Security Audits and Scans (Independent Verification)

Security Audits and Scans (Independent Verification)

Why is this Important:
This type of provision allows institutions of higher education to periodically audit their contracting third parties to ensure that the third party is adhering to contract terms and following industry best practices regarding information security. This helps to protect the institution's data and may offer the institution an avenue to pursue early contract termination if the contracting third party is not meeting stated contractual terms regarding information security.

Reference:
Appendix 1 ISO/IEC 27002:2005, Reference 6.2.3(b); (n) ; (o)

Overview:
Many examples had terms that required the third party vendor to submit to an external compliance audit, penetration test, or external security scan upon request of the originating institution.

Criticality: Category 3 and Category 4.

Sample RFP Language:

1. Has the Proposer undergone and would be willing to provide the results of a Statement on Standards for Attestation Engagements (SSAE) No. 16 (formerly SAS 70) audit, or equivalent independent security audit, to attest to the strength of the Proposer's security practices and procedures? If Proposer objects to providing the audit results, Proposer must, as part of its proposal, identify and describe in detail the reasons for Proposer's objection.
2. If the Proposer were to be selected, would the Proposer agree to a vulnerability scan [penetration test performed by Institution or a party of its choosing of all systems that would interact with the service proposed including any systems that would hold, process, or from which Institution data may be accessed? If Proposer objects to the vulnerability scan [penetration test], Proposer must, as part of its proposal, identify and describe in detail the reasons for Proposer's objection.

#Top

Sample Contract Clauses:

1. [Vendor] agrees to have an independent third party (e.g. Cap Gemini Ernst & Young, Deloitte & Touché, or other industry recognized firms) security audit performed at least once a year. The audit results and [Vendor]'s plan for addressing or resolving of the audit results shall be shared with the Institution within XX (X) days of the [Vendor]'s receipt of the audit results. The audit should minimally check for buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, SQL injection vulnerabilities, and any other well-known (published on bugtraq or similar mailing list) vulnerabilities.
2. The Institution reserves the right to require [Vendor] to provide the results of an audit of security policies, practices, and procedures on an annual or biennial basis. This audit must be performed by a third-party approved by the Institution.
3. The Institution reserves the right to request the results of a vulnerability scan for the [Vendor]'s production environment. Production environment is here defined as all systems that interact with the service contracted for herein including any systems that hold, process, or from which Institution data may be accessed. A vulnerability scan is defined as a scan by a network vulnerability scanner such as Nessus or ISS.
4. The Institution reserves the right to request the results of a formal penetration test. A penetration test is here defined as "the process of using approved, qualified personnel to conduct real-world attacks against a system so as to identify and correct security weaknesses before they are discovered and exploited by others." See http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_04_appx_b_glossary.html
5. Institution and, if the applicable contract or grant so provides, the other contracting party or grantor (and if that be the United States, or an agency or instrumentality thereof, then the Controller General of the United States) shall have access to and the right to examine any pertinent books, documents, papers, and records of [Vendor] involving transactions and work related to this Agreement until the expiration of five years after final payment hereunder. [Vendor] shall retain project records for a period of five years from the date of final payment.
6. The Institution reserves the right to perform audits at their expense to the extent necessary to ensure compliance with the terms of this Agreement. [Vendor] agrees to reasonably cooperate in the performance of such audits.

#Top

special conditions

Questions or comments? Contact us.