<table>
<thead>
<tr>
<th>No</th>
<th>Question/What is it?</th>
<th>Typical Audit Findings</th>
<th>Why it is Important?</th>
</tr>
</thead>
</table>
| 1  | What standard do they use?  
- A way to measure your security stance.  
- NIST, ISO, CoBIT are examples | - No standard used  
- Not following industry best practices | - How do you prove you are doing what you should be?  
(Due diligence)  
- Standards address common risks  
- Increase performance |
| 2  | Do you have an Inventory?  
- Hardware, Software and Licenses  
- Best to have a continual update process  
- Perform a full inventory and true up at least annually | - Inventory out of date  
- No inventory at all  
- Inventory does not match actual assets (lost or stolen) | - Fines related to missing licenses  
- Missing equipment (did it contain sensitive data?)  
- Out of sight, out of mind, open for attack |
| 3  | Does someone monitor audit logs?  
- Audit logging is a detective control  
- Monitoring audit logs is a preventative control | - Audit logs not turned on  
- If audit logs are turned on, they are not monitored | - Accountability  
- Proactive approach |
| 4  | Do they control administrative privileges?  
- Principle of least access  
- Access only to what is needed | - Administrative passwords are not changed  
- Users are local administrators  
- Information Technology (IT) department users use administrator/root accounts | - Administrative rights give attackers greater access to your systems  
- Increases the impact of an incident |
| 5  | Is access based on need to know?  
- Related to #4  
- Includes excessive access | - File shares with "everyone" access  
- More access than needed for job function  
- Data owners doesn’t know who has access to their data | - Will limit the impact of incidents  
- Limit unnecessary disclosure |
| 6  | Does someone monitor account administration?  
- Who watches the watchers?  
- Often administrative accounts have access above all other accounts? | - Excessive administrative privilege use  
- No one knows what Administrators do to systems | - The ability to find incidents during the normal course of business  
- Proper separation of IT staff duties |
| 7  | Do you have malware defenses?  
- Not just Anti-virus  
- Malware, spyware, adware, virus, worms, popups, Trojans | - Anti-virus not kept up-to-date  
- Not on all machines, typically the ones not on the inventory  
- Only anti-virus, not covering all malware  
- Virus activity reports are not shared with Management | - Still a big deal, ability to response to an incident  
- Downtime  
- Attackers use this as an attack victor still |
| 8  | Do you have data loss prevention?  
- How do you stop data leakage  
- Information floods out of organizations | - No idea what data loss prevention is: policy, training, etc.  
- No data loss prevention strategy or data classification  
- Suffer from the illness that "everything" is public | - Liability (PCI data, HR data, etc.) $$$ |
<table>
<thead>
<tr>
<th>No</th>
<th>Question/What is it?</th>
<th>Typical Audit Findings</th>
<th>Why it is Important?</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Do you have an vulnerability assessments?</td>
<td>- No vulnerability scanning&lt;br&gt;- Not following up on vulnerabilities&lt;br&gt;- No internal scanning</td>
<td>- Most attacks are against vulnerabilities that have patches or fixes</td>
</tr>
<tr>
<td></td>
<td>- What holes do you have in your network?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Know your weaknesses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Are there limits set on your network?</td>
<td>- Access to network is not restricted&lt;br&gt;- Unnecessary service and protocols</td>
<td>- Attackers use these&lt;br&gt;- More to manage, increased expenses</td>
</tr>
<tr>
<td></td>
<td>- Limit access to network ports, protocols and services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Do you have an incident response capability?</td>
<td>- No incident response capability&lt;br&gt;- No training, no idea what is needed</td>
<td>- How an incident is handled will determine if you can take legal action, determine the extent of a breach, stop the incident&lt;br&gt;- Liability $$$</td>
</tr>
<tr>
<td></td>
<td>- Need guidelines on how to respond</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Include evidence preservation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Do you have data recovery capability?</td>
<td>- Backups not tested, backup jobs are not configured properly&lt;br&gt;- Backups onsite&lt;br&gt;- No business continuity plan covering IT (EOC)&lt;br&gt;- Data owners are not informed of the backup strategy or data retention&lt;br&gt;- Backup media is not accounted for</td>
<td>- How much downtime can you tolerate?&lt;br&gt;- What if you had to input everything from scratch?</td>
</tr>
<tr>
<td></td>
<td>- It is one thing to have backups, it is entirely different thing to recover</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Do you have a IT risk management process?</td>
<td>- No formal risk management process (ad-hoc)&lt;br&gt;- Control selection not based upon risk&lt;br&gt;- Risk and controls are not documented formally accepted by data/process owners</td>
<td>- Don’t want to over spend on IT security&lt;br&gt;- Don’t want to under spend on IT security</td>
</tr>
<tr>
<td></td>
<td>- IT control selection should be based upon risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Protects against excessive and inadequate controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Do you separation of duties?</td>
<td>- No Separation of Duties (SOD)&lt;br&gt;- No idea of what duties to separate&lt;br&gt;- IT Management doesn’t identify single source knowledge experts</td>
<td>- Prevents or limits fraud&lt;br&gt;- Especially on financial systems</td>
</tr>
<tr>
<td></td>
<td>- Separation of duties in IT tasks as well&lt;br&gt;- Not for all tasks, just critical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>How do you manage 3rd parties?</td>
<td>- No formal agreement&lt;br&gt;- No monitoring of 3rd parties&lt;br&gt;- No notification provision&lt;br&gt;- No provision to address data ownership at contract termination</td>
<td>- Your responsibility to protect your data&lt;br&gt;- You can transfer authority not responsibility&lt;br&gt;- If you have a breach with your data don’t you want to know ASAP?</td>
</tr>
<tr>
<td></td>
<td>- Get it in writing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Include notification, security requirements and audit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Do you have awareness training?</td>
<td>- No ongoing training&lt;br&gt;- Ad hoc, no records of initial training</td>
<td>- Continuous reminder&lt;br&gt;- Just like safety awareness&lt;br&gt;- Limits liability</td>
</tr>
<tr>
<td></td>
<td>- Initially upon hire, annual classes, regular reminders&lt;br&gt;- Including acceptable use (Internet/Email)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Question/What is it?</td>
<td>Typical Audit Findings</td>
<td>Why it is Important?</td>
</tr>
<tr>
<td>----</td>
<td>---------------------</td>
<td>------------------------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>
| 17 | **What do you have for wireless security?**  
- Limit wireless access  
- On a separate network  
- Best available encryption |  
- No encryption or weak encryption (i.e. WEP)  
- Rouge access points  
- 'On internal network'  
- No monitoring of activity  
- Data owners aren't notified of the risk |  
- It is the easiest way into your network |
| 18 | **Do you have application security?**  
- Security has layers  
- Don’t neglect application security |  
- Strong network controls weak ERP controls  
- Audit logs, access control, etc.  
- Data owners don’t know who has access to their data |  
- If you have a control failure you can still stop an attack  
- Network controls focus on external threats not internal  
- Internal fraud will probably include an application |
| 19 | **Do you manage mobile devices?**  
- Control what they connect to when not in your environment  
- Laptops, phones, USB devices  
- Encryption |  
- No control on what connects to your network  
- No protection if it is stolen |  
- Theft  
- Data leakage  
- Bring malware into your environment |
| 20 | **Are you PCI compliant?**  
- If you take credit cards in any way shape or form, you have to comply with the PCI Data Security Standard |  
- Finance thinks it is a IT issue  
- IT thinks it is a Finance issue  
- Not compliant |  
- There is a reason for the controls  
- Liability $$$ |
| 21 | **Do you have penetration tests?**  
- A validity test of the vulnerability scans  
- Typically finds other attack vectors |  
- Don’t know the difference between vulnerability scans and penetration tests  
- No penetration tests |  
- Validate vulnerability scans  
- Vulnerability scans are not 100% accurate |
| 22 | **Do you manage configurations?**  
- Hardware and software configurations  
- Laptops, servers, workstations, firewalls, switches, routers |  
- No standard build for configurations  
- No documentation  
- No validation (continuous monitoring) |  
- It is the one that slips through the cracks that is used by attackers |
| 23 | **Do you have proper data center environment controls?**  
- Safeguards hardware  
- Laptops, servers, workstations, firewalls, switches, routers |  
- No environmental monitoring controls (power, temperature, moisure)  
- No Uninterruptible power supply  
- No air conditioning |  
- Heat and power spikes can take out the servers |