CWBFG - Digital Crown Jewel Standard

CWB Financial Group – Information Security Office (ISO)
August 20, 2020

Contents

CWBFG - Crown Jewel Standard

Purpose

The purpose of the Digital Crown Jewel ("CJ") Standard ("Standard") is to document and communicate the appropriate controls required to manage the governance and protection of CWBFG's CJ assets. Crown Jewels are critical business assets with the highest potential for adverse impact to CWBFG if compromised or taken offline.

Scope

The Standard applies to all CWBFG and all CWBFG's Business Segments and Oversight Functions, as well as vendors and partners that exchange data with CWBFG.

In the case of a merger or acquisition, Management shall ensure that their responsibilities under this Standard are carried out to the extent applicable and appropriate with regard to the newly merged or acquired entity.

Assets in scope are those that are identified and validated as CJ's as per the requirements of this standard.

A CJ is an electronic information asset which, if compromised through a cyber intrusion, would result in a significant financial, operational or reputational impact to the Bank – i.e. material cost beyond CWBFG's financial loss tolerance, loss of the ability to manage, govern, or even operate critical business functions or serious harm to CWBFG's brand, increasing the risk of a 'bank run'.

Considerations for identifying CJ's include:

- Platforms that directly store significant amounts of data, with a breach cost/implication of:
  - 12-month losses resulted from inadequate or failed processes or systems, human factors, or external fraud which exceed $5,000,000
  - Privacy incidents caused by a failure of CWBFG Group people, systems, or processes (over the previous 12 months) which exceed 120/year or 30/quarter
  - Complaints caused by a regulatory consumer obligation violation (over the previous 12 months) of over 10/year
  - Number of Internal Investigations conducted by FSIS, including but not limited to Fraud (over the past 12 months) exceed 12 per year
  - External Fraud losses (annual $ loss) of over $2,500,000
- Where there is zero tolerance for unauthorized access to systems
- Where system availability, which falls below 99% (Approximately 90 hours per year), is unacceptable.
- Applications that if breached, could result in significant theft of funds with no or limited measures to detect or stop the fund transfers in a short period of time.

Adherence to these requirements is expected upon date of publication unless otherwise specified.

1 Standard Requirements

Requirement ID	Description
CJ-1	**Identification of CWBFG’s Crown Jewels** ***CWBFG Information Security Advisory Committee*** must validate that the criteria for CJ addition is consistently applied across the segments by reviewing the Crown Jewel upon identification. Chief Information Security Office (CISO) must review the corresponding rationale and approve any addition and/or change to the list of CJ assets.
CJ-2	**Validation of CWBFG’s Crown Jewels** All new or changes to the classification of a CJ asset must be tabled for review and endorsement at the ***CWBFG Information Security Advisory Committee*** upon identification. To ensure continued alignment with CWBFG’s quantitative Risk Appetite, the CJ asset list **must** be reviewed and validated by ***CWBFG Information Security Advisory Committee*** on an annual basis.
CJ-3	**Control Gap Assessment of CWBFG’s Crown Jewels** The CJ Application Owner with support from appropriate IS staff **must** perform a control gap analysis against the enhanced CJ controls.
CJ-4	**Remediation of CWBFG’s Crown Jewels** Business and Application owners **must** develop and approve remediation plans and/or identify compensating controls for CJ enhanced control gaps within 90 days. Upon completion of remediation, the evidence of completion must be reviewed by the ***CWBFG Information Security Advisory Committee*** within 90 days.
CJ-5	**Reporting of CWBFG’s Crown Jewels** Consolidation of all gaps and status of all remediation activities **must** be tabled as information to Level 2 Risk Committees on a semi-annual basis. This will be part of the CISO overall risk reporting activities.
CJ-6	**Crown Jewel Vendor Management** All Third-Party Service Providers who host or support a Crown Jewel Asset must undergo an annual security assessment process. This process will be triggered by the Security Governance, Risk and Compliance team within Information Services.

2 Exception Management

Adherence to this Standard is mandatory. Any exceptions to the standard must be brought forward to the Security Governance, Risk and Compliance team. An assessment of the corresponding risk will be performed and the request submitted for approval by the ***CWBFG Information Security Advisory Committee.***

3 Ownership and Responsibilities

Ownership: The EVP and Chief Information Officer owns this standard and is responsible for the development, implementation, maintenance, monitoring and reporting with respect to this standard.

Name	Description	Role
Executive Vice-President and Chief Information Officer	Responsible for all Information Technology and Information Security Strategic and Operational activities	Is senior member of CWBFG Information Security Advisory Committee and provides authorization for resourcing and risk decisions affecting CWBFG Crown Jewels.
Senior Vice President, Information Systems	Oversees the operational and strategic activities of the Application Services, Information Management, IS Operations, Infrastructure Services, and Information System Delivery teams.	An advisory member of the CWBFG Information Security Advisory Committee, who ensures the CJ standard is being followed within their organization.
Chief Information Security Office (CISO)	Leads information security practice within IS.	The CISO has the responsibility to oversee the risk management process for all of IS. An advisory member of the CWBFG Information Security Advisory Committee who assists the Sr. VP of IS in administrating the CJ Standard among the various teams. The CISO reserves the right to escalate action on any identified risks they feel place CWBFG in an unacceptable position and will allocation resources as appropriate to mitigate those risks as needed. The CISO is also the accountable individual for ensuring all risks identified are reported appropriately and to work with other groups to create compensating controls when risk levels exceed acceptable tolerances. The CISO can also reclassify risks if they feel the current calculation is inaccurate or does not properly account for the potential severity of a risk event.
Business Line Application Owners	Owns a specific asset or business application	Responsible and accountable to ensure their applications have been appropriately categorized. Accountable to validate that CJ enhanced controls are assessed against the CJ asset and control gaps are assessed.
CWBFG Information Security Advisory Committee	A standing committee of leaders and subject matter experts who enforce compliance against the CJ standard	Provide leadership and governance of the technology control requirements and risk procedures to oversee the bank's most strategic assets. The Council is responsible to ensure CJ identification criteria is applied consistently across the enterprise, risk assessments are completed, control gaps identified, and remedial actions taken by management.

4 Related Policies and Standards

Document Name	Description
CWB - Information Systems Risk Management Standard	Sets out the Risk Management process for IS related assets
CWB Group Risk Appetite Framework Policy	The Risk Appetite Framework Policy (RAF) is the framework of policies and processes that establish and monitor adherence to CWBFG's Risk Appetite. It contains the Risk Capacity, Risk Appetite Statement, and Risk Limits, as well as an outline of the roles and responsibilities of those overseeing its implementation
CWB – Crown Jewel Enhanced Security Controls	A series of enhanced configuration and security hardening requirements for Crown Jewel Assets. These are to be applied in addition to the requirements detailed in the System Security Standard
CWB – System Security Standard	To provide the security requirements for CWBFG systems using a collection of tools, techniques, and hardening best practices

5 Review and Amendment History

Version	Date	Author	Description of Change	Approved By
Draft 0.1	April 2020	Kevin Vadnais	Initial Draft	
Draft 1.0	August 2020	Anne-Marie Lambert	Revisions as per CISO	

Appendix A – Current CJ Inventory

CJ Name	CJ Business Owner	Technical Management	CJ Description	Last Gap Analysis
T-24	AMS, IS	Temenos Team. CWBFG will request modifications as needed. Local resources host application	T24 is an integrated core banking solution that is often referred to as "all in one" technology resource. T24 equips financial institutions with all the necessary tools for managing the entire workflow of banking operations from both back and front end in addition to client relationship management. T24 has established strong reputation in financial services market over the past 14 years.	May 2019
SAS EDW / BI	Information Management Analytics	Supported completely by vendor. Customized as requested. Local resources host application	An enterprise Data Warehouse for compiling data used in reporting across CWBFG. Information is collected and modeled to simplify the generation of actionable reports.	May 2019
Wave	Business Application Services, IS	Line Data is vendor who supports it. Customized as requested. Local resources host application	Wave is a web-based integrated accounting solution exclusively designed for small businesses, freelancers, and consultants. Wave provides features including accounting, invoicing, billing, payment tracking, payroll management, finance management, and receipts.	May 2019
Felix	National Leasing	In-House by CWBFG Staff. National leasing application. Have 40 developers working on this Local resources host application	Felix is a custom developed leasing software used by the National Leasing group.	May 2019
Salesforce	National Leasing and equipment financing	Vendor Managed Cloud Hosted	Salesforce is an online solution for customer relationship management, or CRM. It gives all your departments — including marketing, sales, commerce, and service — a shared view of	May 2019

			customers with one integrated CRM platform.	
Office 365	Infrastructure Operations	Most backend is managed by vendor. Administration of application is controlled by CWBFG IT Staff Cloud Hosted	Productivity suite of tools including word processors, spreadsheets, email applications, and collaboration tools for instant messaging and online voice/video conferences.	May 2019
Maximizer – Cweb / Purefacts	Information Systems	Managed by CWT (Canadian Western Trust) but do follow change board processes at CWBFG. Local resources host application	Maximizer CRM features sales management, marketing automation, customer service and support and business productivity tools with integration with Microsoft products such as Outlook, Word, Excel and SharePoint. Purefacts - industry-leading fee calculator has the flexibility to calculate every wealth management fee needed. This prevents revenue leakage while creating new revenue opportunities for CWBFG	May 2019
Workday	Human Resources / Information Systems	Platform managed by Workday. Cloud Hosted	A SAAS application focused on Human Resource (HR) activities including onboarding, training coordination, talent management, PTO, and other related employee tasks	May 2019
Diligent Board Books	Corporate Management	Vendor managed Cloud Hosted	Diligent Boards, used by 50% of the Fortune 1000, provides boards and executives with modern governance tools that allows the board to expand their reach outside the boardroom as well as meeting requirements such as distribution of board meeting materials in a secure environment.	May 2019
Centrify	Information Systems	Information Systems Local resources host application		May 2020
Active Directory	Infrastructure Services	Information Services	A Microsoft tool used to create, manage, and control the access of users to CWBFG IT resources.	May 2019

		Local resources host application	AD enables access permissions to be managed in a central location and ties in to most applications currently used by CWBFG.	
EMC Avamar Backup Solution	Infrastructure Services	Information Services Local resources host application	EMC Avamar is a backup and recovery solution that features backup software, disk targets and global client-side deduplication.	May 2019
RBC Express Online	Centralized Services, CS-Banking support	All technical aspects managed by vendor. Local resources host application	Online banking management software. Would include thing such as direct deposit interfaces to other financial institutions or wire transfers.	May 2019
Online Banking	CWBDirect Online Banking	Vendor Managed (Central1), customized as requested. Both cloud and local resources host application	Customer facing web banking portal.	May 2019
QRM	Treasury, Data, Infrastructure Services	Information Services Local resources host application	Risk management software used to track CWBFG risk related information.	May 2019