14.4. Software Application Development

Objective

14.4.1. Secure programming methods and testing are used for application development in order to minimise the number of coding errors and introduction of security vulnerabilities.

Context

Scope

14.4.2. This section covers information relating to the development, upgrade and maintenance of application software used on agency systems.

References

14.4.3. Additional information relating to software development is contained in:

Reference	Title	Publisher	Source
ISO/IEC 27001:2013	**A.12.5, Security in Development and Support Processes**	ISO	https://www.iso.org/standard/54534.html
	OWASP Secure Coding Practices - Quick Reference Guide	OWASP	https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
	Secure Code Review	MITRE Corporation	https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/secure-code-review
	Build Security In	DHS – US-CERT	https://www.us-cert.gov/bsi
	Application Security - Application Security & Development A To Z	US Defense Information Security Agency (DISA)	http://iase.disa.mil/stigs/app-security/app-security/Pages/index.aspx
	Writing Secure Code - Michael Howard and David LeBlanc	Microsoft Press	ISBN Book 978-0-7356-1722-3 ISBN eBook 978-0-7356-9146-9

Rationale & Controls

Software development environments

14.4.4.R.01. **Rationale**

Recognised good practice segregates development, testing and production environments to limit the spread of malicious code and minimise the likelihood of faulty code being put into production.
Limiting access to development and testing environments will reduce the information that can be gained by an attacker.

14.4.4.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1635]

Agencies SHOULD ensure that software development environments are configured such that:

- there are at least three separate environments covering:
  - development;
  - testing; and
  - production.
- information flow between the environments is strictly limited according to a defined and documented change policy, with access granted only to system users with a clear business requirement;
- new development and modifications only take place in the development environment; and
- write access to the authoritative source for the software (source libraries & production environment) is disabled.

Secure programming

14.4.5.R.01. **Rationale**

Designing software to use the lowest privilege level needed to achieve its task will limit the privileges an attacker could gain in the event they subvert the software security.

14.4.5.R.02. **Rationale**

Validating all inputs will ensure that the input is within expected ranges, reducing the chance that malicious or erroneous input causes unexpected results.

14.4.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1639]

Agencies SHOULD ensure that software developers use secure programming practices when writing code, including:

- designing software to use the lowest privilege level needed to achieve its task;
- denying access by default;
- checking return values of all system calls; and
- validating all inputs.

Software testing

14.4.6.R.01. **Rationale**

Software reviewing and testing will reduce the possibility of introducing vulnerabilities into a production environment.

14.4.6.R.02. **Rationale**

Using an independent party for software testing will limit any bias that can occur when a developer tests their own software.

14.4.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1643]

Software SHOULD be reviewed or tested for vulnerabilities before it is used in a production environment.

14.4.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1644]

Software SHOULD be reviewed or tested by an independent party as well as the developer.

14.4.6.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1645]

Software development SHOULD follow secure coding practices and agency development standards.