Top Cyber Risks to Include in Your Audit Plan - Update

HCCA – Compliance Institute
April 9, 2019

Johan Lidros CISA, CISM, CGEIT, CRISC, HITRUST CCSFP, ITIL-F
President Eminere Group

Presenter

- Johan Lidros, Founder and President of Eminere Group
- Over 20 years of experience providing information technology security, compliance and governance services in the healthcare industry 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

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 IT audit challenges.
- A wealth of best practices and industry standards are available to help healthcare organizations improve their cyber-security, IT Audit and IT Risk compliance.
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.

- We welcome your questions – don’t save them for the end!

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

- Regulatory requirements
- PII/EPHI Theft
- Telehealth
- Big data and Analytics

Cloud
Data Integrity
Availability
Patient interaction
Social media
Portable devices

Health IT – Enterprise Impact

Health Information Technology

- Hardware and software
- Clinical content
- Human-computer interface
- People
- Workflow and communication
- Internal organization policies, procedures, environment, and culture
- External rules, regulations, and pressures
- System measurement and monitoring
Healthcare IT Characteristics

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

Typical IT Risks

<table>
<thead>
<tr>
<th>Risk List</th>
<th>Risk List</th>
<th>Risk List</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Vendor 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>8. Medical Devices</td>
<td>20. Information/Data Governance</td>
<td>32. IT Cost</td>
</tr>
<tr>
<td>10. Security Awareness</td>
<td>22. Physical Security and 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>
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

AHIA 2017 IT Audit Survey

<table>
<thead>
<tr>
<th>Audit Area</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network security</td>
<td>60.5%</td>
</tr>
<tr>
<td>Identity and Access management</td>
<td>55.3%</td>
</tr>
<tr>
<td>Electronic medical record system</td>
<td>44.7%</td>
</tr>
<tr>
<td>Business continuity/disaster recovery</td>
<td>44.7%</td>
</tr>
<tr>
<td>IT general controls</td>
<td>44.7%</td>
</tr>
<tr>
<td>Financial systems</td>
<td>42.1%</td>
</tr>
<tr>
<td>Change management</td>
<td>42.1%</td>
</tr>
<tr>
<td>HIPAA Security</td>
<td>42.1%</td>
</tr>
<tr>
<td>Patch management</td>
<td>39.5%</td>
</tr>
<tr>
<td>PCI compliance</td>
<td>39.5%</td>
</tr>
<tr>
<td>Mobile device security/BYOD</td>
<td>39.5%</td>
</tr>
<tr>
<td>Vendor management</td>
<td>36.8%</td>
</tr>
<tr>
<td>Biomedical devices</td>
<td>34.2%</td>
</tr>
<tr>
<td>Cloud security</td>
<td>34.2%</td>
</tr>
<tr>
<td>Pre- or Post-implementation review</td>
<td>34.2%</td>
</tr>
<tr>
<td>HIPAA Privacy</td>
<td>34.2%</td>
</tr>
<tr>
<td>Security Incident Management</td>
<td>31.6%</td>
</tr>
</tbody>
</table>
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
- PCI
- Mobile Device Management
- Patch Management
- Cybersecurity
- New Systems

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
- GDPR/State privacy...
Added Value Audits – Hidden Opportunities

- **Life Cycle Management**
  - Application/Tool functionality
  - Tools
  - Cost
  - Age
  - Utilization
  - Budget/capacity/acquisition processes

- **Identity and Access management**
  - Number of systems
  - Authentication
  - Resources for management of access management (FTE/cost)

IT Audit Plan Considerations

- **Comprehensive IT Risk Assessment**
- **Build Long Term IT Audit Plan**
- **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 Management/Board

- Health IT
- IT Governance
- Information Governance
- Information Security
- IT Standards
- Measurements and Metrics
Actions to Reduce Risk

- Leadership
  - Information governance
  - Multidisciplinary Involvement
  - Vendor selection and Involvement
  - Change management
  - Monitor system effectiveness

- 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

- Drivers
  - PERFORMANCE: Business Goals
  - CONFORMANCE: HIPAA, PCI, etc.

- Enterprise Governance
  - Balanced Scorecards
  - COSO

- IT Governance
  - COBIT

- Best Practice Standards
  - RISK IT
  - ITIL
  - ISO27000/HITRUST
  - PMI
  - CMMI

- Processes and Procedures
  - IT Risk Management
  - IT Service Management
  - Security/Risk Principles
  - Project Management Principles
  - System Development
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**

- **MEASURE OF ACTIVITY**: Frequency of review of the type of security events to be monitored.
- **MEASURE OF PROCESS**: Number of access violations.
- **MEASURE OF IT**: Number of incidents with business impact.
- **MEASURE OF BUSINESS**: Number of incidents causing public embarrassment.

**DRIVE PERFORMANCE**

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

---

**Board / Executive IT Risk Dash Board**

<table>
<thead>
<tr>
<th>Capability</th>
<th>Key Risk</th>
<th>Risk Level</th>
<th>Risk Mitig. Paid</th>
<th>Regulatory Mandates Tracked</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Risk Management</td>
<td>Assets are not defined.</td>
<td>7</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Information &amp; Asset Inventory</td>
<td>Access lists and procedures for classifying, identifying and handling</td>
<td>6</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>information and assets are not managed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Protection</td>
<td>Authorization controls stated to protect sensitive information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Only to restrict collection of personal information for only necessary uses</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security Program Management</td>
<td>Information security program is not aligned with business</td>
<td>13</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td></td>
<td>requirements.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity &amp; Access Management</td>
<td>Policies and procedures have been established for information security</td>
<td>17</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>Threat &amp; Vulnerability Management</td>
<td>Accounts and access to network resources are not standard</td>
<td>16</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Includes details for key access controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third Party Security</td>
<td>No audit plan is in place to address outsourced IT services.</td>
<td>13</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Records for access controls are not tracked</td>
<td>14</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>F Operations</td>
<td>Information security practices are not integrated into IT operations</td>
<td>24</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(change rights, incident sign, etc.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Continuity &amp; Disaster recovery</td>
<td>Information security policies are not documented</td>
<td>8</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ability to recover from an outage has not been tested</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical &amp; Environmental Controls</td>
<td>Control procedures related to IT hardware are not implemented</td>
<td>20</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Environmental controls (power, temp, etc.) to support IT operations are</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>not sufficient.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization Security &amp; Awareness</td>
<td>System and system security responses are not documented</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Actions do not follow their security guidelines</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T Compliance Management</td>
<td>Appropriate mechanisms to monitor and mitigate compliance issues are not</td>
<td>13</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td></td>
<td>implemented.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:
- Low: Risk increasing
- Medium: Risk acceptable
- High: Risk decreasing

Note: Risk Level reflects the level of risk associated with each category. Risk Mitig. Paid indicates the level of mitigation efforts. Regulatory Mandates Tracked reflects the level of compliance with regulatory requirements.
Regular Security Reporting

- **Risk Management Program**
  - Status management program – see example next page – Dashboard
  - 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**
  - CMS Quality Measurements

### CMS Quality Measurements - Examples

<table>
<thead>
<tr>
<th>Quality Area</th>
<th>Quality Requirements</th>
<th>CMS Reference</th>
<th>Goal</th>
<th>Current Status</th>
<th>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, Verify assets and classification annually and obtain data owner approval</td>
<td>CP-10(3) SE-1</td>
<td>100% of all Information System Assets Classified annually and approved by data owner</td>
<td>70% of all Information System Assets Classified</td>
<td>Data Owner</td>
<td>CISO</td>
</tr>
</tbody>
</table>
# 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

# Resources

- **AHIMA**
  - Information Governance Framework [http://www.ahima.org/topics/infogovernance](http://www.ahima.org/topics/infogovernance)
- **AAMI**
  - TIR57: Principles for medical device security—Risk management [www.aami.org](http://www.aami.org)
  - TIR57: Principles for medical device – Post-market security management for device manufacturers (In development)
- **Bipartisan Policy Center**
- **AAMI Medical Device Cybersecurity – A guide for HTM professional**
- **Bipartisan Policy Center**
  - Critical Security Controls for Effective Cyber Defense [https://www.cisecurity.org/controls/](https://www.cisecurity.org/controls/)
- **Center for Internet Security (CIS)**
  - Top Threats to Cloud Computing: Deep Dive
  - OWASP Secure Medical Device Deployment Standard
- **CRICO**
- **CMS**
  - Recommendations to Providers Regarding Cyber Security January 13, 2017
  - CMS Acceptable Risk Safeguards (ARS) – Security and Privacy
- **ECRI Institute**
  - Patient Safety Annual Top 10 studies of patient safety risks
  - Recall information devices
Resources

- FDA
  - Management of Cybersecurity in Medical Devices – Guidance for Industry and FDA Staff
- FFIEC
  - Information Security Booklet Released September 2016
  - Cyber security assessment framework
    https://www.ffiec.gov/cyberassessmenttool.htm
- Healthcare Industry Cybersecurity Taskforce (HRB)
  - Report on improving cybersecurity in the healthcare industry
- Healthcare & Public Sector Coordinating Council (HSPCC) with HSCC Joint Cybersecurity Working Group (JWCG)
  - MEDICAL DEVICE AND HEALTH IT JOINT SECURITY PLAN
    https://healthcarecouncil.org/the-joint-security-plan/
  - Healthcare Industry Cybersecurity Practices
    https://www.phe.gov/Preparedness/planning/biosafetyinformation.html
- HITRUST
  - Privacy
  - NIST CSF
  - The addition of the Center for Internet Security Critical Security Controls (CIS CSC)
  - Precision Medicine Initiative (PMI)
  - OCR Audit Protocol
  - FEDRAMP Support for Cloud and IaaS Service Providers
  - FFIEC IT Examination Handbook for Information Security
- HHS – Agency for Healthcare Research and Quality
  - 2017 NATIONAL HEALTHCARE QUALITY AND DISPARITIES REPORT
- HITRUST
  - Privacy
  - NIST CSF
  - The addition of the Center for Internet Security Critical Security Controls (CIS CSC)
  - Precision Medicine Initiative (PMI)
  - OCR Audit Protocol
  - FEDRAMP Support for Cloud and IaaS Service Providers
  - FFIEC IT Examination Handbook for Information Security
- Joint Commission.
  - Sentinel event alert #54: safe use of health information technology. Oakbrook Terrace, IL: Joint Commission; 2015; Available from: www.jointcommission.org/safehealthit
  - Sentinel event alert #42: Safely implementing health information and converging technologies. Joint Commission; 2008; Available from: www.jointcommission.org/safehealthit
- MDIIS Medical Device Innovation, Safety and Security Consortium
  - MDISS Tool – security risk assessment medical devices Tool MDRAP
    https://mdrap.mdiss.org
- NACD – National Association of Corporate Directors
  - 2017 Cyber Risk Oversight
- NIST
  - Cybersecurity Framework - Framework for Improving Critical Infrastructure Cybersecurity version 1.1 January 2017
  - Cybersecurity Resource Center Beta
    https://beta.csrc.nist.gov/
  - Guide for Cybersecurity Incident Recovery
- ONC
  - National Association of Corporate Directors
    - 2017 Cyber Risk Oversight
  - NIST
    - Cybersecurity Framework - Framework for Improving Critical Infrastructure Cybersecurity version 1.1 January 2017
    - Cybersecurity Resource Center Beta
      https://beta.csrc.nist.gov/
    - Guide for Cybersecurity Incident Recovery
  - ONC
    - Report of the evidence on Health IT Safety and interventions May 2016
    - SAFER Guidelines
      https://www.healthit.gov/safer
    - EHR Contracts Untangled SELECTING WISELY, NEGOTIATING TERMS, AND UNDERSTANDING THE FINE PRINT September 2016
    - 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
- OCR
  - HIPAA Audit Program
    (Privacy, Breach and Security)
  - Security Culture Framework
    https://securitycultureframework.net/
Regulatory Requirements - Changes

- CMS - Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers.
  - Must be in compliance with Emergency Preparedness regulations to participate in the Medicare or Medicaid program.
- Effective date, on November 16, 2017.
  - Testing
  - Cyber event

Health IT – Identify and Assess

- How to Identify and Address Unsafe Conditions Associated with Health IT
  - Office for the National Coordinator of Health Information Technology
SAFER Guides

SAFER – Checklist

Recommended Practices for Phase 2 — Using Health IT Safely

11. The status of orders can be tracked in the system. (Worksheet 11)

12. Clinicians are able to override computer-generated clinical interventions when they deem necessary. (Worksheet 12)
### SAFER Guides

**Recommended Practice**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Clinicians are able to override computer-generated clinical interventions when they deem necessary.</td>
</tr>
</tbody>
</table>

**Rationale for Practice or Risk Assessment**

Computers cannot practice medicine. Disallowing clinician overrides of computer-generated interventions implies that computers have access to more accurate data and greater medical knowledge and expertise than clinicians. This is rarely true.

**Assessment Notes**

**Follow-up Actions**

**Suggested Sources of Input**

- Clinicians, support staff, and/or clinical administration
- EMIR developer
- Health IT support staff

**Examples of Potentially Useful Practices/Scenarios**

- Hard stop alerts (i.e., the user must take an action before proceeding) are used only for the most egregious potential errors. Hard stop alert overrides are closely monitored and reviewed often.
- The alert override rate (i.e., the number of point-of-care alerts that clinicians override divided by the total number of point-of-care alerts generated) is monitored, and alerts with high override rates are reviewed.

Read the Computerized Provider Order Entry with Decision Support Guide for related recommended practices.

---

### Another Resource: RiskIT! Weekly Newsletter

[Subscribe to Eminere Group’s Risk IT! Newsletter](https://www.emineregroup.com/subscribe/)
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?

For questions please contact

- **Johan Lidros**
  - johan.lidros@emineregroup.com
  - (813) 832-6672 x-9101
  - (813) 355-6104 (cell)

- **Tom Smith**
  - tom.smith@emineregroup.com
  - (813) 832-6672 x-9112
  - (501) 837-4001 (cell)