Secure Software Design Standard

CWB Financial Group – Information Security Office

Document Version – V1.0

May 27, 2020

CWB Financial Group

Contents

Document Summary

Brief Overview

CWBFG requires software development to incorporate information security activities at every phase of the system development lifecycle.

Secure software development contributes to the reliability of the information technology environment by ensuring software-based vulnerabilities are identified and remediated during development stage well in advance of the application being deployed into the production environment. Software development may be conducted by either/or internal and external entities that use a variety of software development methodologies. CWBFG expects that these methodologies align with this standard and Open Web Application Security Project (OWASP) Secure Coding Practices.

As per the CWBFG ***Information Security Logical Architecture***, this standard supports the following principles:

- Zero Trust
- Defense in Depth
- Protection of Information Assets
- Assurance of Correct and Reliable Operation
- Defense Against Threats

Purpose

This standard provides the security requirements for new system development, code enhancements and/or code reuse scenarios; and ensures information security is designed and implemented within the development lifecycle for all CWBFG information systems.

Scope

This standard applies to all individuals who use, provision, and support CWBFG's technology assets, regardless of where these assets are located (e.g. Corporate or Cloud Service Providers). This also applies to authorized third parties who use or provide services, manage, or support CWBFG's technology assets.

Out of Scope

This standard does not include any specifics on how to write secure code. Instead, it is advised that developers leverage trusted development sources available over the Internet (e.g. OWASP, SANS, etc.)

Standard Statements

Security in Development and Support Process

CWBFG requires all developers of the information systems, system components, or information system services to follow a documented development process that: (SA-15)

- explicitly addresses security requirements;
- identifies the standards and tools used in the development process;
- documents the specific tool options and tool configurations used in the development process; and
- documents, manages, and ensures the integrity of changes to the process and/or tools used in development;

General Requirements

- Based on the classification of the information that is to be used, processed and stored in the new system, the design must provide for appropriate security features to be available, as defined in the ***Information Classification Standard*** and the ***Data Protection Standard***.
- CWBFG Information Owners and Application Services must ensure:
  - secure software development techniques are used for new developments and in code enhancements or code reuse, such as API scenarios. Rules for the development of software and systems must be applied consistently to all development efforts;
  - software and systems developed for CWBFG's use follow a set of secure development processes and apply them consistently;
  - developers are trained for secure coding best practices, standards and testing;
  - code review are perform to confirm source code is secure, prior to implementation into production; and
  - source code downloaded from open source websites (e.g. GitHub, Source forge etc.) are reviewed for any backdoors, copyright infringement or misalignment with this standard.
    - Source code analysis tools, vulnerability scans and penetration testing can be used to identifying any insecure code (See the Software Testing section for more details).

Security in the Software Development Lifecycle

Information security requirements must be incorporated into the software development lifecycle stages. The following sections highlight the information security requirements for each stage.

Business Requirements Specification

- The focus within the business requirements stage is on the functionality of the system. This is expressed in business terms rather than technical requirements and can be linked back to the business need for the system. The business is uniquely placed to give a clear understanding to the development team of the security requirements of the information that the new system will hold and process.
- The business requirements must specify:
  - who the Information owner is, their opinion of the value of the information to the business and the impact to the business if there is a loss of confidentiality, integrity and availability;
  - the classification of the system and/or information asset, as per the ***Information Classification Standard***;
  - the anticipated use cases, where access will be made from (internal, external or both) and any legal, regulatory environment the system must operate within, or any contractual obligations.
- A risk assessment must be performed by the Information Security Office GRC team as part of the project to ensure that the implications of the above issues are fully understood by all parties.

Preparing the Development Environment

- Prior to developing code, a secure development environment must be established for the project.
  - All development work must exhibit a separation between production, development, and test environments, and at a minimum have at least a defined separation between the development/test and production environments unless prohibited by licensing restrictions or an exception is approved.
  - These separation distinctions allow better management and security for the production systems, while allowing greater flexibility in the pre-production environments.

- Development teams must protect Production information systems by:
  - establishing Security Zones to separate production environments from test and development environments;
  - preventing the use of test and development identities and credentials for Production information systems. Testing must not be performed on Production systems;
  - storing source code (or equivalent) in a secure location away from the Production environment and restricting access to authorized individuals. Rules for code release must be documented;
  - preventing access to compilers, editors and other tools from Production information systems;
  - using approved change management processes for promoting software from development/test to Production information systems; and
  - prohibiting the use of Production information in development, test or training information systems, unless equivalent controls are implemented as documented in ***Data Protection Standard***.

Secure Development Environment

- A risk assessment must be performed by the Information Security Office GRC team to assess the risks associated with individual system development efforts and establish secure development environments for system development. Considerations include, but are not limited to the:
  - sensitivity of data to be processed stored or transmitted by the system;
  - applicable external and internal requirements (e.g., from regulations, policies and standards);
  - need for segregation between different development environments;
  - existing security controls which support system development;
  - trustworthiness of individuals working in the environment;
  - degree of outsourcing associated with system development;
  - access controls for the development environment;
  - monitoring for changes made to the environment and source code stored therein;
  - backup storage requirements; and
  - controls used to protect information transmitted to and from the environment.

Secure Development

- Depending on the coding environment, languages, databases, tools and other components selected, secure coding and configuration guidelines must be adopted. These guidelines must be evaluated to ensure they provide adequate protection from the various types of potential risks identified in the risk assessment.
- Other requirements that will need to be determined include the:
  - secure coding guidelines for each programming language to be used;
  - security checkpoints within the development milestones;
  - secure source code repositories;
  - security in the version control and updates; and
  - required application security knowledge.

Application Program Interface (API) Security

- The role of APIs in modern application infrastructure is to provide authentication and access and therefore it has become essential to keep these APIs secure. Please refer ***API Security Guidelines*** for more detailed requirements.

Software Testing

- Software Testing means an activity to check whether the actual results match the expected results to provide stakeholders with information about the quality of the software product or service under test. Software testing can also provide an objective, independent view of the software to allow the business to appreciate and understand the risks of software implementation. Test techniques include the process of executing a program or application with the intent of finding software bugs (errors or other defects), and verifying that the software product is fit for use. From Security perspective, Information Owners must:
  - ensure new, upgraded or enhanced systems undergo thorough testing and verification during the development processes.
    - A detailed schedule of test activities, inputs and expected outputs under a range of conditions must be prepared as part of testing and verification processes.
    - Where technically feasible, testing should be performed in a realistic test environment.
    - Testing should also extend to receive components and integration access points with other systems.
  - ensure development acceptance testing include testing of information security requirements and adherence to secure system development practices.
  - ensure test data used follows the requirements detailed in the ***Data Protection Standard***;
  - determine the level of testing required, based on the classification and categorization of the system.
    - Internet facing systems must be fully tested by independent third parties for vulnerabilities and fully remediated prior to deployment into Production.
  - determine timing and frequency of running independent vulnerability assessment to detect defects in application code;
  - consider the expertise level of the developer has for avoiding, finding and fixing vulnerabilities. Use of source code analysis tools that assist with finding known vulnerabilities. Two common types of analysis tools include:
    - Static Application Security Testing (SAST) tools are used early in the software development process to test the application from the inside out (white box testing tools) and do not require a running system to perform the evaluations. These tools test the source code, the byte code or the binaries line by line to expose weaknesses in the software before it is deployed. By detecting the flaws in the code early in the process, weaknesses can be fixed before hackers detect them.
    - Dynamic Application Security Testing (DAST) is performed from the outside looking in. It is a process that takes place while the application is running and it tries to penetrate the application in a variety of ways to identify potential vulnerabilities, including those outside the code and in third-party interfaces.

Security in Outsourced Development

- When system development is outsourced, development activities must be supervised, managed and the delivered solution must meet the requirements defined in the system development agreement.
- The Information Owner must obtain assurance that the external party complies with these following rules for secure development:
  - Outsourced development must follows the same steps used for in-house development efforts, including:
    - licensing arrangements, code ownership, and intellectual property rights to the outsourced content;
    - quality and security functionality of the information system including the requirements for secure design, coding and testing practices;
    - testing requirements for the information system and/or application code to identify any common vulnerabilities and/or malicious code, prior to deployment into CWBFG production environment. All high and medium risk findings must be fully remediated;
    - escrow arrangements, in case the source code was no longer available due to a failure of the outsourcer;
    - contractual right to audit the build environment used to create the deliverables, and the development processes and controls used;
    - file transfer methods to be used for bulk loads of information required to support the development efforts; and
    - remote access methods to be used, to access internal CWBFG information and/or internal systems. The CWBFG sponsor needs to ensure the service provider reviews and adheres to CWBFG's ***Network Access Standard***, as well as processing the CWBFG Non-Disclosure Agreement.

Selection of Outsourced Vendor/Developer

- Standard procurement procedures must be used in the selection and engagement of an appropriate outsourced developer. Use of these procurement procedures will ensure the developer:
  - delivers the software to the required standard;
  - meets the delivery timescales required;
  - represents best value for CWBFG;
  - meets the specified security requirements; and
  - assesses any sub-contractor's alignment with security requirements, if the use of sub-contractors are used by the outsourced developer for any aspects of the development.

Supervision and Monitoring

- Measures must be put in place to ensure adequate supervision of the activities of the outsourced developer and regular monitoring of progress.
- For large projects with significant time gaps between deliverables, an agreed method of verifying interim progress must be in place so that early warning is given of delays.

Reviews and Acceptance

- Review points must be established as part of the project planning process to verify progress and give formal acceptance of the software deliverables created. These will involve appropriate testing activities and code reviews.
- The outsourced software developer must be required to provide evidence of the security testing activities carried out during the development, including tests for concealed malware, backdoors and known vulnerabilities.
- Where appropriate a security review of developed code may be engaged with a suitable third party with the relevant security expertise.

Audit of Development Methods

- CWBFG must have the contractual right to undertake a second party audit of the outsourced development provider. This may be to review whether the development methods used by the outsourced developers comply with their contractual obligations and agreements.
- For larger projects, it is recommended that a risk assessment be carried out prior to the placing of the order for software development to ensure that assurances given during the sales process are valid.

Intellectual Property

- Unless the software is licensed under a formal agreement, contractual arrangements with an outsourced software developer must state that the ownership of the code produced on our behalf rests with CWBFG.
- It is important that any software that is developed under an outsourcing contract is understood to be our intellectual property. Appropriate legal advice must be taken particularly if the outsourcer is based outside of our home country.

Escrow

- Arrangements must be made for CWBFG to be able to legally access the source code of any developments undertaken, if the outsourcer's business terminates. This must be the case during development and if appropriate after the code has been delivered.

Exceptions

All exceptions to this standard must be documented and approved by both the information owner and the Chief Information Security Officer. Exceptions to this standard must be documented and registered as a risk as per the Information Security Governance, Risk, and Compliance processes. Identified risks must be assessed by the CWBFG Information Security Office and mitigated in partnership with the business owner and third-party service providers.

Enforcement

Failure to comply with this standard may impact the business and reputation of CWBFG. Depending on the circumstances, CWBFG will act to correct violations of this standard through training, counselling, disciplinary action, termination of employment, civil action or criminal prosecution.

It is the policy of CWBFG to handle information security incidents so as to minimize their impact on the confidentiality, integrity, and availability of CWB information systems, applications, and data. An information data breach incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information that interferes with information technology operations. All such incidents must be reported to the CWBFG Information Security Office.

Roles and Responsibilities

Role	Responsibility
Chief Information Security Officer	• Accountable for the creation, maintenance, and implementation of this standard where applicable. • Accountable to have and maintain written standards and procedures necessary to ensure implementation of and compliance to this standard. • Accountable to provide appropriate support and guidance to assist employees to fulfill their responsibilities of complying with this standard.
Sr. Manager, Information Security Program Management	• Responsible for the creation and maintenance of this standard and supporting policy where applicable. • Responsible to have and maintain written standards and procedures necessary to ensure implementation of and compliance to this standard. • Responsible to provide support and guidance to assist employees to fulfill their responsibilities of complying with this standard. • Consulting with Sr. Manager, Security Governance, Risk and Compliance and Sr. Manager, Security Operations, as required.
CWB's Executive Leadership Team, Senior Leadership Team, Directors, and Managers	• Understand and comply with this standard and supporting policy in its entirety. • Responsible to create and maintain processes and procedures to support this standard and supporting policy. • Responsible to ensure that all appropriate personnel are aware of and comply with this this standard and supporting policy. • Responsible for the creation of appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this standard and supporting policy.
CWB employees, contractors, third-party service provider, etc.	• Understand and comply with this standard and supporting policy in its entirety. • Implement this standard with supporting processes and procedures. • Report vulnerabilities and breaches.

Appendix A – Document Control

Document Status

Document Name	SDLC Security Standard
Document Owner	Chief Information Security Officer
Version	Version 1.0
Publication Date	
Information Classification	Internal Use
Revision Status	Final
Custodian	Sr. Manager, Information Security Program Management
Organization	CWBFG Information Security Office
Retention Period	Retain for ongoing use
Master Storage Location	

Revision History

Version	Author	Contributor	Description of Changes
Draft 0.1	Vikram Singh	Joanne Pearson	Document creation
Draft 0.2	Joanne Pearson		Document review and updates
Draft 1.0	Vikram Singh	Joanne Pearson	Document review by: Michael Thompson, Jose Barril, Reinhardt Tonn, Mark Doubinin, Thomas Matthews and National Leasing
Draft 2.0	Vikram Singh	Joanne Pearson	Finalize Draft for CISO review
Final V1.0	Joanne Pearson	Cory Gould	Feedback incorporated and published in Keylight

Appendix B - Definitions

The following table highlight key definitions used in this Standard.

CISO	Chief Information Security Officer
CWBFG	Canadian Western Bank Financial Group
OWASP	The Open Web Application Security Project (OWASP) is a non-profit foundation that works to improve the security of software. The OWASP Foundation is the source for developers and technologists to secure the web.
SANS	SysAdmin, Audit, Network, Security (SANS) Institute is a private U.S. for-profit company that specializes in information security, cybersecurity training and selling certificates.
Software Development Lifecycle (SDLC)	Software development is the process of conceiving, specifying, designing, programming, documenting, testing, and bug fixing involved in creating and maintaining applications, frameworks, or other software components