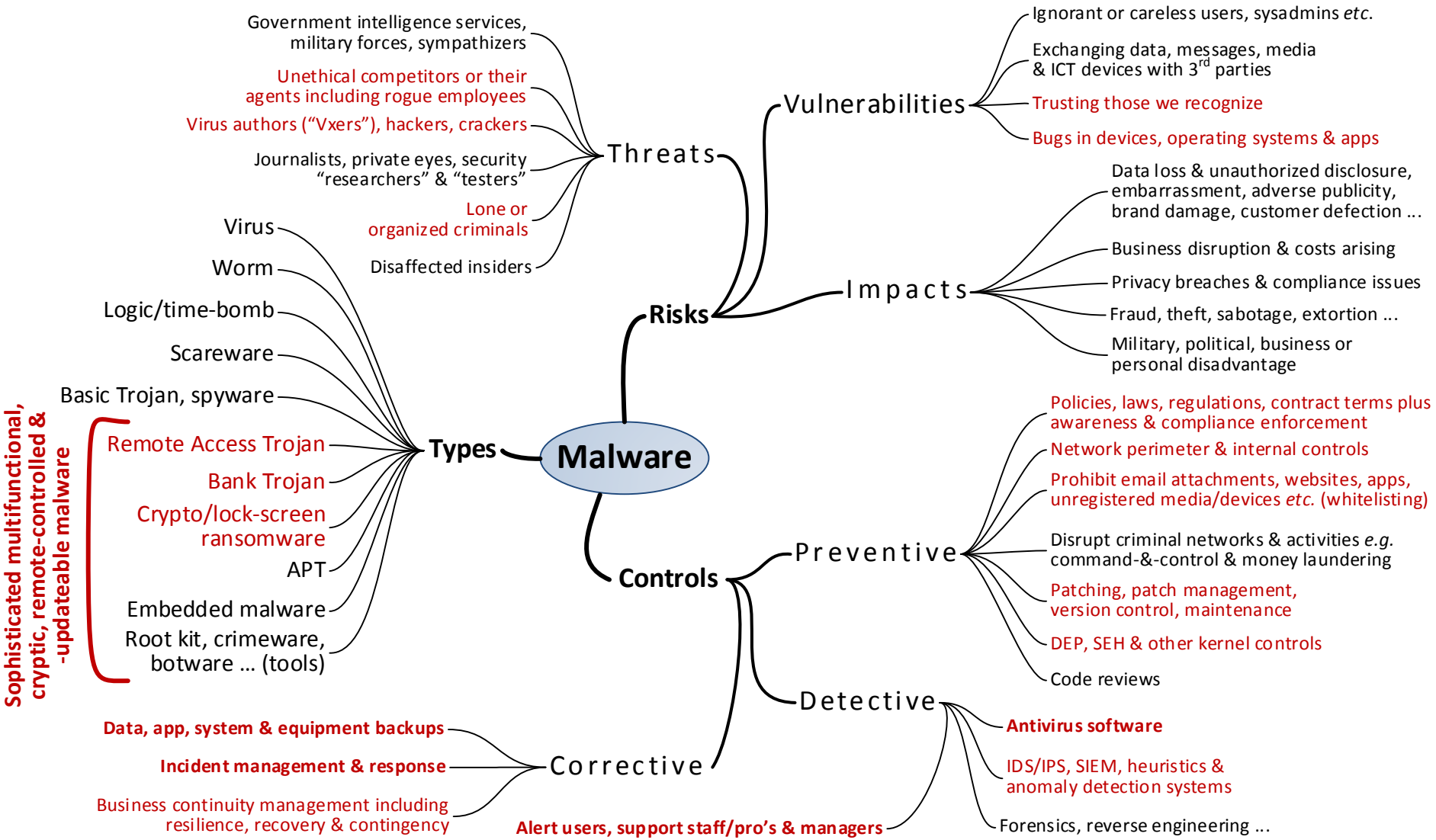
Malware *Internal Controls Questionnaire*



Check	SWOT	Notes	Ref
1 Introduction			
1.1 In order to customize and elaborate on the generic ICQ, research the risks and controls typically relating to malware. Read the other security awareness materials.	*The checks in this ICQ/checklist are general prompts to get you started, not a definitive set of specific questions to ask. This is not a script but a generic template that does not directly address your organization's issues and requirements (e.g. compliance obligations, business/strategic objectives). It is meant to be customized and used sensibly by experienced, competent reviewers or auditors.* ***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 neither legal nor information security advice!***		
1.2 Consult professional colleagues in Information Security, IT Audit, Risk Management, IT, PC/Tech Support, Help Desk *etc*. for background information and to identify any specific concerns or recent incidents involving malware with or affecting the organization and its peers.			
2 General malware controls			
2.1 **Malware risks**: review the corporate risk register (or equivalent) to determine whether malware has been appropriately analyzed and rated/ranked against other information security risks and other business risks. Does the risk description adequately reflect the current situation with bank Trojans, ransomware, mobile malware, data-stealing malware, APTs, multifunctional remote-controlled malware and malware in IT systems at source?	*Does this row represent a* ***S****trength,* ***W****eakness,* ***O****pportunity or* ***T****hreat?*	*Describe your findings here, succinctly. Distinguish facts supported by evidence from presumptions, opinions and conjecture.*	*Reference your evidence here*
2.2 **Malware strategy**: review the organization's strategy towards malware, including aspects such as: monitoring and responding to changing risks; investing appropriately in prevention, detection *and* correction; proactively managing and maintaining antivirus, network security, backups and business continuity arrangements; avoiding 'technical monoculture' (*e.g*. deliberately using a mix of UNIX- and Windows-based systems); isolating network domains to limit outbreaks; and proactively learning from malware incidents.			

Check	SWOT	Notes	Ref
2.3 **Malware policies**: review the organization's policies, standards, procedures and guidelines relating to malware, network and system security, incident and business continuity management. Determine whether they are reasonably up-to-date, comprehensive, consistent and usable. In particular, check whether employees are explicitly forbidden from disclosing malware or other information security incidents outside the organization unless authorized.			
2.4 **Training and awareness**: review the training and awareness activities associated with malware and other relevant policies, procedures *etc*. Does the awareness program cover all applicable topics and aspects and all applicable audiences? Is it both informational *and* motivational? How well is it working in practice [consider using an awareness maturity metric]? Does the awareness program adequately cover new/emerging malware-related risks such as ransomware and bank Trojans?			
2.5 **Antivirus software**: review the organization's use of antivirus software. Check the requirements specification and the process for selecting suitable package/s (possibly different ones on desktops, mobiles, servers *etc*.). Are all relevant devices running up-to-date antivirus? How does the organization handle BYOD, IoT and other devices that may not be regularly networked? How, by whom and when are antivirus updates tested, especially before updating business- or safety-critical systems?			

Check	SWOT	Notes	Ref
2.6 **Antivirus management**: review the arrangements to manage antivirus software across the entire portfolio of IT systems. How are signature file updates and antivirus patches received, tested and implemented in practice? Check the management console for appropriate monitoring and metrics. Confirm whether patches and sig file updates are staggered across different groups of systems, allowing time to confirm that there are no untoward consequences (such as patch failures/conflicts and perhaps hackers' use of the rollout mechanism to distribute malware!).			
2.7 **Data backups**: review the backup arrangements for all IT systems (including servers, desktops, mobile devices and BYOD). Are there regular offline backups of hard drives, network drives, cloud storage and so forth? Has the backup regime been professionally specified and designed, proven by suitable testing, and subject to strict change control? Are sufficient backup cycles retained to recover from cryptic malware infections that are not immediately recognized as such, just in case recent backups are unusable due to being infected or encrypted?			

Check	SWOT	Notes	Ref
2.8 **Hardware and firmware backups**: if the organization suffers a particularly nasty and widespread malware incident that simultaneously renders numerous IT systems unusable, can sufficient suitable replacement hard drives, firmware *etc*. be obtained at short notice? In particular, assess the arrangements for business- and safety-critical systems and bespoke hardware. Are all relevant firmware images properly backed up/archived in practice? Is there a management process?			
2.9 **Containment**: explore the manner in which suspected malware outbreaks are rapidly identified and contained/isolated pending further analysis. Evaluate the effectiveness of the process using evidence concerning actual invocations, tests and exercises (if there are none, raise that as a significant threat!). Is there a suitable blend of automated and manual activities? Is the organization truly capable of escalating and expediting the response to malware-related incidents that rapidly expand in scope or severity? Are additional internal and external resources available if needed (begging questions about how information security incidents are dynamically prioritized relative to ongoing business activities by management).			

Check	SWOT	Notes	Ref
2.10 **APT (Advanced Persistent Threats) and embedded malware**: assess the extent to which management has considered and appreciates the severity of APT and embedded malware risks and the significance of such attacks *if* the organization is ever targeted. Is there a rational strategic approach to treating the risks? Does someone appropriate "own" the risks, and do they actively monitor this fluid situation? Is there a mechanism for escalating matters urgently to senior management if the risks change markedly (*e.g.* if other organizations in the same industry admit to having been compromised, if equipment vendors or third parties disclose embedded malware, if threats are received, or if business opportunities are lost due to otherwise unexplained information leakage or cybertage)?			
3 Network and system security controls			
3.1 **Intrusion detection/prevention**: assess the extent to which firewalls, IDS/IPS, network logging and monitoring *etc*. are capable of detecting and preventing worms and other network malware incidents. In particular, consider the risk of cryptic/covert malware including APTs and embedded malware using low-and-slow mechanisms and encryption for command and control purposes, and to exfiltrate valuable information. Review actual malware incidents to determine how well the security systems worked in practice. If there have apparently been none, poke harder at the malware identification aspects: is evidence of actual worms, Trojans *etc*. not being collected? Are the warning signs being neglected? Or is it really credible that there have been no such incidents?			

Check	SWOT	Notes	Ref
3.2 **Network segmentation**: review the network security architecture for evidence that markedly different classes or types of traffic are logically and/or physically segmented, with strict access controls being applied at any contact points (*e.g.* various types of firewall, VLANs). Consider the risks of different types of malware infecting multiple segments, and determine whether the controls are truly adequate to prevent widespread infections. In particular, check that links to security devices, plus security logs and other security traffic, are well-secured to prevent hackers (further!) compromising network security.			
3.3 **System segmentation**: review the system security architecture for evidence that markedly different classes or types of system are logically and/or physically segmented, with strict access controls. Pay particular attention to (a) the protection of security-relevant systems such as those used to manage, monitor and configure security, make backups, collate and report on security logs, authenticate users, issue digital certificates, detect intruders *etc*., with additional controls such as dual-factor authentication for privileged accounts; and (b) hardening of critical servers and applications. If hackers have somehow gained a foothold in the network, what stops them successively compromising additional systems up to and including the security management systems? How will they be detected and tackled? **Can you be certain that hackers and malware are not already at large on the network, right now?**			

Check	SWOT	Notes	Ref
3.4 **Security logs:** review the arrangements for collecting, analyzing, reporting and acting on security logs, alarms, alerts and other automated security reporting. Review the metrics. Look in more detail at events/incidents that have been identified and addressed using logs *etc*. to check the efficiency of the process. Review a sample of logs *etc*. for suspicious events that have not been identified as such and/or addressed to check the effectiveness of the process. Focus especially on logs *etc*. relating to security and other high-risk systems, such as important business servers: are events suitably prioritized?			
3.5 **Source code reviews**: if there is a genuine risk of malware being deliberately introduced in bespoke or commercial software (including patches and drivers), firmware or hardware, determine whether code reviews, testing, configuration management controls *etc*. are adequate to block such attacks.			
4 Incident and business continuity management			
4.1 **Malware-related incident management**: review the arrangements to identify, report, respond/react, investigate, recover and learn from malware-related incidents. Look for 'improvement opportunities' that seem to have fallen-between-the-cracks and been forgotten. Check that (where applicable) action plans have been completed, and necessary improvements have been implemented and proven, focusing especially on business- and safety-critical systems and networks.			

Check	SWOT	Notes	Ref
4.2 **Forensics**: does the organization have the capability to conduct forensic investigations following major incidents? If not, are there contractual arrangements in place to obtain the requisite expertise on demand, most likely at short notice? Either way, check their competence, skills, training records *etc*., preferably by reviewing their performance on actual malware incidents.			
4.3 **Business Impact Analysis**: confirm whether a comprehensive BIA has assessed the availability requirements for all business processes (implying a comprehensive inventory of the processes and supporting/enabling infrastructure) on an even-handed, methodical basis. Is the BIA actively maintained and up-to-date? Check whether recent business and IT changes have been duly reflected in the BIA and continuity arrangements.			
4.4 Business continuity: check whether suitable business continuity arrangements are in place, especially for the business- and safety-critical processes and infrastructure (*e.g*. using high-availability, redundant and resilient IT systems with automated failover and disaster recovery arrangements, managed through teamwork rather than by individuals). Have they been appropriately tested? Are they actively maintained? Are regular exercises held?			
4.5 **Miscellaneous**:		*Are there other issues or concerns about malware that don't fit into the previous sections? Identify loose ends, nagging doubts, things that perhaps ought to be investigated further the next time this area is reviewed …*	

Check	SWOT	Notes	Ref
5 Conclusion			
5.1 **SWOT summary (main items only)**: **Strengths**: **Weaknesses**: **Opportunities**: **Threats**:			
5.2 **Overall conclusions & key issues**:			
5.3 **Recommendations for management**:			
*** End of ICQ ***			