

CITADEL INFORMATION GROUP, INC.

Information Security Self-Assessment Management Checklist

This checklist is designed for Senior Management (President, CEO, CFO, or CIO) to quickly assess their organization's management of critical information assets.

Critical information assets include *critical* and *sensitive information* — financial information, customer lists, price lists, customer orders, manufacturing schedules, inventory levels, product specifications, trade secrets, proprietary information, intellectual property, and other confidential information — as well as the computer-communications systems in which they reside.

Securing critical information means (i) keeping it confidential, providing access only to those having a legitimate need for it, (ii) maintaining its integrity, assuring that all changes are authorized and intended and (iii) providing for its availability.

Critical information assets must be protected against attacks from ordinary hackers, industrial spies, and cyber-terrorists as well as from accidents or natural disasters that might disclose, damage, destroy critical information assets, or make them unavailable.

A robust information security posture is based on four imperatives: (i) protect information assets from attack; (ii) detect illicit attacks on information assets; (iii) quickly recover from attacks, accidents or natural disasters and (iv) comply with applicable security and privacy laws, regulations, and policies.

Question 1 of the checklist identifies one's need to manage the security of critical information assets. Questions 2 – 7 assess the general management of critical information assets while questions 8 – 13 assess the technical management of these assets. Questions 14 and 15 shift the emphasis from the management of critical information assets to the assurance of management effectiveness.

While every "No" answer to any of questions 2 – 15 is a cause for concern, the customary order for correcting information security weaknesses is to first manage the technology infrastructure (questions 8 – 13) and then turn attention to general management challenges (questions 2 – 7).

- | | Yes | No |
|--|--------------------------|--------------------------|
| 1. Does your organization's computer network contain sensitive or critical information? | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Do you have an executive responsible for managing the protection of critical information assets, is this person explicitly trained in information security, and have you allocated budget and resources for protection? | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Does the Board or Executive Management review the organization's information security posture at least semi-annually? | <input type="checkbox"/> | <input type="checkbox"/> |

	Yes	No
4. Has your organization documented information security policies consistent with its business needs, organizational structure, legal obligations, insurance policies, and risk management processes?	<input type="checkbox"/>	<input type="checkbox"/>
5. Is all <i>critical and sensitive information</i> explicitly identified as such and restricted to those having a “need to know?”	<input type="checkbox"/>	<input type="checkbox"/>
6. Are all employees and contractors provided regular ongoing information security training, including training in the safe handling of email and in password selection and protection, and are they held accountable for violations of security policy?	<input type="checkbox"/>	<input type="checkbox"/>
7. Have you coordinated your information security posture with customers, suppliers, and other trading partners whose computer systems you access or who access your computer systems?	<input type="checkbox"/>	<input type="checkbox"/>
8. Does your organization have documented recovery procedures to follow should a break-in, virus infestation or other security event occur?	<input type="checkbox"/>	<input type="checkbox"/>
9. Does your organization back-up all workstations and servers at least weekly, are multiple backups stored offsite, and are back-ups periodically tested to ensure the ability to restore data if necessary?	<input type="checkbox"/>	<input type="checkbox"/>
10. Has your organization’s <i>system architecture</i> been explicitly designed in accordance with network security principles and practices, including the use of firewalls?	<input type="checkbox"/>	<input type="checkbox"/>
11. Is virus protection software on all servers and workstations and is someone explicitly responsible for monitoring virus alerts and ensuring that virus protection is up-to-date?	<input type="checkbox"/>	<input type="checkbox"/>
12. Is someone explicitly responsible for monitoring security patches and alerts, and ensuring hardware and software systems are up-to-date and properly protected?	<input type="checkbox"/>	<input type="checkbox"/>
13. Is access to servers, routers, and other network technology physically restricted to those whose job responsibilities require access?	<input type="checkbox"/>	<input type="checkbox"/>
14. Would you know if someone was illegitimately accessing critical information assets?	<input type="checkbox"/>	<input type="checkbox"/>
15. Has your organization had an independent 3 rd - party information security vulnerability assessment or penetration test within the last 12 months?	<input type="checkbox"/>	<input type="checkbox"/>

Citadel Information Group ... Securing the critical information assets of middle market businesses, mid-sized government agencies, and the non-profit community. Contact us at info@citadel-information.com to schedule a free information security briefing.