Top IT and Cyber Risks to include in your Audit Plan: 2020 Update

HCCA – Compliance Institute
March 30, 2020
Nashville, TN

Today’s Presenter

• Johan Lidros, Founder and President of Eminere Group
• Has provided information technology governance and information security services in the healthcare industry for 20 years in Europe and in the United States
• Well-versed in accepted IT and information security standards/frameworks (ISO27000, HITRUST, NIST, COBIT, CIS, etc.) and has participated in several related committees
• Certifications: CISA, CISM, CGEIT, ITIL-F, CRISC, HITRUST CCSFP
Table of Contents

• Introduction
  • Key IT and Cyber Risks to Audit
  • Board and Management Communication
  • Best Practices and Additional Resources
  • Wrap-up and Q&A

Objectives

• You will learn:
  • The latest key IT and Cyber Risks you need to monitor and audit;
  • How to discuss IT and Cyber Risks with management, and
  • How to turn IT and Cyber Risks into opportunities.

• We will share:
  • Trending IT governance and security best practices;
  • Accepted industry standards, and
  • Sources for further research.

• Your Questions! We welcome your questions – don’t save them for the end!
Introduction

- Information technology (IT) is critically important for healthcare organizations.
- The complexity and rate of change of technology can dramatically impact risk and compliance.
- The latest IT and cyber threats can challenge a healthcare provider’s ability to deliver quality outcomes.
- Improvements in IT Governance can help prepare organizations for to manage Health IT and traditional IT risks
- A wealth of best practices and industry standards are available to help healthcare organizations improve their cyber-security, IT Audit and IT Risk compliance.

Healthcare System Challenges

Technology offers powerful tools, but is not – by itself – the solution!

Cybersecurity can be an enabler – but is often seen as an inhibitor!
Common Attack Vectors-Weakest Link

- Email
- Authentication
- Privileged Accounts
- Web Application

Equifax Breach – What happen?

Maersk – notpetya – World Forum Davos

“It cost us between 250-300 million dollars, and yet I argue it was a very important wake-up call....”

“Average is not good enough…”

“stop being naïve…”

“we have to be pro-active…”

“need for radical improvement of infrastructure for all organizations…”

• https://www.youtube.com/watch?v=VaqIYlYmDbA

Auditing and IT Risk, Governance, etc.

• IIA 2120 - Risk Management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

• Determining whether risk management processes are effective is a judgment resulting from the internal auditor’s assessment that:
  • Organizational objectives support and align with the organization’s mission;
  • Significant risks are identified and assessed;
  • Appropriate risk responses are selected that align risks with the organization’s risk appetite; and
  • Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.
Table of Contents

• Introduction
• Key IT and Cyber Risks to Audit
  • Board and Management Communication
  • Best Practices and Additional Resources
• Wrap-up and Q&A

Health IT - Definition

• The term “Health IT” is broadly used currently and refers to an array of technologies to store, share, and analyze health information.

“Health IT systems compromise the hardware and software that are used to electronically create, maintain, analyze, store, or receive information to help in the diagnosis, cure, mitigation, treatment, or prevention or disease.”

Office for the National Coordinator of Health Information Technology
Typical Health IT Systems

<table>
<thead>
<tr>
<th>Health IT Systems</th>
<th>Example</th>
</tr>
</thead>
</table>
| Administrative/billing or practice management system | • Coding/billing system  
|                                                 | • Master patient index  
|                                                 | • Registration/appointment scheduling system                           |
| Automated dispensing system                      | • Medication dispensing cabinet                                         |
| Computerized medical devices                      | • Infusion pumps with dose-error-reduction capability  
|                                                 | • Patient monitoring systems (e.g., cardiac, respiratory, fetal)       |
| Electronic health record (EHR) or EHR component   | • Bar-coded medication administration  
|                                                 | • Clinical decision support system  
|                                                 | • Clinical documentation system (e.g., progress notes)  
|                                                 | • Computerized provider order entry  
|                                                 | • Pharmacy system                                                       |
| Human interface device                            | • Keyboard,  
|                                                 | • Monitor/display/Touchscreen  
|                                                 | • Mouse  
|                                                 | • Speech recognition system                                             |
| Laboratory information system                     | • Microbiology system  
|                                                 | • Pathology system  
|                                                 | • Test results                                                          |
| Radiology/diagnostic imaging system               | • Picture archiving and communication system                            |

Key Drivers Impacting Health IT

- Regulatory requirements
- PII/EPHI Theft
- Telehealth
- Big data Analytics
- Cloud
- Patient interaction
- Social media
- Portable devices
- Confidentiality
- Data integrity
- Application
- Patient Safety
- Information Governance
- Information Security

Compliance Institute
March 29—April 1 • Gaylord Opryland • Nashville
Health IT – Enterprise Impact

Healthcare IT Characteristics

- Diversified IT environment
- Medical Devices/Biomedical/Health Technology and IT systems coming together
- EMR and HIE are changing the IT environment – Still...
- Location of healthcare services provided
  - On-site
  - Telehealth
  - Internet of Things
- Cloud is getting common and more outsourcing
- Many regulatory requirements and more to come....
- Constantly new and changing threats/risks related to the use of technology
- The “value” of information
- Immature IT/Information Security
Typical Key IT Risks

<table>
<thead>
<tr>
<th>Risk List</th>
<th>Risk List</th>
<th>Risk List</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Vendor/Supplier Management</td>
<td>13. Data Warehouse and Other Data Repositories</td>
<td>25. PCI-DSS Compliance</td>
</tr>
<tr>
<td>3. Identity and Access Management</td>
<td>15. IT Governance / IT Security Governance</td>
<td>27. Resources and IT Skills</td>
</tr>
<tr>
<td>6. Electronic Communication (Email, Texting, Faxing)</td>
<td>18. Disposal of Electronic Media</td>
<td>30. Grants w. IT Security Requirements / Research (CMMC, DFARS, etc.)</td>
</tr>
<tr>
<td>8. Medical Devices/Health Technology</td>
<td>20. Information/Data Governance</td>
<td>32. IT Cost</td>
</tr>
<tr>
<td>10. Security Awareness</td>
<td>22. Physical Security; IT Environmental Controls</td>
<td>34. Telehealth</td>
</tr>
<tr>
<td>11. Internet Usage and Social Media</td>
<td>23. End-User Devices (Workstations, Tablets, Laptops, USBs, Smart phones, etc.)</td>
<td>35. Privacy/GDPR/State Privacy, etc.</td>
</tr>
<tr>
<td>12. Audit Trail and Logs</td>
<td>24. IoT</td>
<td></td>
</tr>
</tbody>
</table>

Top 10 Health Technology Hazards—ECRI 2020

1. Misuse of Surgical Staplers
2. Adoption of Point-of-Care Ultrasound Is Outpacing Safeguards
3. Infection Risks from Sterile Processing Errors in Medical and Dental Offices
4. Hemodialysis Risks with Central Venous Catheters—Will the Home Dialysis Push Increase the Dangers?
5. Unproven Surgical Robotic Procedures May Put Patients at Risk
6. Alarm, Alert, and Notification Overload
7. Cybersecurity Risks in the Connected Home Healthcare Environment
8. Missing Implant Data Can Delay or Add Danger to MRI Scans
9. Medication Errors from Dose Timing Discrepancies in EHRs
10. Loose Nuts and Bolts Can Lead to Catastrophic Device Failures and Severe Injury
Health IT Risks – ECRI 2018

1. Ransomware and Other Cybersecurity Threats to Healthcare Delivery Can Endanger Patients
2. Endoscope Reprocessing Failures Continue to Expose Patients to Infection Risk
3. Mattresses and Covers May Be Infected by Body Fluids and Microbiological Contaminants
4. Missed Alarms May Result from Inappropriately Configured Secondary Notification Devices and Systems
5. Improper Cleaning May Cause Device Malfunctions, Equipment Failures, and Potential for Patient Injury
6. Unholstered Electrosurgical Active Electrodes Can Lead to Patient Burns
7. Inadequate Use of Digital Imaging Tools May Lead to Unnecessary Radiation Exposure
8. Workarounds Can Negate the Safety Advantages of Bar-Coded Medication Administration Systems
9. Flaws in Medical Device Networking Can Lead to Delayed or Inappropriate Care
10. Slow Adoption of Safer Enteral Feeding Connectors Leaves Patients at Risk

Polling Question #1

• What is your organization's top IT Risk Challenge? Select your top 3.
A. Privacy – GDPR, CCPA – California Consumer Privacy Act (Jan 1, 2020)
B. IT Governance
C. Identity & Access Management (IAM)
D. Cyber Risk/Network Security
E. Medical Devices Management / IOT/ Health Technology
F. Business Continuity / Disaster Recovery
G. Mobile Devices - BYOD
H. IT Vendor Management
I. Security Awareness / Phishing
J. Blockchain
K. Others. Please list
Most Common Audit Areas

- Identity and Access Management
- EMR Core System
- IT General Controls
- HIPAA
- Financial Systems
- Vendor Management
- Business Continuity and Disaster Recovery
- Network Security/Cybersecurity
- PCI
- Mobile Device Management
- Patch Management
- New Systems
- Privacy

Polling Question #2

What is your most critical System?
A. EMR
B. Financial System
C. Pharmacy
D. Data Warehouse
E. PACS
F. Password/Encryption key vault
Additional Key Risks to Audit

- Health IT
  - Internet of Things
  - Telehealth
  - Apps (internet of things)
  - Risk Management
  - Medical Devices
- Data Warehouse
- HIE
- Information Governance
- IT Governance
- Patient Communication/Portal
- Backup Management
- Security Awareness Training
- Emergency Management/BCP/DR
- Departmental IT

Added Value Audits – Hidden Opportunities

- Life Cycle Management
  - Application/Tool functionality
  - Inventories
  - Cost
  - Age
  - Utilization, ownership
  - Budget/capacity/acquisition processes
- Identity and Access management
  - Number of systems
  - Authentication
  - Resources for management of access management (FTE/cost)
- IT Value/IT Cost
  - You cannot manage what you do not measure!
IT Audit Plan Considerations

• Comprehensive IT Risk Assessment
• Build Long Term IT Audit Plan
• IT Governance Audit
• Regular Audit of Key Control Areas
  • Value added internal benchmarks
  • Trends
• Framework Based
  • Standard benchmark
• Pro-Active Audits/Value Added Work
  • Pre-implementation
  • Committees
• Value – Cost – Investment – i.e. Performance
• Audit Tools – Key Component for Effective and Efficient IT Risk Management

Table of Contents

• Introduction
• Key IT and Cyber Risks to Audit
• Board and Management Communication
• Best Practices and Additional Resources
• Wrap-up and Q&A
Discussion Areas with Management / Board – Tone from the To

- Health IT
- IT Governance
- Information Governance
- Information Security
- IT Standards
- Measurements and Metrics

• It Pays to Have a Digitally Savvy Board – MIT White paper

  Magazine: Spring 2019 Issue Research Highlight  March 12, 2019  Reading Time: 10 min  https://sloanreview.mit.edu/article/it-pays-to-have-a-digitally-savvy-board/
Actions to Reduce Risk

- Leadership
  - Governance !!!
  - Multidisciplinary Involvement
  - Vendor selection and Involvement
  - Change management
  - Control effectiveness and efficiency
- Safety culture and process improvement
  - Comprehensive system analysis/risk assessments/failure mode and effects analysis
  - Shared involvement and responsibility
  - System implementation and upgrades

IT Governance Framework
**IT Goals and Metrics-Key Performance Indicators & Key Goal Indicators**

You cannot manage what you do not measure!

**DEFINE GOALS**

- **ACTIVITY GOAL**: Understand security requirements and threats.
- **PROCESS GOAL**: Detect and resolve unauthorized access.
- **IT GOAL**: Ensure IT services can resist and recover from attacks.
- **BUSINESS GOAL**: Maintain enterprise reputation and leadership.

**MEASURE**

- **PROCESS METRICS**: Frequency of review of the type of security events to be monitored.
- **IT METRICS**: Number of access violations.
- **BUSINESS METRICS**: Number of incidents with business impact.

**DRIVE PERFORMANCE**

- Key Performance Indicators (KGI) & Key Goal Indicators (KPI)

---

**Board / Executive IT Risk Dash Board**

<table>
<thead>
<tr>
<th>Category</th>
<th>Is Risk</th>
<th>Risk Level</th>
<th>Risk Mgr Plan</th>
<th>Regulatory Audit</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Risk Management</td>
<td>Yes</td>
<td>High</td>
<td>1</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Information &amp; Asset Inventory</td>
<td>Yes</td>
<td>High</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>Information Protection</td>
<td>Yes</td>
<td>High</td>
<td>3</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Information Security Program</td>
<td>Yes</td>
<td>High</td>
<td>4</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>Incident &amp; Access Control</td>
<td>Yes</td>
<td>High</td>
<td>5</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Threat &amp; Vulnerability Management</td>
<td>Yes</td>
<td>High</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Third Party Security</td>
<td>Yes</td>
<td>High</td>
<td>7</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>IT Operations</td>
<td>Yes</td>
<td>High</td>
<td>8</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>Business Continuity &amp; Disaster</td>
<td>Yes</td>
<td>High</td>
<td>9</td>
<td>9</td>
<td>6</td>
</tr>
<tr>
<td>Physical &amp; Environmental Controls</td>
<td>Yes</td>
<td>High</td>
<td>10</td>
<td>10</td>
<td>6</td>
</tr>
<tr>
<td>Organization Security &amp; Awareness</td>
<td>Yes</td>
<td>High</td>
<td>11</td>
<td>11</td>
<td>6</td>
</tr>
<tr>
<td>IT Compliance Management</td>
<td>Yes</td>
<td>High</td>
<td>12</td>
<td>12</td>
<td>6</td>
</tr>
</tbody>
</table>

**Legend**

- **Risk Rating**: Low, Medium, High
- **Trend**: Risk increasing, Risk decreasing, No change

---

*HCCA Compliance Institute*
March 29–April 1, Gaylord Opryland, Nashville

Register now
Regular Security Reporting

- **Risk Management Program**
  - Status management program – see example previous page – Dash board
  - Number of risk assessments performed – Defined assessments and analysis per IT and organization projects, to include change control.
  - Time to remediate issues – The time between identification and remediation.

- **Vulnerability Management**
  - Issues by Status – When a vulnerability is identified on a system the first time, it is a new data point that should inform and, depending on the situation, drive an action.
  - Remediation Time - Measure the length of time from identification to remediation and is a measure of the efficiency of the patch and remediation cycle.
  - Mean time to Patch – The time between identification of a needed patch and the installation of the required patch.

- **Exceptions**
  - The number of information security policy exceptions requested and granted

- **Incident Management**
  - Number of Events - Events are activities or indicators that warrant further investigation and can be indicators of incidents.
  - Number of Incidents - Incidents occur when a material event or events have occurred and require a formal response activity.

- **Specific Initiatives**
  - Program/projects

---

<table>
<thead>
<tr>
<th>Quality Area</th>
<th>Quality Requirements</th>
<th>CMS Reference</th>
<th>Goal</th>
<th>Current Status Accountable</th>
<th>Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information System Assets (Medical Devices, Server, End User Computing Devices, Databases, Software, Data)</td>
<td>Identify and classify all information system assets</td>
<td>CP-2(8)</td>
<td>100% of all information system assets classified annually and approved by data owner</td>
<td>70% of all Information System Assets Classified and approved by data owner.</td>
<td>Data Owner CISO</td>
</tr>
</tbody>
</table>

---
Polling Question #3

- How confident are you that you are providing executive leadership sufficient information to help them manage IT Risk?
  - Very Confident
  - Confident
  - Not Very Confident
  - Unsure

Polling Question 4

- Who should approve your IT risk management dashboard?
  a) CIO
  b) Board
  c) Executive Management
  d) All
Table of Contents

- Introduction
- Key IT and Cyber Risks to Audit
- Board and Management Communication

Best Practices and Additional Resources
- Wrap-up and Q&A

News on Standards

- NIST Privacy Framework
- TIR97 – Biomedical devices
- Pre-market Requirements for Medical Device Cybersecurity – Health Canada
- Core Cybersecurity Feature Baseline 2 for Securable IoT Devices – NIST 8529
- NACD – A Board Primer on Block Chain
- Essential Eight Maturity Model – Australian Cyber Security Center
- Penetration Testing for the Financial Industry GFMA, SIFMA, AFME, ASIFMA
- The Healthcare and Public Health Sector Coordinating Council (HSCC) – Several papers
- NIST -Identifying and Protecting Assets Against Ransomware and Other Destructive Events.
  - https://www.healthit.gov/playbook/
Health IT Playbook

Resources

- Research Findings: Technology and Clinician Cognitive Overload – Easing the Pain. – HIMSS Analytics
Resources

- **AAMI** [www.aami.org](http://www.aami.org)
  - TIR57: Principles for medical device security—Risk management
  - TIR97: Principles for medical device - Post-market security management for device manufactures
  - AAMI Medical Device Cybersecurity – A guide for HTM professional
- **The Center for Internet Security (CIS)**
  - Critical Security Controls for Effective Cyber Defense [https://www.cisecurity.org/controls/](https://www.cisecurity.org/controls/)
  - Regular updates OS security standards.
- **Center for Disease Control and Prevention (CDC) and HHS**
- **Cloud Security Alliance**
  - Cloud Controls Matrix version v3 [https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/](https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/)
  - Top Threats to Cloud Computing: Deep Dive
- **OWASP** Secure Medical Device Deployment Standard
- **CMS**
  - CMS Acceptable Risk Safeguards (ARS) Includes detailed privacy and security controls mapped to HIPAA, and NIST
  - Recommendations to Providers Regarding Cyber Security January 13, 2017

**ISACA**
- COBIT – Leading IT Governance Framework

**FDA**

**Healthcare Industry Cybersecurity Taskforce (HHS)**
- Report on improving cybersecurity in the healthcare industry

**Healthcare & Public Sector Coordinating Council (HSCC) with HSCC Joint Cybersecurity Working Group (JCGW)**
- Healthcare Industry Cybersecurity Practices [https://www.phe.gov/Preparedness/planning/405d/Pages/default.aspx](https://www.phe.gov/Preparedness/planning/405d/Pages/default.aspx)

**HITRUST**
- [www.hitrustalliance.net](http://www.hitrustalliance.net)

**MDISS Medical Device Innovation, Safety and Security Consortium**
- MDISS Tool – security risk assessment medical devices Tool MDRAP [https://mdrap.mdiss.org](https://mdrap.mdiss.org)
Resources

- NACD – National Association of Corporate Directors
  - Cyber Risk Oversight [Website Link]
- NIST
  - Cybersecurity Framework - Framework for Improving Critical Infrastructure Cybersecurity version 1.1 January 2017
  - Cybersecurity Resource Center [Website Link]
  - Core Cybersecurity Feature Baseline 2 for Secureable IoT Devices – NIST 8529
  - NIST Privacy Framework 1.0 [Website Link]
- IT Security Architecture to protect from Ransomware
- Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events (Website Link)
- ONC – Health IT
  - SAFER Guides - [Website Link]
  - How to Identify and Address Unsafe Conditions Associated with Health IT
  - The Role of Health IT Developers in Improving Patient Safety in High Reliability Organizations
  - Health IT Playbook [Website Link]
- OCR
  - HIPAA Audit Program (Privacy, Breach and Security)
  - Penetration Testing for the Financial Industry GFMA, SIFMA, AFME, ASIFMA
    - [Website Link]
- Secured Culture Framework
  - Security Awareness Framework [Website Link]
- Shared Assessments/BITS
  - IT Vendor Management. First developed for Financial industry now general vendor management and other industries including healthcare. [Website Link]

Table of Contents

- Introduction
- Key IT and Cyber Risks to Audit
- Board and Management Communication
- Best Practices and Additional Resources
- Wrap-up and Q&A
Conclusion

• Risk based Long Term Audit Plan
  • Health IT
  • Key Controls
  • Operational efficiency

• Drive Measurements and Metrics
  • Board and Management discussions
  • Audits

• Several good practices and standards exist to guide you in most areas

Questions??
Key weekly updates

• Interested in on-going IT Governance and IT Security updates?
  • Sign up for our weekly newsletter “RiskIT” at www.emineregroup.com

Contact Johan

• Johan Lidros
  • Johan.lidros@emineregroup.com
  • w (813) 832-6672 x9101
  • c (813) 355-6104