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
Embracing the New Normal

- COVID-19
- Impact to Internal Audit Functions
- Everything Digitized

IT Audit Resources

IT Audit Planning
# THE NEW NORMAL
## Post COVID-19

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

**CONFIRMED/1M**

Albania > Armenia > Azerbaijan > Belarus = Bosnia and Herzegovina = Bulgaria = Croatia = Czechia = Georgia = Hungary = Kazakhstan = Kosovo = Kyrgyzstan = Moldova = Montenegro = North Macedonia = Romania = Russia = Serbia = Tajikistan = Turkey = Ukraine = Uzbekistan

**DEATHS/1M**

Albania > Armenia > Azerbaijan > Belarus = Bosnia and Herzegovina = Bulgaria = Croatia = Czechia = Georgia = Hungary = Hungary = Kazakhstan = Kosovo = Kyrgyzstan = Moldova = Montenegro = Montenegro = North Macedonia = Romania = Russia = Serbia = Tajikistan = Turkey = Ukraine = Uzbekistan

![Bar chart showing confirmed and deaths per million for each country](chart.png)
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
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)
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?

Someone who can understand the Business and IT Alignment Challenges
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?

- Auditor Management
- RPA / CAATs
- Client Management
- Portfolio Management
- Project Management
- Risk Management (and Planning)
- Workpaper Management
## IT Audit Planning

1. Understand the enterprise context and strategy.
   - Understand enterprise strategy.
   - Understand enterprise goals.
   - Understand the risk profile.
   - Understand current IT-related issues.

2. Determine the components of the IT audit universe.
   - Consider the components of a governance system.
   - Determine the IT audit portfolio.
   - 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 Components vs. IT Audit Portfolio Examples

<table>
<thead>
<tr>
<th>Governance System Component</th>
<th>IT Audit Portfolio Examples</th>
<th>Potential Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processes</td>
<td>COBIT® 2019 processes</td>
<td>COBIT 2019 Governance and Management Objectives<a href="#">^3</a></td>
</tr>
<tr>
<td>Organizational Structures</td>
<td>Third-party suppliers, subsidiaries, divisions of the enterprise</td>
<td>Enterprise resource planning (ERP) system, enterprise structure documentation, organization charts</td>
</tr>
<tr>
<td>Principles, Policies, Procedures</td>
<td>Privacy, laws, regulations and other compliance requirements</td>
<td>Legal, privacy, security, and governance, risk and compliance (GRC) functions</td>
</tr>
<tr>
<td>Information</td>
<td>How IT audit reports its performance</td>
<td>Audit committee requirements</td>
</tr>
<tr>
<td>Culture, Ethics and Behavior</td>
<td>Audit recommendation follow-ups, new IT initiatives</td>
<td>Internal audit and management—scheduled recommendation completion dates, completed recommendations</td>
</tr>
<tr>
<td>People, Skills and Competencies</td>
<td>Training to be undertaken by IT audit; training to be given by IT audit; audit of general IT awareness training</td>
<td>Training plans, personal development plans</td>
</tr>
<tr>
<td>Services, Infrastructure and Applications</td>
<td>Applications, databases, websites, operating systems, virtual machines, etc.</td>
<td>IT asset register</td>
</tr>
</tbody>
</table>

Source: ISACA Journal - 2019 May 1 - “Developing the IT Audit Plan Using COBIT 2019”
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**.
(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
(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

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

(4) Review existing policies, guidelines
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
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 ....

Your will is the most accurate way to Predict the Future.

- Elon Musk
THANK YOU!