrive in a future that can't be predicted

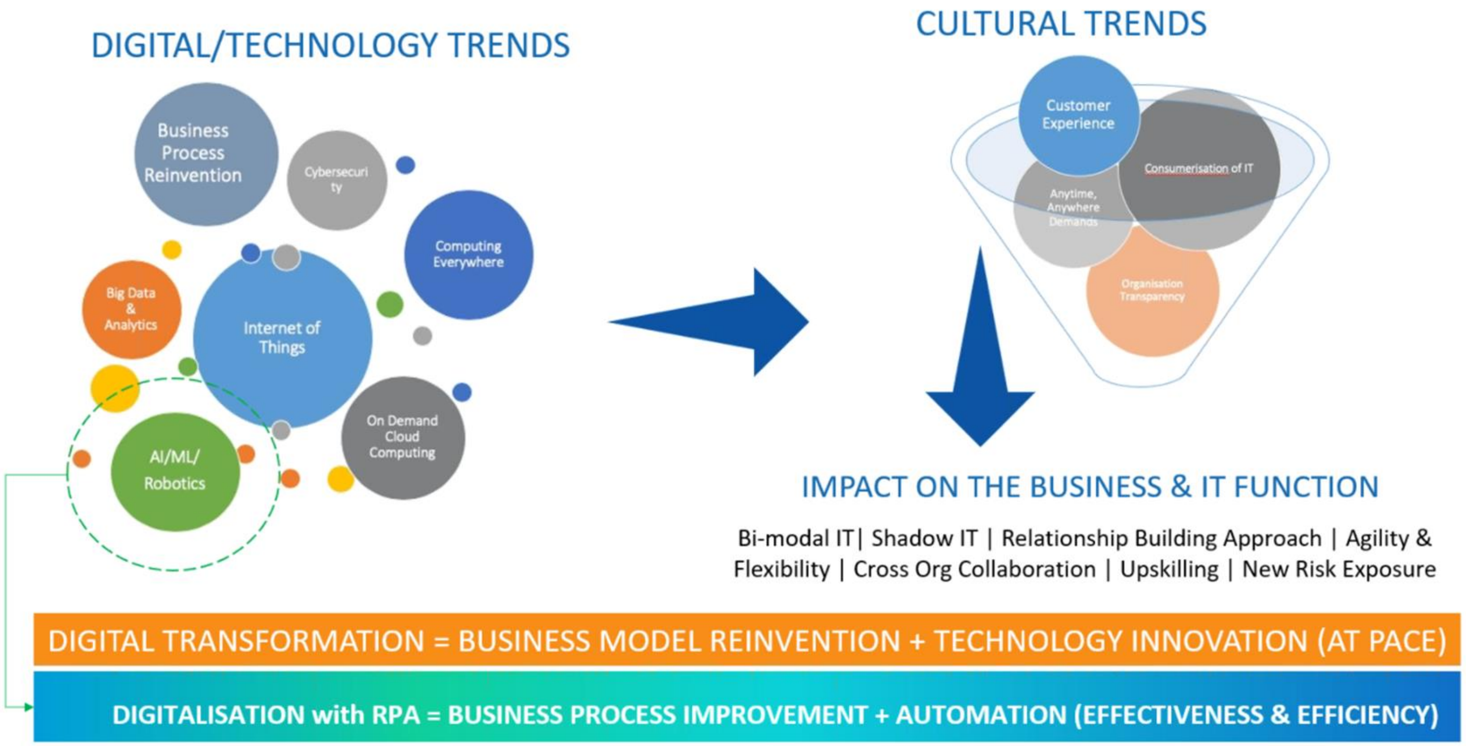
So Keep Empowering Yourself !

Source: Video "What skills will an Auditor in the Future need?" (CA - A/NZ)

IT Audit Resources

Who should we be looking for?

- □ AI
- □ Machine Learning
- □ Big Data
- □ RPA
- □ Blockchain
- □ DevSecOps
- □ Agile / SCRUM
- □ Digital Transformation
- □ Ecosystem
- □ UI / UX
- □ Design Thinking
- □ Cloud computing
- □ SaaS, IaaS, PaaS
- □ VPN
- □ API
- □ SDK
- □ Quantum Computing
- □ Nanotechnology
- □ Disruptive Technologies
- □ SOC



DIGITAL/TECHNOLOGY TRENDS

CULTURAL TRENDS

IMPACT ON THE BUSINESS & IT FUNCTION

Bi-modal IT| Shadow IT | Relationship Building Approach | Agility & Flexibility | Cross Org Collaboration | Upskilling | New Risk Exposure

DIGITAL TRANSFORMATION = BUSINESS MODEL REINVENTION + TECHNOLOGY INNOVATION (AT PACE)

DIGITALISATION with RPA = BUSINESS PROCESS IMPROVEMENT + AUTOMATION (EFFECTIVENESS & EFFICIENCY)

Someone who can understand the Business and IT Alignment Challenges

- □ Zoom
- □ Webex (Cisco)
- □ Teams (MS)
- □ Meet (Google)
- □ KOL
- □ IoT
- □ VR / AR
- □ 5G
- □ FinTech, RegTech, EdTech, HealthTech
- □ Cryptocurrency
- □ e-Wallets
- □ e-Payments
- □ QR codes
- □ Drones
- □ Chatbots
- □ 3D printing
- □ Wearables
- □ Gig economy
- □ Smart City / Government
- □ Millennial

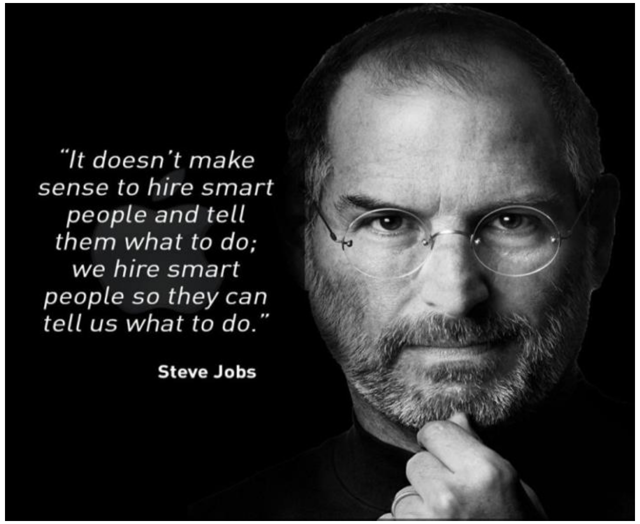
IT Audit Resources

Who?

- □ **In-house Auditors**
  - □ Urgent need to up-skill and re-skill
  - □ Consider Secondments
  - □ Sharing Best Practices

- □ **Collaboration**
  - □ Compliance
  - □ Internal Control
  - □ Risk Management
  - □ Security
  - □ Privacy
  - □ Fraud Investigation
  - □ External Audit

- □ **Co-Sourcing**
  - □ Technical Areas
  - □ Periodic, As Needed
  - □ Knowledge Transfer

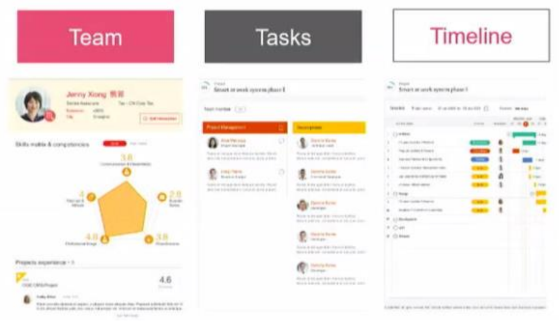


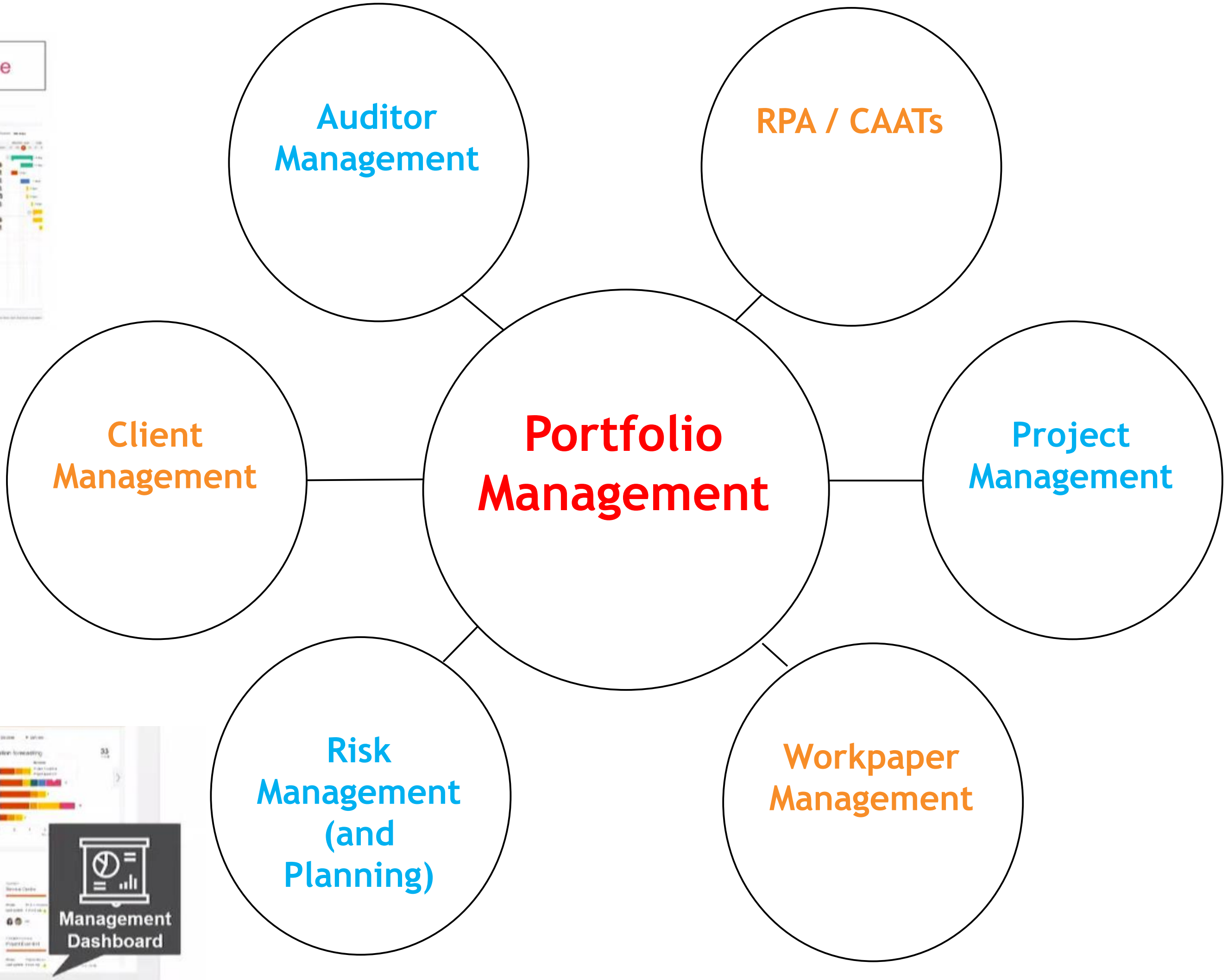
"It doesn't make sense to hire smart people and tell them what to do; we hire smart people so they can tell us what to do."

Steve Jobs

IT Audit Resources

How?




Portfolio Management

Auditor Management

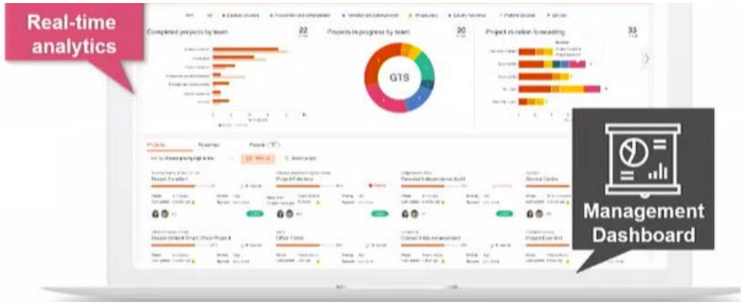
RPA / CAATs

Client Management

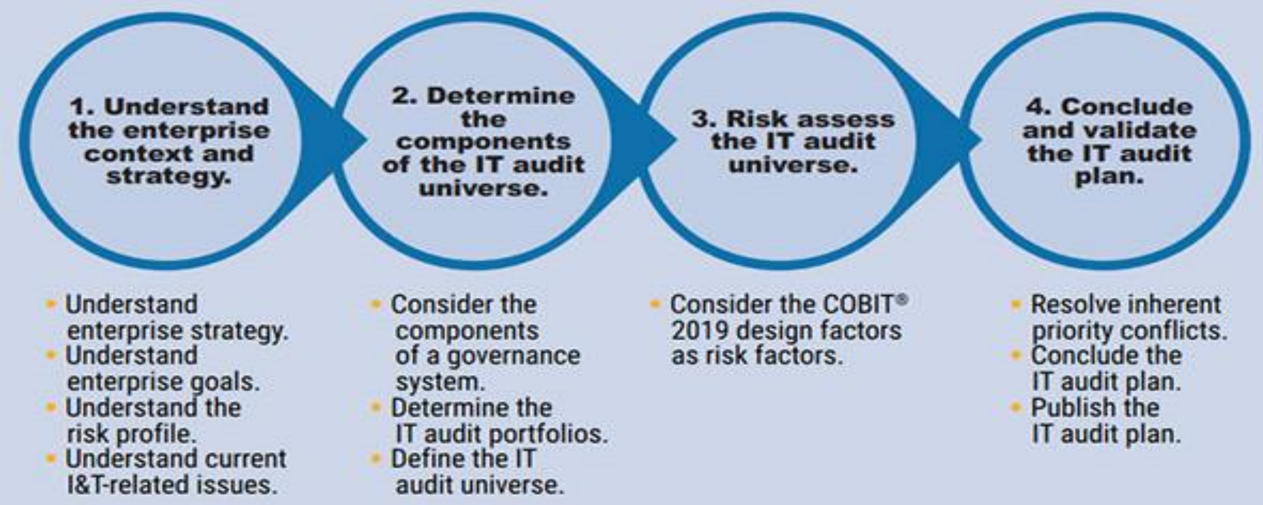
Project Management

Risk Management (and Planning)

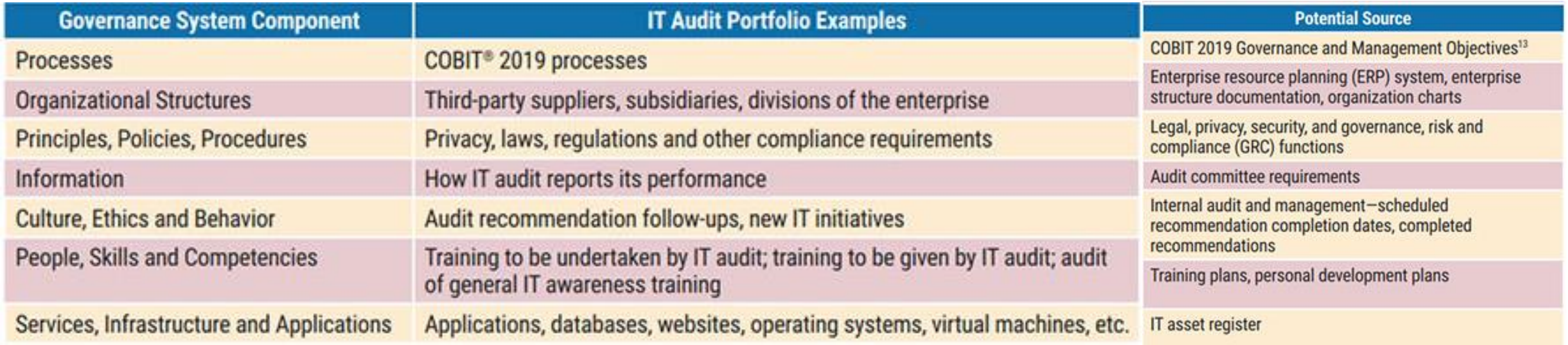
Workpaper Management



IT Audit Planning


1. Understand the enterprise context and strategy.
2. Determine the components of the IT audit universe.
3. Risk assess the IT audit universe.
4. Conclude and validate the IT audit plan.

1. Understand the enterprise context and strategy.
   - Understand enterprise strategy.
   - Understand enterprise goals.
   - Understand the risk profile.
   - Understand current I&T-related issues.
2. Determine the components of the IT audit universe.
   - Consider the components of a governance system.
   - Determine the IT audit portfolios.
   - Define the IT audit universe.
3. Risk assess the IT audit universe.
   - Consider the COBIT® 2019 design factors as risk factors.
4. Conclude and validate the IT audit plan.
   - Resolve inherent priority conflicts.
   - Conclude the IT audit plan.
   - Publish the IT audit plan.



Governance System Component	IT Audit Portfolio Examples	Potential Source
Processes	COBIT® 2019 processes	COBIT 2019 Governance and Management Objectives[13]
Organizational Structures	Third-party suppliers, subsidiaries, divisions of the enterprise	Enterprise resource planning (ERP) system, enterprise structure documentation, organization charts
Principles, Policies, Procedures	Privacy, laws, regulations and other compliance requirements	Legal, privacy, security, and governance, risk and compliance (GRC) functions
Information	How IT audit reports its performance	Audit committee requirements
Culture, Ethics and Behavior	Audit recommendation follow-ups, new IT initiatives	Internal audit and management—scheduled recommendation completion dates, completed recommendations
People, Skills and Competencies	Training to be undertaken by IT audit; training to be given by IT audit; audit of general IT awareness training	Training plans, personal development plans
Services, Infrastructure and Applications	Applications, databases, websites, operating systems, virtual machines, etc.	IT asset register

Source: ISACA Journal – 2019 May 1 – "Developing the IT Audit Plan Using COBIT 2019"

IT Audit Planning

Annual Planning

- Consider adopting an **Agile Portfolio Management** approach
  - Embrace short-term prioritisation
  - Regular review/updates to the audit plan (to mirror the changing pace of risk and assurance needs)
- Allow for **increased flexibility** in the audit plan:
  - Try to assist in **new projects / initiatives**
  - This is the best time to build rapport, and to demonstrate IA’s value
- **Collaborate with key stakeholders** (including the AC) to understand any new and/or elevated risks, and to assess how best to support with the provision of assurance
- Increasing the number of progress meetings held with key stakeholders across the business. Where possible use video calls to **build rapport and establish trust**.

IT Audit Planning

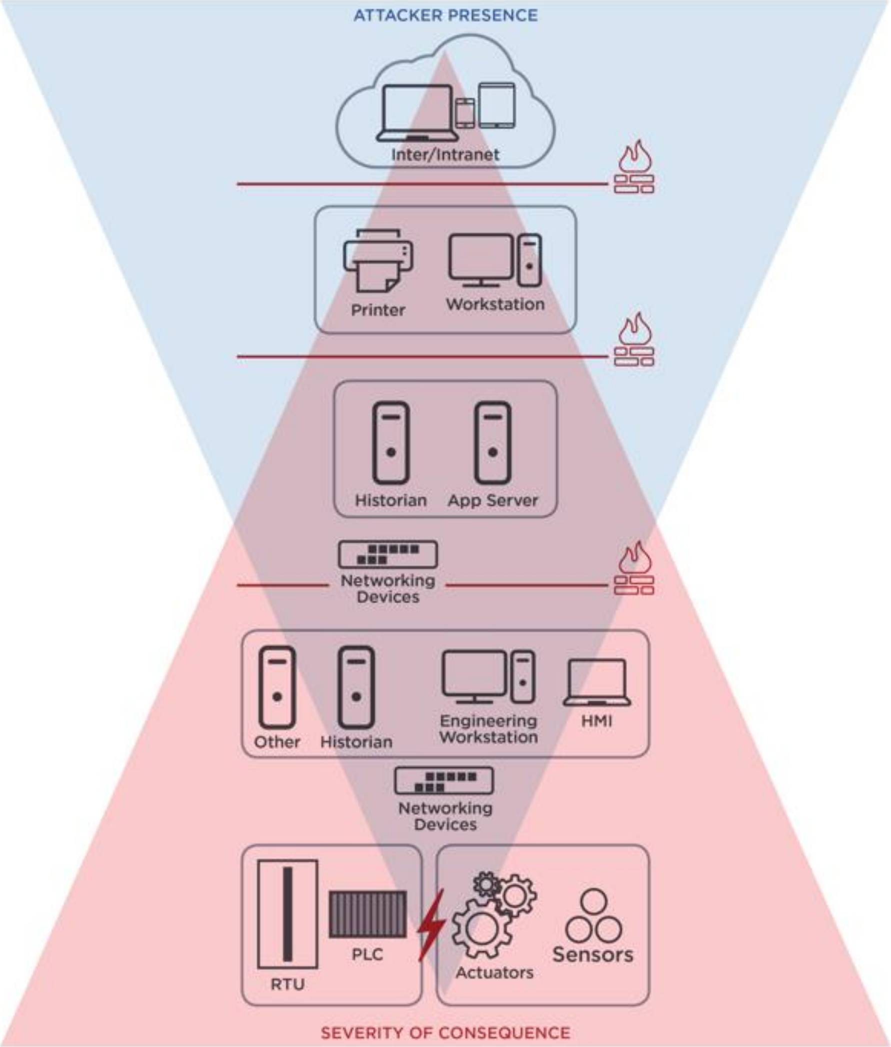
Annual Planning – Suggested Focus Areas

(1) Cybersecurity (Ransomware, Cyber Extortion)

- □ User Access Controls
- □ Data backup and recovery
- □ Regulatory Requirements on Data Privacy (GDPR, etc)

Ransomware - prevents you from accessing your data

Cyber Extortion - A threat to make your data public to others



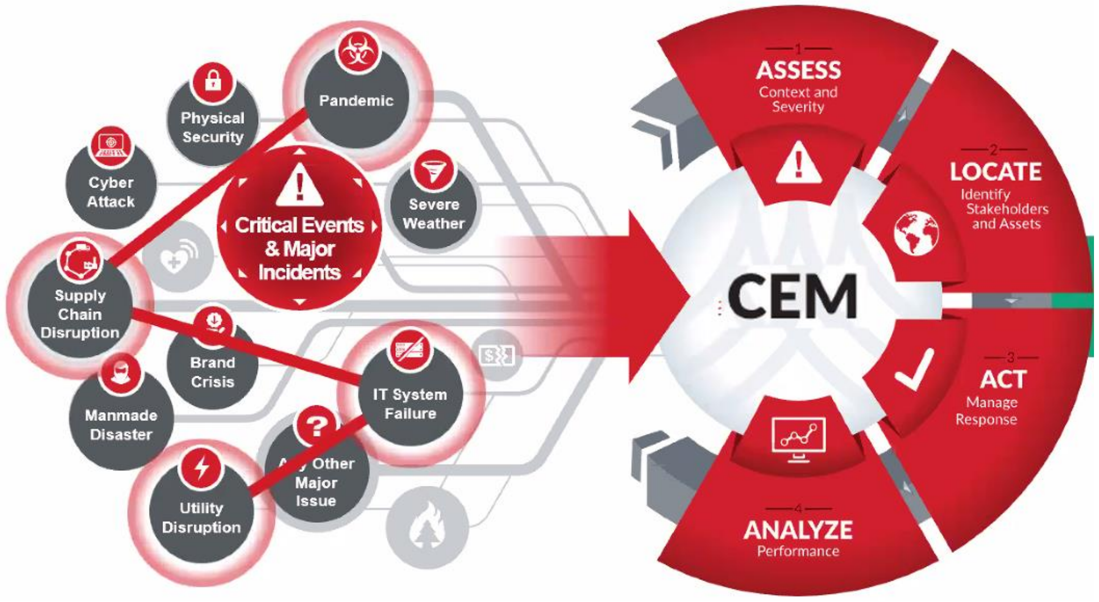
IT Audit Planning

Annual Planning – Suggested Focus Areas

(2) Business Continuity

- □ Disaster recovery (CEM)
- □ Segregation of critical teams (in case of quarantines)
- □ Reviewing digital capabilities from transactions to customer interactions
- □ Re-visit BIA and “worst case scenarios”
- □ Media Management Plans

Patient died after a Ransomware Attack hits a German hospital



(3) Review IT processes that are NOT governed by IT

(4) Review existing policies, guidelines

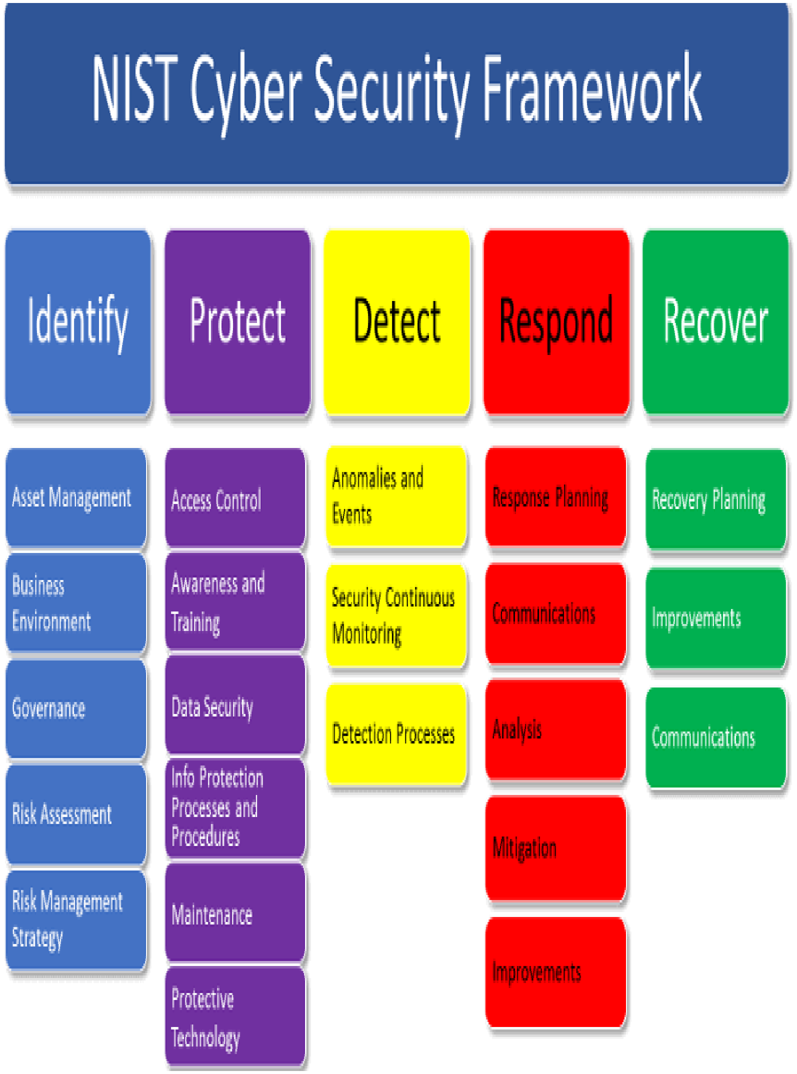
IT Audit Planning

Engagement Planning

Suggested Areas of Focus:

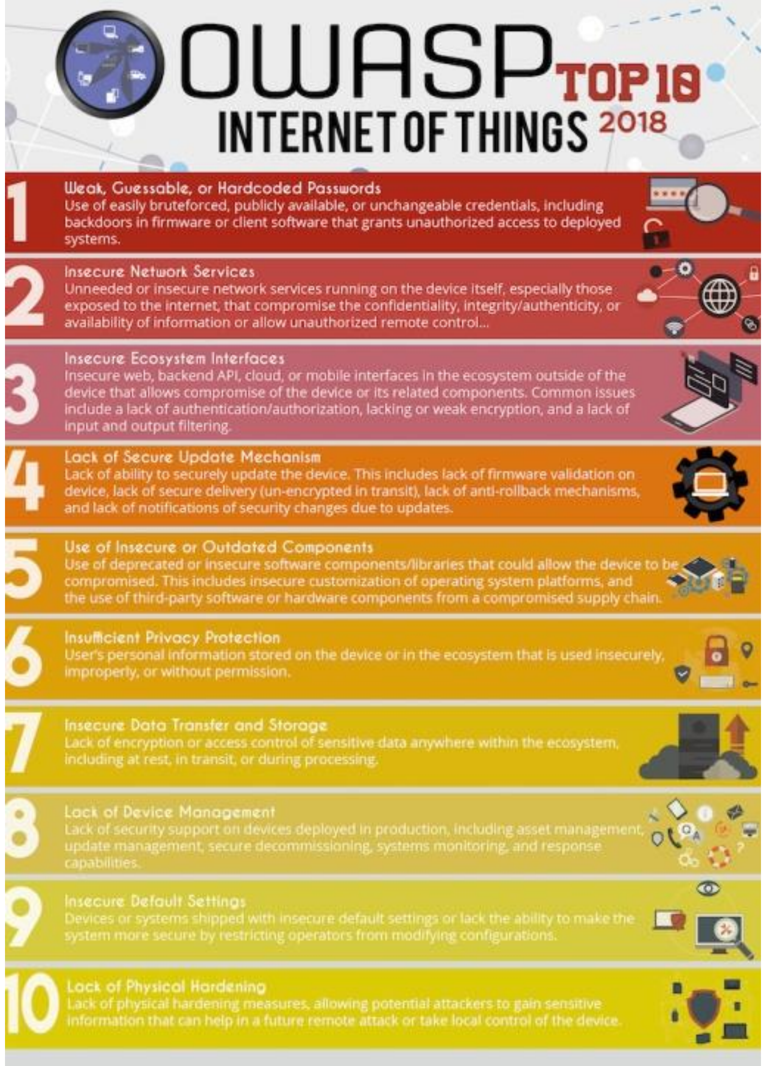
- □ Feasibility of Remote Auditing
- □ Electronic documentation availability (+ capability to scan paper documents)
- □ Remote walkthroughs (‘talk-throughs’), progress updates and report of emerging findings
- □ Availability of new technologies to deliver work, such as Microsoft Teams, Zoom, or Skype for virtual meetings/workshops (Consider recording such interactions to enhance IA evidence)
- □ Deployment of analytics to increase coverage, and focus on outliers
- □ Control override (employees seeking workarounds to existing controls in time of uncertainty)
- □ Increasing risks of fraud

Useful IT Audit Resources



NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			



OWASP TOP 10 INTERNET OF THINGS 2018

1 **Weak, Guessable, or Hardcoded Passwords**
Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

2 **Insecure Network Services**
Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...

3 **Insecure Ecosystem Interfaces**
Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

4 **Lack of Secure Update Mechanism**
Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

5 **Use of Insecure or Outdated Components**
Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.

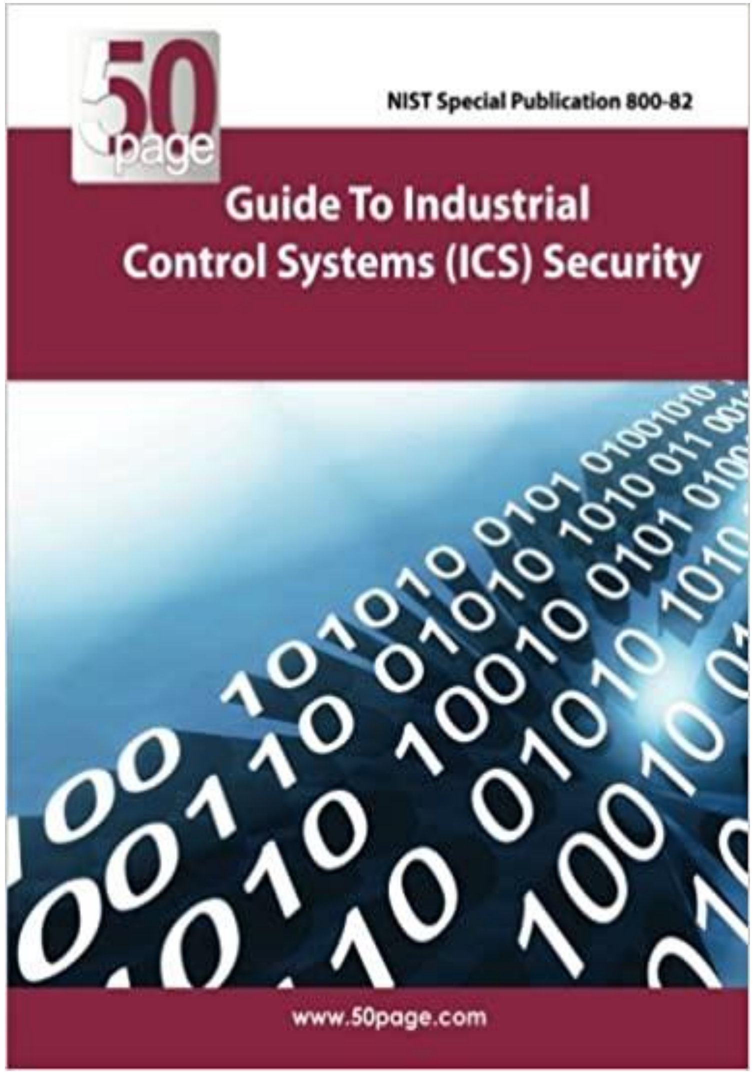
6 **Insufficient Privacy Protection**
User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

7 **Insecure Data Transfer and Storage**
Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

8 **Lack of Device Management**
Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.

9 **Insecure Default Settings**
Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.

10 **Lack of Physical Hardening**
Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.



50 page

NIST Special Publication 800-82

Guide To Industrial Control Systems (ICS) Security

www.50page.com

What’s Next

□ **Auditors**

- □ Assess your skills fit (vs the Future)

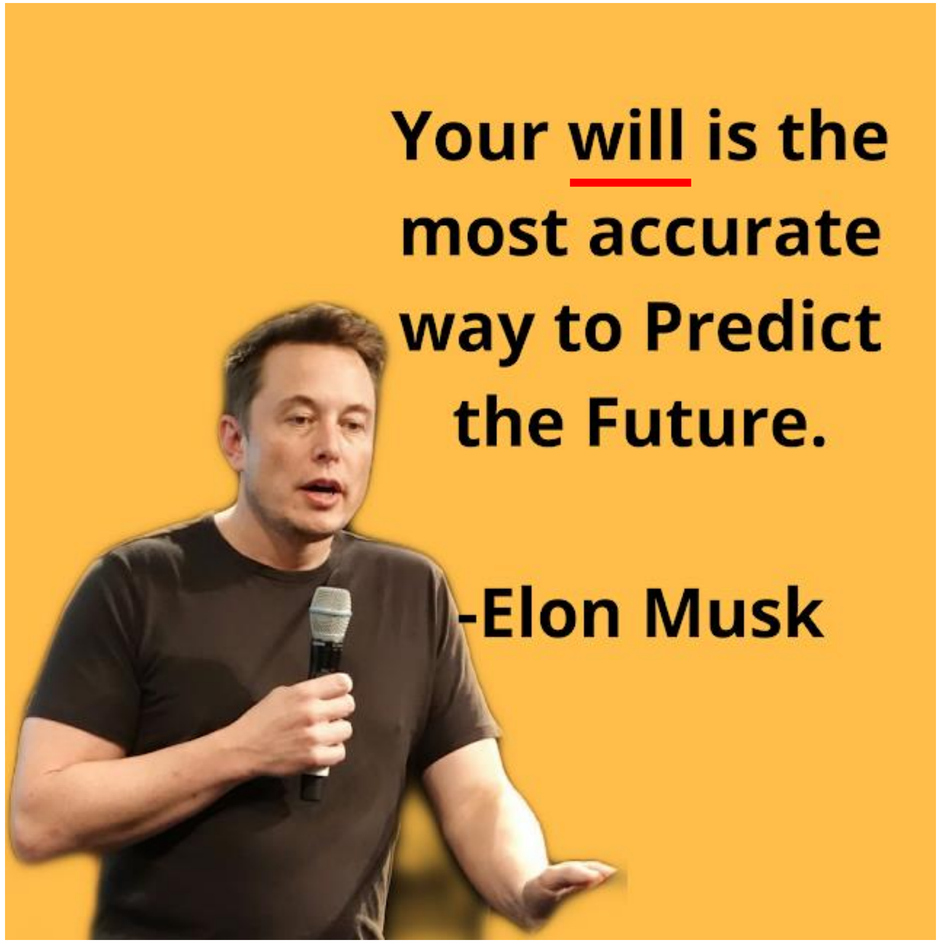
□ **Audit Leaders**

- □ Invest in RPA and AI
- □ Recruit and empower “digital-savvy” employees

□ **Governments / Organisations**

- □ Prepare for dramatic shifts in work and workforce distribution patterns
- □ Embrace Technologies, and Digital Transformation
- □ Focus on UI / UX

No one knows what the digital future will be ….



THANK YOU!