



Controls review checklist – authentication

Check	SWOT	Notes	Ref
1 Introduction			
1.1 Review other NoticeBored awareness materials on identity theft, authentication, integrity, access controls <i>etc.</i> for background information.			
1.2 Review the content of the organization's policies, standards and procedures relating to authentication. Assess whether they are reasonably up-to-date, comprehensive, consistent and usable. Have they been formally endorsed/mandated by management? Are there suitable mechanisms for dissemination, training and awareness?			
1.3 Consult colleagues in Information Security Management, IT audit, SOX <i>etc.</i> for background information & to identify any specific concerns relating to authentication of individuals (users, employees, system administrators, customers <i>etc.</i>), systems, networks, programs, patches and updates <i>etc.</i>			
1.4 Note: many of the tests in this checklist are best performed using automated security audit tools to examine large numbers of user ID records <i>etc.</i> If you have access to such tools, take time to familiarize yourself with their capabilities, commands and limitations, perhaps using a test or standalone system.			
2 User authentication (login)			
2.1 User IDs: review user ID records on a selected sample of systems for evidence of: invalid user IDs; default user IDs;			

Check	SWOT	Notes	Ref
<p>redundant or dormant user IDs; duplicate user IDs; shared userIDs; and other similar issues. Pick a range of types of system as inadequate authentication processes even on “low risk” systems may still permit unauthorized access to the network.</p>			
<p>2.2 User ID allocation processes: review the processes for allocating new user IDs to new users, for determining and setting appropriate system access rights, and for withdrawing access rights when people move locations/departments or leave the company. Are there suitable emergency processes to cancel access promptly if people are dismissed? How are temporary and shared user IDs controlled? Are there special authorization and/or authentication processes for privileged user IDs, access to especially sensitive systems/functions <i>etc.</i>? Are they adequate?</p>			
<p>2.3 eCommerce user authentication: review arrangements to authenticate remote users of eCommerce facilities. Look for examples of authentication failures, frauds <i>etc.</i> and determine whether the controls are adequate to identify such failures and minimize the risk.</p>			
<p>2.4 Other remote user authentication: review the suitability of arrangements to authenticate and control access by dial-in users, wireless networkers <i>etc.</i> e.g. VPNs. Are there special controls to limit remote privileged access?</p>			
<p>2.5 Phishing and identity theft controls: review the organization’s controls to limit the risks associated with phishing and identity theft. If a phisher targeted the organization’s customers, how would the organization identify and respond to the attack? Have there been any such incidents? How effective have the controls been in practice?</p>			

Check	SWOT	Notes	Ref
3 Physical access controls			
<p>3.1 Site access control processes: review arrangements to issue and control staff passes, visitor passes <i>etc.</i> Are staff members, managers, visitors, maintenance workers, IT support engineers <i>etc.</i> all adequately authenticated when passes are issued? Are passes adequately checked when people arrive at sites? What about when they are wandering on-site, or leaving site with corporate equipment <i>etc.</i>? Are the controls equally effective at all hours including overnight and holidays?</p>			
<p>3.2 Monitoring site access: review systems and processes for monitoring physical access to corporate sites and sensitive facilities, including intruder alarms, card pass systems, CCTV <i>etc.</i> Assess the effectiveness of these controls to identify and respond to possible intruders. Look for evidence relating to the operation of these controls (<i>e.g.</i> security logs).</p>			
<p>3.3 Site access tests: determine whether 'physical penetration tests' are ever conducted. If so, check the reports to assess the status and to assess the extent and quality of testing performed. If not, consider undertaking such tests yourself, or commissioning such tests from a competent and trusted third party (<i>be extremely careful to obtain explicit [clearly documented] permission from senior management before commencing such tests!</i>).</p>			
<p>3.4 Site penetration: imagine you are intent on obtaining unauthorized physical access to the site. How might you get in? How far would you be able to get without being challenged? Consider preparing an case-study/demonstration for senior management, perhaps using a stills or video camera to gather evidence.</p>			

Check	SWOT	Notes	Ref
4 Logical access controls			
4.1 Logical access: review logical access controls on a selection of systems. Determine broadly speaking whether controls are effective at all levels including access from/to the network, system, applications and data.			
4.2 Authentication and access: look specifically at the relationship between authentication of users or programs and access to data. Are there any realistic situations you can foresee which could lead to unauthorized access? Are user access rights determined by managers using defined user rôles, for example, and are those rôles appropriate? Are access rights, rôles and users-in-rôles routinely reviewed by management? Examine any evidence of recent checks to determine the effectiveness and extent of checks performed. Have any issues been fully resolved?			
5 Data validation controls			
5.1 Manual data entry controls: review manual data entry validation controls for a sample of systems, especially systems accepting critical information that ends up being part of, or heavily influencing, vital corporate information systems (such as financial accounting systems, sales and procurement systems <i>etc.</i>).			
5.2 Automated data entry controls: review validation controls for automated system interfaces for a sample of systems, especially systems accepting critical information that ends up being part of, or heavily influencing, vital corporate information systems (such as financial accounting systems, sales and procurement systems <i>etc.</i>) [note: there may be Sarbanes-Oxley Act implications for these systems and controls].			

Check	SWOT	Notes	Ref
5.3 Development of data validation controls: review broadly how data validation controls are specified, designed, developed and tested. Look for evidence (such as security design documentation) on a small selection of key systems. Are automated tests employed?			
5.4 eCommerce data validation: review the data validation controls for eCommerce and similar Internet-accessible systems. Look especially for evidence of suitable range and type validation, and for controls against SQL injection, cross-site scripting and other forms of attack.			
6 Conclusion			
6.1 SWOT summary (main items only): Strengths: Weaknesses: Opportunities: Threats:			
6.2 Overall conclusions & key issues:			
6.3 Recommendations:			
*** End of checklist ***			