.

BURDELL BANK
CLOUD SECURITY POLICY

Michael Chi, Matthew Jinks, Pablo Schelcher, Dylan Yost

Table of Contents

.

1. Purpose

This Cloud Security Policy for Banks aligns with the National Institute of Standards and Technology's (NIST) Risk Management Framework SP 800-53 guidelines and best practices. The policy establishes minimum standards for securing cloud infrastructure and services used by Burdell Bank.

2. Scope

This policy applies to all cloud-based services and systems operated used for Burdell Bank operations. It also applies to any employees, contractors, and third-party vendors with access to our cloud-based systems and services.

3. Cloud Service Provider (CSP) Selection & Management:

3.1 Responsibilities of CISO

When adopting a cloud-based solution, it is the responsibility of the bank's Cloud Information Security Officer (CISO) to take the following steps:

Step	**Task**
A	Specify the services or applications that will be supported by the cloud-based solution [29].
B	Identify the necessary functional capabilities for the cloud-based services [29].
C	Recognize the privacy and security needs essential for implementing strong security measures for the cloud-based service, guaranteeing adherence to the NIST security category requirements [29].
D	Deploy the most suitable cloud environment architecture that integrates both cloud service and deployment models, such as: I. Public models using IaaS, PaaS, or SaaS II. Private models using IaaS, PaaS, or SaaS III. Hybrid models using IaaS, PaaS, or SaaS [29]

E	Identify the responsible actors for each cloud service environment or ecosystem (what resources are the bank's responsibility and what resources are the CSPs responsible?) [29]
F	Ensure that the CSP implements baseline security controls, complies with privacy and security requirements, and provides additional compensating controls [29].
G	Allocate and document security parameters that correspond to the specific security requirements and needs of the bank [29].
H	Create supplementary internal enhancements to augment the fundamental security and privacy controls enforced by the CSP [29].
I	Enumerate any additional requirements for implementing security and privacy controls that do not meet the fundamental security standards [29].

3.2 Risk Assessment

The CISO establishes a risk-assessment methodology and documents all resources and services to be integrated into the cloud. The methodology includes procedures for identifying threats and vulnerabilities, determining which assets are most likely to be affected by attacks, and assessing the likelihood and impact of risks [1]. The assessment is repeatable and performed quarterly at minimum. At minimum, the assessment is updated annually to reflect the most current threats posing the largest risks to cloud computing solutions.

3.3 Service Level Agreement

The CISO negotiates Service Level Agreements (SLAs) to ensure CSPs meet the bank's availability, performance, security, privacy, and regulatory requirements [2].

3.4 Implementation Management

The CISO ensures that controls are properly implemented and monitored. Control implementations are done by the CISO or allocated to authorized personnel. Due diligence is performed to ensure that control requirements and implementations specified in SLAs are compliant. Continuous monitoring of all security and privacy controls are performed to ensure their ongoing effectiveness [3].

4. Policy Controls

4.1 Access Controls

The bank prevents unauthorized access to cloud-based systems and data using the following access control measures:

Identification & Authorization	All users accessing cloud-based resources are identified and authenticated using multi-factor authentication [4]. The CISO develops a standard for password to manage their complexity, expiration, and reuse. *Corresponding NIST SP 800-53 Controls: IA-2*
Separation of Duties	Separation of duties is enforced to prevent any single user from having complete control over a cloud-based resource [5]. Administrative functions are separated from user functions, and administrative access is granted only to authorized personnel. *Corresponding NIST SP 800-53 Controls: AC-5*
Remote Access	Remote access to cloud-based resources is granted only to authorized personnel using secure and encrypted communication channels [6]. Remote Access is monitored and logged. Access is revoked immediately upon termination of employment or contract. *Corresponding NIST SP 800-53 Controls: AC-18*
Monitoring & Logging	Access to cloud-based resources is monitored and logged to detect and respond to any security incidents or breaches

Controls enforced by CISO.

4.2 Awareness and Training

The CISO ensures the Bank provides security awareness and training to all actors that have access to the bank's cloud based services and resources. The controls to ensure this are:

Security Awareness	All employees and contractors accessing cloud-based resources receive annual security awareness training to familiarize themselves with the bank's security policies and procedures as well as the risks and threats associated with cloud computing [7]. This training is provided upon hire and annually thereafter.

	Corresponding NIST SP 800-53 Controls: AT-2
Role-based Training	All employees and contractors accessing cloud-based resources receive role-based security training that is relevant to their specific job responsibilities [8]. This training includes best practices for securing cloud-based resources, such as password management, data encryption, and incident response. *Corresponding NIST SP 800-53 Controls: AT-3*
Testing and Evaluation	The effectiveness of the security awareness and training program is periodically tested and evaluated. This includes conducting phishing simulations and incident response drills to ensure that employees and contractors are able to identify and respond to security threats.
Remedial Training	Employees and contractors who fail to comply with security policies and procedures receive remedial training to address their deficiencies. This training is documented and monitored to ensure its effectiveness

4.3 Audit and Accountability

The CISO implements the following audit and accountability controls for cloud-based resources to detect and respond to security incidents and breaches:

Audit Trail Generation	Audit trails are generated for all cloud-based resources accessed by the bank [9]. These audit trails capture user and system activity including logins, logouts, file accesses, and configuration changes. *Corresponding NIST SP 800-53 Controls: AU*
Audit Trail Storage	The audit trails are protected from unauthorized modification, deletion, or access.
Audit Review Analysis	Audit trails are reviewed and analyzed daily to identify any anomalous activity. Any security incidents or breaches detected are reported to authorized personnel for investigation and response [10]. *Corresponding NIST SP 800-53 Controls: AU-6*
Incident Response	The CISO has an incident response plan in place to respond to security incidents and breaches detected through audit trails. This plan includes procedures for reporting, investigating, and containing security incidents. Additionally there are procedures in place for notifying affected parties and restoring affected systems [11].

	Corresponding NIST SP 800-53 Controls: IR-6

4.4 Configuration Management

The CISO shall implement the following configuration management controls for cloud-based resources:

Configuration Baseline	Configuration baselines are established for all cloud-based resources to ensure that they are configured in accordance with security policies and standards [12]. These baselines are reviewed and updated annually to reflect changes in security requirements or cloud service provider offerings. *Corresponding NIST SP 800-53 Controls: CM-2*
Change Management	All changes to cloud-based resources are managed through a formal change management process that includes testing and approval procedures [13]. Changes are documented and reviewed to ensure that they do not adversely affect the security of cloud-based resources. *Corresponding NIST SP 800-53 Controls: CM-3*
Patch Management	All cloud-based resources are patched regularly to address known vulnerabilities and weaknesses. Patches are tested and applied promptly to minimize the risk of security incidents or breaches [14].
Asset Inventory	An inventory of cloud-based resources is maintained to ensure that they are properly managed and secured. This inventory includes information on the location, ownership, and configuration of each resource [15].

4.5 System and Communications Protection

The CISO ensures that the bank protects the confidentiality, integrity, and availability of information systems and communications by implementing the following controls:

Access Control	Access to cloud-based resources is restricted to authorized personnel and systems
Encryption	Sensitive data transmitted to and from cloud-based resources is encrypted using approved encryption algorithms. Encryption keys are managed securely to prevent unauthorized access [16].

	Corresponding NIST SP 800-53 Controls: SC-12
Network Segmentation	Cloud-based resources are segmented from other networks to minimize the risk of unauthorized access or lateral movement by attackers [17]. Segmentation is implemented using firewalls or other approved mechanisms.
Malware Protection	Cloud-based resources are protected from malware using anti-malware software and other approved mechanisms [18]. Malware signatures are updated regularly to minimize the risk of infection. *Corresponding NIST SP 800-53 Controls: SC-7*

4.6 Availability:

The CISO implements the following controls to maintain availability of cloud-based resources:

Failure Prevention Controls	Proactive measures are implemented to prevent and mitigate cloud-based resource failures. These measures include implementing redundancy and fault tolerance mechanisms, regularly testing system backups, and implementing automated failover and disaster recovery procedures [19]. *Corresponding NIST SP 800-53 Controls: CP-9, CP-10*
Service Level Agreements	Service Level Agreements are established with cloud service providers to ensure that cloud-based resources meet the bank's availability and reliability requirements. SLAs include provisions for service uptime, response time, and support [20].
Disaster Recovery Plan	A disaster recovery plan is developed and implemented for cloud-based resources to ensure the timely recovery of critical systems and data in the event of a disaster or other disruptive event. The plan includes procedures for data backup and restoration, system recovery, and communication with stakeholders [21]. *Corresponding NIST SP 800-53 Controls: CP-9, CP-10*
Proactive Monitoring	Proactive monitoring of cloud-based services is implemented to detect and resolve issues before they result in service disruptions. This includes monitoring the availability and performance of cloud-based resources, implementing alerts and notifications for potential issues, and conducting regular system health checks.

.

4.7 Continuous Monitoring

The bank implements continuous monitoring of its cloud infrastructure and services to detect and respond to security incidents and vulnerabilities. This includes the monitoring of user activity and network traffic [22]. This CISO ensures the following controls are implemented:

Automated Monitoring	CISO deploys automated monitoring tools to continuously monitor cloud-based resources for security events such as unauthorized access attempts, malware infections, and data breaches. Monitoring includes network traffic, system logs, and user activity [23]. *Corresponding NIST SP 800-53 Controls: CA-7*

5. Compliance

5.1 Compliance Officer

The Compliance Officer ensures that the bank complies with all applicable regulatory standards, iThe Compliance Officer will collaborate closely with the CISO to ensure that all cloud-based resources comply with all regulatory standards.

5.2 Regulations

The Burdell Bank complies with all relevant regulatory requirements and guidance, including but not limited to:

Federal Financial Institutions Examination Council (FFIEC) Guidelines	The bank complies with the FFIEC Guidelines on outsourcing technology services and cloud computing. This includes conducting due diligence on cloud service providers, establishing Service Level Agreements (SLA), and ensuring that cloud providers are subject to regular audits [24]
Office of the Comptroller of Currency (OCC) Guidelines	The bank complies with OCC Guidelines on Third-Party Relationships. This includes establishing due diligence processes, assessing the risks associated with third-party relationships, and ensure that third-party relationships are subject to regular monitoring and oversight [25]
Federal Deposit Insurance Corporation (FDIC) Guidelines	The bank complies with FDIC Guidelines on Technology Risk Management. This includes establishing management processes, implementing controls to manage risks, and ensuring that third-party relationships are subject to regular monitoring and oversight [26]
Gramm-Leach-Bliley Act (GLBA)	The bank will comply with GLBA requirements for protecting the privacy and security of customer data. This includes implementing appropriate administrative, physical, and technical safeguards to protect customer data [27]
Payment Card Industry Data Security Standards (PCI DSS)	The bank will complies with PCI DSS security standards for protecting payment card data. This includes implementing appropriate security controls, conducting regular security assessments, and reporting security incidents [28]

6. Enforcement

The permissions of employees who seek to use unauthorized services are removed until they complete security training. Repeated efforts to utilize illegal services or deliberate violation of the Cloud Policy will result in harsher consequences, such as written reprimands, suspension of access to the bank's cloud-based services and systems, termination of employment, and possible legal action (lawsuit, etc.). To maintain a secure and compliant environment, the bank requires all employees to adhere to the Cloud Policy.

.

References

[1] I. T. L. Computer Security Division, “Release search - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/control?version=5.1&amp;number=RA-3. [Accessed: 15-Mar-2023]

[2] L. Rosencrance, S. Louissaint, and K. Brush, “What is a service-level agreement (SLA)?,” *IT Channel*, 12-Jan-2021. [Online]. Available: https://www.techtarget.com/searchitchannel/definition/service-level-agreement. [Accessed: 15-Mar-2023].

[3] RSI Security, “Understanding cloud security policy: NIST's recommendations,” RSI Security, 15-Jun-2022. [Online]. Available: https://blog.rsisecurity.com/understanding-cloud-security-policy-nists-recommendations/. [Accessed: 15-Mar-2023].

[4] I. T. L. Computer Security Division, “Release search - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/control?version=5.1&amp;number=IA-2. [Accessed: 15-Mar-2023].

[5] I. T. L. Computer Security Division, “Release search - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/control?version=5.1&amp;number=AC-5. [Accessed: 15-Mar-2023].

[6] I. T. L. Computer Security Division, “Release search - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/control?version=5.1&amp;number=AC-17. [Accessed: 15-Mar-2023].

[7] I. T. L. Computer Security Division, “Release search - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/control?version=5.1&amp;number=AT-2. [Accessed: 15-Mar-2023].

[8] I. T. L. Computer Security Division, “Release search - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/control?version=5.1&amp;number=AT-3. [Accessed: 15-Mar-2023]

[9] I. T. L. Computer Security Division, “Release search - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/controls?version=5.1&amp;family=AU. [Accessed: 15-Mar-2023].

[10] I. T. L. Computer Security Division, “Release search - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/control?version=5.1&amp;number=AU-6. [Accessed: 15-Mar-2023].

[11] I. T. L. Computer Security Division, “Release search - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/control?version=5.1&amp;number=IR-6. [Accessed: 15-Mar-2023].

[12] I. T. L. Computer Security Division, “Release search - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/control?version=5.1&amp;number=CM-2. [Accessed: 15-Mar-2023].

[13] I. T. L. Computer Security Division, “Release search - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/control?version=5.1&amp;number=CM-3. [Accessed: 15-Mar-2023].

[14] D. Essex and B. Posey, “What is patch management? lifecycle, benefits and best practices,” Enterprise Desktop, 17-Jun-2022. [Online]. Available: https://www.techtarget.com/searchenterprisedesktop/definition/patch-management. [Accessed: 15-Mar-2023].

.

[15]“Cyber security guidelines for information asset management: Roles and ...” [Online]. Available: https://www.qcert.org/sites/default/files/public/documents/cs-csps_iam_roles_and_responsibilities_eng_v1.1.pdf. [Accessed: 15-Mar-2023].

[16]I. T. L. Computer Security Division, “Release search - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/control?version=5.1&amp;number=SC-12. [Accessed: 15-Mar-2023].

[17]“Best practices for network segmentation in the cloud,” IANS. [Online]. Available: https://www.iansresearch.com/resources/all-blogs/post/security-blog/2021/07/13/best-practices-for-network-segmentation-in-the-cloud. [Accessed: 15-Mar-2023].

[18]I. T. L. Computer Security Division, “Release search - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/control?version=5.1&amp;number=SI-7. [Accessed: 15-Mar-2023].

[19]I. T. L. Computer Security Division, “Release search - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/controls?version=5.1&amp;family=CP. [Accessed: 15-Mar-2023].

[20]I. T. L. Computer Security Division, “Release search - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/control?version=5.1&amp;number=RA-3. [Accessed: 15-Mar-2023].

[21]I. T. L. Computer Security Division, “Release search - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/controls?version=5.1&amp;family=CP. [Accessed: 15-Mar-2023].

[22]I. T. L. Computer Security Division, “Release search - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/control?version=5.1&amp;number=CA-7. [Accessed: 15-Mar-2023].

[23]“Cloud.gov,” Home. [Online]. Available: https://cloud.gov/docs/ops/continuous-monitoring/. [Accessed: 15-Mar-2023].

[24]Ffiec Press Release. [Online]. Available: https://www.ffiec.gov/press/pr043020.htm. [Accessed: 15-Mar-2023].

[25]“Third-party relationships: Risk management guidance,” OCC, 30-Oct-2013. [Online]. Available: https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html. [Accessed: 15-Mar-2023].

[26]“Banker Resource Center: Information Technology (IT) and Cybersecurity,” FDIC. [Online]. Available: https://www.fdic.gov/resources/bankers/information-technology/. [Accessed: 15-Mar-2023].

[27]the P. N. O. Staff and S. T. Nguyen, “Gramm-Leach-Bliley Act,” Federal Trade Commission, 16-Feb-2023. [Online]. Available: https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act. [Accessed: 15-Mar-2023].

[28]“Document library,” PCI Security Standards Council, 16-Feb-2023. [Online]. Available: https://www.pcisecuritystandards.org/document_library/. [Accessed: 15-Mar-2023].

[29]RSI Security, “Understanding cloud security policy: NIST's recommendations,” RSI Security, 15-Jun-2022. [Online]. Available: https://blog.rsisecurity.com/understanding-cloud-security-policy-nists-recommendations/. [Accessed: 15-Mar-2023].