## Recommended Security Assessment Frequencies

<table>
<thead>
<tr>
<th>Category</th>
<th>Audit Activity</th>
<th>Recommended Audit Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paths of Attack</td>
<td>Perform external vulnerability scan</td>
<td>Quarterly</td>
</tr>
<tr>
<td></td>
<td>Perform external application penetration test</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Conduct analog line wardueling</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Validate web content filtering</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Review DMZ service/servers</td>
<td>Annually</td>
</tr>
<tr>
<td>Software Patch-Level and Use Compliance</td>
<td>Perform software inventory and patch comparison</td>
<td>Quarterly</td>
</tr>
<tr>
<td></td>
<td>Review installed software and software license inventory</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Conduct rogue wireless access point scan</td>
<td>Quarterly</td>
</tr>
<tr>
<td></td>
<td>Review firewall configuration review (includes reviewing ALL firewall rules)</td>
<td>Quarterly</td>
</tr>
<tr>
<td></td>
<td>Evaluate internal network partitioning</td>
<td>Quarterly</td>
</tr>
<tr>
<td></td>
<td>Capture and review raw packets</td>
<td>Annually</td>
</tr>
<tr>
<td>Network Security Architecture</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure Best Practices Comparison</td>
<td>Conduct industry peer comparison</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Performs global IT architectural standards comparison</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Review encryption policy compliance</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Review key revocation procedure</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Review key store access management and inventory emergency key store</td>
<td>Annually</td>
</tr>
<tr>
<td>Encryption Usage and Key Handling</td>
<td>Review vendor and trusted partner access</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Validate external party access contracts and management approval for access</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Review trust-level dependencies and management</td>
<td>Annually</td>
</tr>
<tr>
<td>Trust-Level Dependencies and Management</td>
<td>Inventory all systems vs. systems with current, active virus protection</td>
<td>Quarterly</td>
</tr>
<tr>
<td></td>
<td>Conforms server and workstation virus signature updates</td>
<td>Quarterly</td>
</tr>
<tr>
<td></td>
<td>Conduct email antivirus / anti-spam effectiveness study</td>
<td>Quarterly</td>
</tr>
<tr>
<td>Virus Protection and Management</td>
<td>Review termination list vs. access removed, new hires vs. access granted</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Validate role separation between (production, dev, ... ) environments</td>
<td>Quarterly</td>
</tr>
<tr>
<td></td>
<td>Validate role separation for account provisioning function</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Review elevated privilege accounts</td>
<td>Quarterly</td>
</tr>
<tr>
<td></td>
<td>Review use of shared accounts (Administrant, root, Oracle, ...)</td>
<td>Quarterly</td>
</tr>
<tr>
<td></td>
<td>Validate demotion/management of production data sets process</td>
<td>Annually</td>
</tr>
<tr>
<td>Role/Function Segmentation and Access Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Access</td>
<td>Validate remote access is only via approved methods</td>
<td>Quarterly</td>
</tr>
<tr>
<td></td>
<td>Review remote access accounts</td>
<td>Quarterly</td>
</tr>
<tr>
<td>Password Policy and Use</td>
<td>Conduct brute-force password cracking</td>
<td>Quarterly</td>
</tr>
<tr>
<td></td>
<td>Evaluate password strength policy</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Review use of multi-factor authentication</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Evaluate administrative/highly privileged password freshness and storage</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Test lost password reset process</td>
<td>Annually</td>
</tr>
<tr>
<td>Organizational and Security Measures</td>
<td>Validate change and configuration management process compliance</td>
<td>Quarterly</td>
</tr>
<tr>
<td></td>
<td>Validate critical procedures documentation</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Inventory eDiscovery support tools</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Review IT security policy</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Validate management designation of security oversight responsibility</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Validate management acknowledgment of annual comprehensive IT security audit</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Review Information Security Program components</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Review integration of IT security criteria with organization's purchasing process</td>
<td>Annually</td>
</tr>
<tr>
<td>Physical Network and System Infrastructure</td>
<td>Conduct data center walkthrough</td>
<td>Daily</td>
</tr>
<tr>
<td></td>
<td>Perform server inventory and reconciliation</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Review data center physical access control system and users with DC access</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Review access control system for all IT infrastructure (UDE, MDF etc.)</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Conduct master physical key inventory/reconciliation</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Review console access and/or KVM concentrator access</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Check/maintain environmental management and monitoring</td>
<td>Monthly</td>
</tr>
<tr>
<td></td>
<td>Review media and retired equipment disposal practices</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Verify data backup procedures and perform data recovery test</td>
<td>Quarterly</td>
</tr>
<tr>
<td>Telecommunication Safeguards</td>
<td>Conduct telco circuit inventory/reconciliation</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Evaluate clear text vs. encrypted data sent externally</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Review voicemail, fax/efax security</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Review toll (“long-distance”) safeguards</td>
<td>Annually</td>
</tr>
<tr>
<td>Level and Methods of Ongoing Vigilance</td>
<td>Conduct incident response drill</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Review intrusion detection/prevention system effectiveness (event detection/reporting)</td>
<td>Quarterly</td>
</tr>
<tr>
<td></td>
<td>Review new IDS/IPS and systems/network monitoring events</td>
<td>Daily</td>
</tr>
<tr>
<td></td>
<td>Validate vulnerability announcement review process</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Review emerging technology evaluation process</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Manually review server, application, and device logs</td>
<td>Weekly</td>
</tr>
<tr>
<td></td>
<td>Inventory internal accessible hosts and services</td>
<td>Monthly</td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>Conduct formal review of organization's compliance with applicable regulatory standards</td>
<td>Annually*</td>
</tr>
<tr>
<td></td>
<td>Test disaster recovery and/or business continuity plan</td>
<td>Semi-Annually</td>
</tr>
</tbody>
</table>

*Some standards, such as PCI DSS, may require more frequent review.*