Internal Audit

“Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes”
Internal Audit

• Promotes organizational improvement
• Provides risk-based assurance
• Aligns with the strategies, objectives and risks of the organization
• Proactive and future-focused
• Communicates effectively
In the midst of cybersecurity incidents and risks, the question arises:

*Where Should Internal Audit Stand?*
Starts from the Top:

- Have a cybersecurity expertise on the Board
- Make cybersecurity a constant Board agenda item
- Define & establish a cybersecurity roadmap
- Regularly review cybersecurity strategies for effectiveness
- Monitor & evaluate
Internal Audit

• Understand the business crown jewels – Key processes and products.
• Understand the underlying IT environment.
• Assess the current risks.
• Identify threats and vulnerabilities
Key Questions:

• Is cybersecurity on the current, previous and future audit plans?
• How frequently do we audit cybersecurity?
• Does Internal Audit have cybersecurity audit skills?
• Are cybersecurity issues communicated in business language?
<table>
<thead>
<tr>
<th>Function</th>
<th>Function</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.AC Identity Management and Access Control, PR.AT Awareness and Training, PR.DS Data Security, PR.IP Information Protection Processes and Procedures, PR.MA Maintenance, PR.PT Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE Anomalies and Events, DE.CM Security Continuous Monitoring, DE.DP Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>RS.RP Response Planning, RS.CO Communications, RS.AN Analysis, RS.MI Mitigation, RS.IM Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.RP Recovery Planning, RC.IM Improvements, RC.CO Communications</td>
</tr>
</tbody>
</table>

Reference: NIST Cybersecurity V1.1
A HISTORICAL TIMELINE

The COBIT® Framework

**1995**
- Windows 95, Java, and HTML 2.0 (first formal HTML standard) debuted, as did Amazon.com, craigslist.com, match.com and eBay.

**1997**
- Original wireless LAN standard (IEEE 802.11) released, DVD technology appeared, and Google.com registered as domain—incorporating a year later and launching in 1999.

**1996**
- ISACA released the first edition of COBIT framework.

**1998**
- The debut of the second edition of COBIT added Control to its framework.

**2000**
- A third edition of COBIT, with new Management Guidelines, was published.

**2001**
- Internet Archive’s "Wayback Machine" (archive.org) launched, Wikipedia started publishing, and Apple released iPod.

**2002**
- U.S. Sarbanes-Oxley law revolutionized corporate recordkeeping and retention standards, leading to new IT regulatory requirements.

**2003**
- Third Wi-Fi standard created proliferation of “hotspots” as Skype, LinkedIn and WordPress started up. U.S. CAN-SPAM Act became law.

**2004**
- COBIT 4.0 becomes the fourth edition in the COBIT series of releases.

**2005**
- ISACA created an online version of the third edition of COBIT.

**2006**
- Twitter founded and Google acquired YouTube.

**2007**
- Apple iPhone signaled move to touchscreen devices, Apple App Store went online one year later.

**2012**
- ISACA publishes COBIT 5, an update that adds design factors and focus areas to make it more practical and customizable.

**2014**
- Internet of Things (IoT) technology standard ushered new wave of smart devices.

**2015**

**2016**
- ISACA acquired CMMI Institute and its business maturity and capability models, adding these resources to the ISACA/COBIT framework portfolio.

Reference: www.isaca.org
### Governance Objectives

<table>
<thead>
<tr>
<th>EDM01</th>
<th>EDM02</th>
<th>EDM03</th>
<th>EDM04</th>
<th>EDM05</th>
</tr>
</thead>
</table>

### Management Objectives

#### Align, Plan & Organize (APO)
- APC01: Managed I&T Framework
- APC02: Managed Strategy
- APC03: Managed Enterprise Architecture
- APC04: Managed Innovation
- APC05: Managed Portfolio
- APC06: Managed Budget & Costs
- APC07: Managed Human Resources
- APC08: Managed Relationships
- APC09: Managed Service Agreements
- APC10: Managed Vendors
- APC11: Managed Quality
- APC12: Managed Risk
- APC13: Managed Security
- APC14: Managed Data

#### Build, Acquire & Implement (BAI)
- BAI01: Managed Programs
- BAI02: Managed Requirements Definition
- BAI03: Managed Solutions Identification and Build
- BAI04: Managed Availability and Capacity
- BAI05: Managed Organizational Change
- BAI06: Manage IT Changes
- BAI07: Manage IT Change Acceptance and Transitioning
- BAI08: Managed Knowledge
- BAI09: Managed Assets
- BAI10: Managed Configuration
- BAI11: Managed Projects

#### Deliver, Service & Support (DSS)
- DSS01: Managed Operations
- DSS02: Managed Service Requests & Incidents
- DSS03: Managed Problems
- DSS04: Managed Continuity
- DSS05: Managed Security Services
- DSS06: Managed Business Process Controls

#### Monitor, Evaluate & Assess (MEA)
- MEA01: Managed Performance and Conformance Monitoring
- MEA02: Managed System of Internal Control
- MEA03: Managed Compliance with External Requirements
- MEA04: Managed Assurance

*Reference: COBIT 2019 Framework: Governance and Management Objectives, Chapter 1 Introduction*
Areas to Assess:

• Penetration testing & vulnerability assessment; frequency, remediation & reporting
• Effectiveness of patch management procedures
• Review for critical security systems configurations
• Review for end points controls
• Training & awareness program
Areas to Assess:

- Access controls; logical & physical
- Third party management
- Detection capabilities
- Business Continuity planning & disaster recovery
- Data backup arrangements
- Incident Response planning
“Internal Auditors are Partners of Management”
CYBER SECURITY AND RESILIENCE SYMPOSIUM

TOWARDS A RESILIENT AVIATION CYBERSPACE

AMMAN, JORDAN | 15-17 OCTOBER 2019