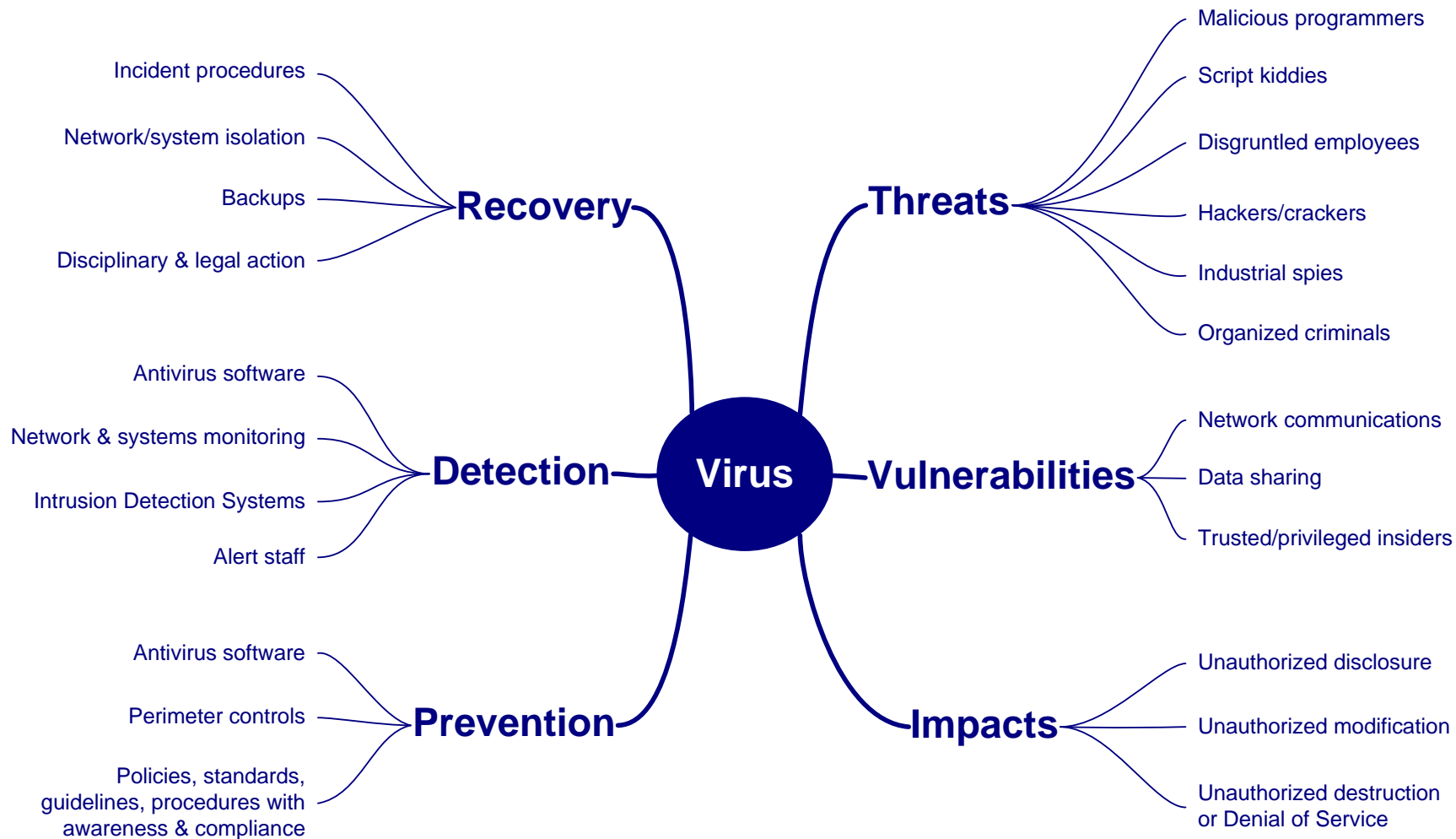




Controls review checklist – malware



Check	SWOT	Notes	Ref
1 Introduction			
1.1 Review other security awareness materials on malware for background information on the risks and expected controls.	<p><i>Note: the questions in this internal controls review checklist are intended more as general prompts or reminders than specific items to check. The checklist as supplied is generic and does not address your organization's specific requirements (e.g. privacy and other compliance obligations, business/strategic objectives) that are normally identified during the scoping phase of an independent audit or management review. It is unlikely to be sufficiently comprehensive without modification. It is intended for use by experienced IT auditors and similar competent persons. Use at your own risk. If malware is important to your organization, seek more specific advice and assistance from suitably qualified and experienced advisors with knowledge of your particular circumstances and obligations. This is NOT legal advice!</i></p> <p><i>The SWOT column and summary section are used to analyze and record significant findings that deserve management attention.</i></p> <p><i>The Ref column is used to reference evidence, policies, interview notes etc. collected and examined during the review.</i></p>		
1.2 Review the content of the organization's policies, standards, procedures and guidelines relating to malware. Assess whether they are, on the whole, reasonably up-to-date, comprehensive, consistent and usable. Have they been formally endorsed or mandated by management? Are there suitable mechanisms for dissemination, awareness and compliance?			
1.3 Consult colleagues in Information Security Management, IT Audit, Risk Management, Compliance etc. for background information and to identify any specific concerns or incidents relating to malware.			
2 Malware risks			
2.1 Risk assessment: how are malware risks (threats, vulnerabilities and impacts, including those shown on the mind-map) assessed and monitored by the organization? Is this an <i>ad hoc</i> or systematic process? Is it periodically reviewed and updated? Are responsibilities and accountabilities for actions arising suitably assigned?			
2.2 Risk management: having identified and assessed malware risks, how does the organization respond? Look for examples of changes to policies, technical controls etc. in response to malware risks.			
3 Antivirus controls			
3.1 Business issues: identify whether there has been a formal business decision, endorsed by senior management, regarding the licensing and use of antivirus (anti-malware) software and other antivirus controls. Are investment decisions like this revisited periodically to			

Check	SWOT	Notes	Ref
<p>ensure the controls remain appropriate to the risks? Review the investment business case (if available). Does the organization's approach to malware control still make good commercial sense?</p>			
<p>3.2 Technical architecture: review documentation describing the organization's antivirus software. Review the choice of antivirus software <i>e.g.</i> does the architecture incorporate multiple antivirus vendors and cover all relevant platforms/operating systems? Are suitable deployment, management and monitoring mechanisms/procedures specified and documented? Are all relevant platforms covered, including PDAs and smart phones?</p>			
<p>3.3 Implementation: discuss the implementation, configuration, management, maintenance, updating and monitoring of antivirus software with relevant IT support people. Tease out any practical issues, constraints or concerns, such as platforms that cannot be protected, systems that cannot be frequently updated <i>etc.</i> Review a sample of systems representing a range of platforms/operating systems (including desktops, email and other application servers and portables for example) to confirm whether the antivirus software is running correctly and has been updated recently. If possible, validate any central antivirus monitoring and reporting capabilities. Does the central system accurately report the specific systems assessed?</p>			
<p>3.4 Testing: how, by whom and when is the antivirus system tested? In conjunction with Information Security Management, consider seeding selected systems with the EICAR antivirus test file to check that antivirus software correctly detects it, raises warnings and initiates appropriate corrective action. If user desktops, laptops <i>etc.</i> or servers are 'infected' with EICAR, track the proportion that are properly reported by users as malware</p>			

Check	SWOT	Notes	Ref
incidents.			
<p>3.5 Documentation and awareness: review any policies, user guides, guidelines, briefings, intranet pages and any other user and technical awareness, training or educational materials relating to the virus/malware issue. Are they professionally presented, up-to-date and useful? Are they sufficiently comprehensive, clear and explicit to give unambiguous directions to users and IT support staff, especially in the event of a malware incident? Are they officially endorsed or mandated and supported by management? Also review the dissemination and use of malware awareness/training/educational materials in practice. Do they reach all relevant people in the organization? Do they engage the audience/s and secure their support for/use of the malware controls? Are there information security management professionals who monitor the malware threat environment and respond appropriately to new threats as they emerge? Seek examples.</p>			
<p>3.6 Backups: assess how comprehensive and up-to-date are system backups. Check that sufficient backup cycles and original installation media are retained to enable restoration to a known clean state in case a rootkit or similar cryptic form of malware may have infected the system some while before it was detected.</p>			
<p>3.7 Malware incidents: investigate/review a sample of actual malware incidents using records, post-incident reports <i>etc.</i> from the IT Help/Service Desk and/or antivirus response team, and by discussing the incidents with users affected. Determine whether the incidents were well managed, promptly and efficiently resolved, and whether any improvement lessons have been implemented in practice (not just 'recommended for future action'). Look out for any examples of malware incidents that were not handled through the accepted virus incident</p>			

Check	SWOT	Notes	Ref
management procedures, and for any other exceptions to the agreed processes (exceptions <i>may</i> be justified but should not just happen by accident or omission). Was disciplinary or legal action ever taken against those responsible?			
4 Other malware issues			
4.1 Other forms of malware: given that malware is often used to spread adware, spyware, 419 advance fee frauds and related scams such as phishing, keyboard loggers and so forth, assess the extent to which these and other threats are covered by the organization's security controls. Are controls such as independent code reviews, reliable software and data backups, clued-up and alert technical support staff <i>etc.</i> in place and reasonably effective in practice? Watch out for any examples of actual malware incidents along these lines that were not well covered by the conventional antivirus controls. Even if there appears to have been no such incidents to date, assess the likely risk given that these are common real-world threats.			
4.2 Logic bombs, trapdoors, covert channels <i>etc.</i>: are managers (especially IT managers) aware of the threat of malicious acts by disgruntled employees/users with privileged systems access, such as the insertion of logic bombs? Review the controls to prevent and detect such incidents e.g. code reviews, change controls and divisions of responsibility. Do similar controls apply to code developed externally for the organization under contract? Consider also the possibility of malware-infected systems sending out confidential data through the network: are intrusion detection systems configured to identify such connections? Have any been found?			
4.3 Miscellaneous: this section can be used to raise other issues or concerns about malware that don't fit into the previous sections. Identify here any loose ends,			

Check	SWOT	Notes	Ref
nagging doubts, things that perhaps ought to be investigated further the next time this area is reviewed and issues that were not sufficiently confirmed by the evidence to make it into the present report yet at the same time were not totally discounted by the evidence.			
5 Conclusion			
5.1 SWOT summary (main items only): Strengths: Weaknesses: Opportunities: Threats:			
5.2 Overall conclusions & key issues:			
5.3 Recommendations:			
*** End of checklist ***			