|  |
| --- |
| Fifth ThirD Bank |
| FTB Cloud Security Framework |
|  |
|  |
| **Fifth Third Bank** |
| **5/31/2017** |

|  |
| --- |
|  |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version no. | Changed by | Change | Change Date | Approved By | Approval Date |
| 0.5 | Brian Cummings | 1. Revised the Change Log 2. Accepted all prior changes | 5/31/2017 |  |  |
| 0.4 | Brian Cummings | Revised per Arunkumar. S feedback | 5/19/2017 | Arunkumar. S | 5/31/2017 |
| 0.3 | Brian Cummings | Cosmetic and cross-ref edits | 5/12/2017 | N/A | N/A |
| 0.2 | Brian Cummings | Revisions to completely incorporate requirements | 5/5/2017 | N/A | N/A |
| 0.1 | Brian Cummings | Incorporated FTB InfoSec Requirements from the “FTB\_Cloud InfoSec Requirements” workbook | 4/28/2017 | N/A | N/A |
| WIP 0.2 | Don Lykins | Incorporate offline edits by self and Brian Cummings | 4/24/2017 | N/A | N/A |
| WIP 0.1 (offline edit) | Brian Cummings | Modified every narrative section | 4/23/2017 | N/A | N/A |
| WIP 0.1 | Don Lykins | Edited original | 4/17/2017 | N/A | N/A |

**Change Log**

Table of Contents

[Introduction 3](#_Toc484156490)

[Purpose of Document 3](#_Toc484156491)

[Document Ownership & Maintenance 3](#_Toc484156492)

[Response Instructions 3](#_Toc484156493)

[Cloud Computing Overview 4](#_Toc484156494)

[Cloud Deployment Models 4](#_Toc484156495)

[Cloud Service Models 5](#_Toc484156496)

[Cloud Stack 6](#_Toc484156497)

[Security Controls 6](#_Toc484156498)

[Security Solution Layers 8](#_Toc484156499)

[Security Controls Applied to the Solution Layers 9](#_Toc484156500)

[FTB Cloud Security Requirements 9](#_Toc484156501)

[Foundation Layer Controls 9](#_Toc484156502)

[Internet Layer Controls 12](#_Toc484156503)

[Service Layer Controls 14](#_Toc484156504)

[Compliance Layer Controls 18](#_Toc484156505)

# Introduction

## Purpose of Document

Fifth Third Bank (FTB) plans to transform current service delivery to a next-gen model using hybrid-cloud. This document introduces the FTB security capability model for cloud based environments that are based on FTP Information Security Policies and Standards and incorporate mandated security requirements and best practices including PCI–DSS, GLBA, HIPPA, FFIEC, ISO 27K, Cloud Security Alliance Cloud Control Matrix (Version V3.0.1) and other best practices to protect PCI, PHI, NPI, PII, and other FTB information in electronic form classified as Public, Internal Use, Confidential, or Restricted.

The FTB hybrid cloud will use private virtual cloud architecture both on- and off-premise. The objective of FTB Information Security is to leverage and extend/integrate existing solutions and practices as much as possible to secure the hybrid cloud; and to avoid proliferation of solutions, and an increase in identity and access administration workloads.

FTB is obligated to:

1. Define the Bank’s information security, business continuity, and disaster recovery requirements and recommendation for various cloud hosting environments.
2. Identify alignment and gaps in cloud provider native services with regard to the above policies, standards, and compliance requirements.

FTB has defined its security requirements in the context of a cloud security capability model that uses a layered approach to cloud solutions, and identifies the security capabilities that apply within each layer. The layers are applied based on the sensitivity of the data within the cloud environment and the channel used to access the application and data. Further, the security requirements were defined with reference to FTB Information Security Policies, Standards, and Solutions as documented and confirmed or supplemented through interviews with FTB Information Security subject matter professionals.

# Document Ownership & Maintenance

This document is owned and maintained by the:  
FTB Vice President, Deputy Chief IS Officer, Information Security Strategy & Information Assurance. The document will be maintained as a “living document” with additions and changes made on a timely basis to retain relevance to FTB evolving cloud information security requirements.

# Response Instructions

Respondents should examine the entire document to gain context, and then provide their proposed solutions to the requirements in the “Solution Recommendations” column of the table found in the FTB Cloud Security Requirements section below. The requirements have broad applicability across IaaS, PaaS, and SaaS cloud service models. Accordingly, respondents should indicate N/A to those requirements that, in their opinion, do not apply to their services/solutions.

# Cloud Computing Overview

Cloud computing introduces the concept of shared asset ownership and responsibility. An important point to clarify when determining ownership in the cloud environment is whether an organization is a cloud provider or tenant. The ownership is especially relevant when security controls are implemented. There are a number of controls that are available at different levels of the cloud stack. The ownership and responsibility to deploy and manage the security controls is based on the ownership role of the organization, the cloud deployment model, and the cloud service model used by the tenant.

To establish a common understanding of terms, Table 1 below provides commonly understood definitions for cloud tenant and cloud provider.

Table 1: Cloud Computing Overview

|  |  |
| --- | --- |
| **Organization Role** | **Description** |
| Tenant / Consumer | Fifth Third Bank contracting a metered service from the provider. |
| Provider | The entity that built the cloud deployment, and is offering metered services to one or more tenants. |

## Cloud Deployment Models

Cloud services can be deployed in different ways, depending on the organizational structure and the provisioning location of the cloud environments. Four deployment models are usually defined, namely private, public, community, and hybrid as illustrated below in Table 2.

Table 2: Cloud Deployment Models

|  |  |
| --- | --- |
| Organization Role | Description |
| On-Premise Private Cloud | The cloud infrastructure is provisioned for exclusive use by Fifth Third Bank comprising multiple consumers. It may be owned, managed, and operated by the Bank, a third party, or some combination of them, and it exist on Bank premises. |
| Off-Premise Virtual Private Cloud | The capability provided to Fifth Third Bank is to provision processing, storage, networks, and other fundamental computing resources where the Bank is able to deploy and run arbitrary software, which can include operating systems and applications. The Bank does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). |
| Community | A community cloud is managed and consumed by multiple entities that share a similar business model. For example a government could choose to set up a community cloud that is then consumed by different government agencies. |
| Hybrid | The cloud infrastructure is a composition of two or more distinct cloud infrastructures (On-Premise Private, Community, or Off-Premise Virtual Private) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). |

## Cloud Service Models

Service delivery in cloud computing is comprised of three different service models, namely IaaS, PaaS and SaaS. The cloud service model determines which components of an IT solution are outsourced to the cloud service provider. It’s common to use several service models at the same time. An overview of these cloud service models is contained in Table 3 below.

Table 3: Cloud Service Models

|  |  |
| --- | --- |
| Organisation Role | Description |
| IaaS | **Infrastructure as a Service:** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).. |
| PaaS | **Platform as a Service:**  The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. |
| SaaS | **Software as a Service:** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. |

## Cloud Stack

The cloud computing stack is often illustrated as a series of layers, as shown in the graphic in Figure 1 below. At each layer, different security control options are made available to the tenant. The options vary greatly based on the cloud service model and the services the tenant is consuming from the provider. However, the Cloud Stack is not entirely useful to define security control requirements, so FTB has elected to define its security requirements in the context of the Security Capability Domain framework described in the balance of this document, and ultimately address all of the elements of the Cloud Stack.



Figure 1: Cloud Stack

# Security Controls

Security controls are the technical and procedural elements that deliver the necessary security capabilities while being as least intrusive on the business as possible. A security control is a response to, or countermeasure for a risk. Security controls reduce risk, they don’t eliminate them. Every information asset has multiple risks and every risk may have a security control.

Security capabilities are required (built or acquired) to consistently apply across the cloud services and environments. This is required to ensure that cloud services meet all required levels of security. A security framework consisting of controls tailored for cloud helps in setting a baseline for these foundational security capabilities.

Security is one of the key concerns for organizations shifting services to the cloud. It does not however mean that cloud services are less secure; in fact cloud could be relatively more secure than traditional onsite environments due to the need for cloud providers to demonstrate and sustain security controls and practices to obtain and retain clients across government organization and highly regulated industriescompanies such as FTB. FTB expects a strong collaboration with its cloud service providers to define and implement integrated, end-to-end security controls across its hybrid cloud.

Responsibility for Cloud Security Controls – Off Premise Virtual Private Cloud

It is understood that security is a shared responsibility between the consumer and the provider with varying degrees of responsibilities based on the type of service model being used. (IaaS, PaaS or SaaS). However, it is also recognized that the ultimate responsibility of protecting its data lies with the consumer. The responsibility for security controls when aligned with the various cloud service models is illustrated in the diagram below. For hybrid cloud, the consumer is fully responsible for all aspects of security of its on-premise cloud environmet.

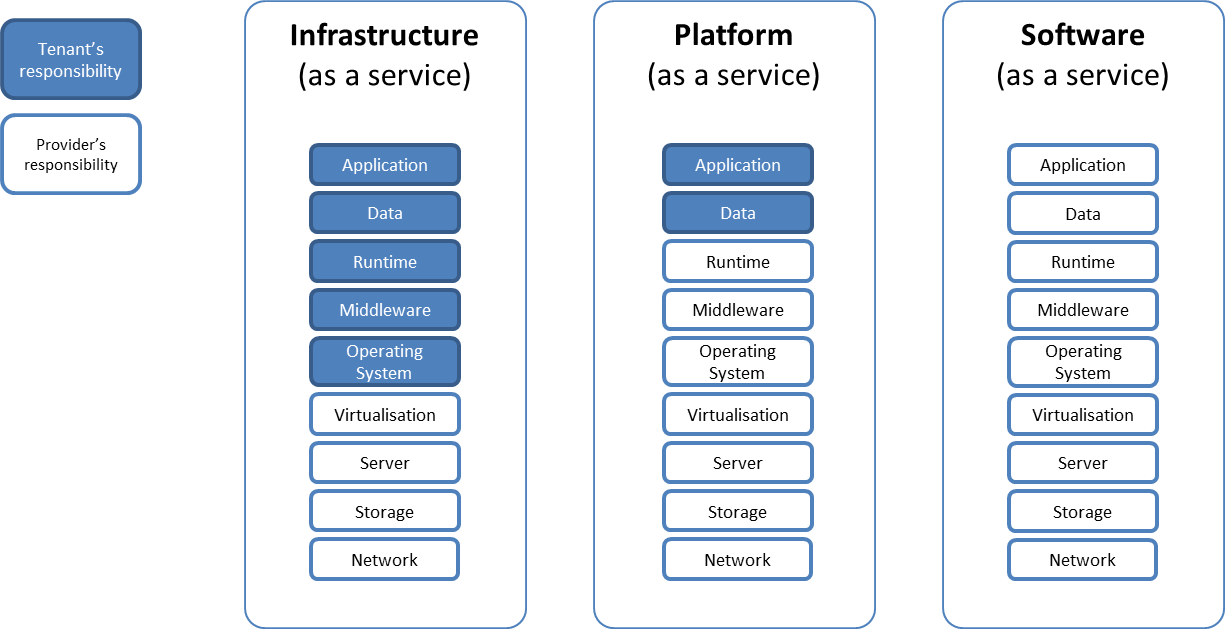


Figure 2: Responsibility Model

## Security Solution Layers

The relevant security controls to deploy are dependent on the importance of the information and assets the controls are protecting. To apply a consistent approach to deploying controls, a layered mode is employed, as illustrated below.

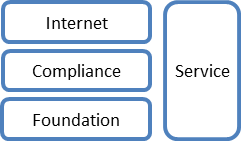


Figure 3 : Security Solution Layers

Each layer up the stack introduces additional security controls that build on the lower layers, the exact controls deployed depend on the nature of the application implemented in the cloud environment.

|  |  |
| --- | --- |
| **Solution Layer** | **Description** |
| Foundation | The baseline of controls that should be in place for all environments. This level of protection will ensure there’s a basic level of protection deployed. |
| Internet | The controls that should be in place when an application within the environment or network segment is visible to the Internet. These controls are deployed in addition to the Compliance level. |
| Service | Security controls made available as a service used for the management and monitoring of the other cloud environments and virtual systems. These services should be in their own network segment and well protected from all other environments. |
| Compliance | The controls that should be in place based on compliance requirements and the classification of assets within the environment or network segment. These controls are deployed in addition to controls at the Foundation level. |

## Security Controls Applied to the Solution Layers

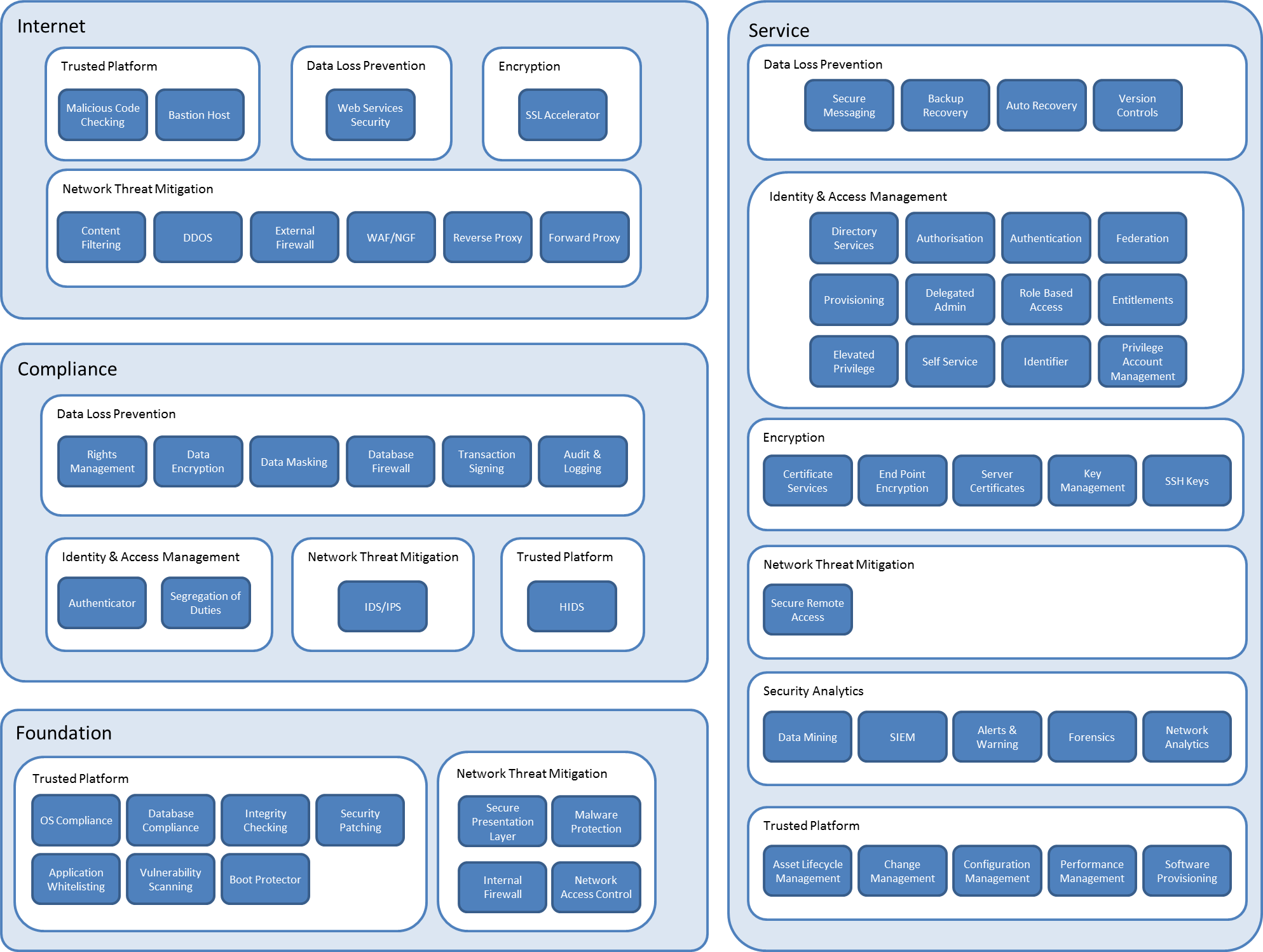


Figure 4: Security Solution Layer Controls Map

Applying security capabilities to the cloud solutions layer model illustrates the controls that are required at each layer. It also makes it obvious which controls are required depending on the cloud services model deployed by the tenant.

## FTB Cloud Security Requirements

FTB cloud security requirements are organized and presented below consistent with the layers and control elements in Figure 7 above. Solution Recommendations should be as specific as possible and should reference the specific products, tools, and processes needed to implement the Solution.

### Foundation Layer Controls

|  |  |  |  |
| --- | --- | --- | --- |
| **Domain** | **Control** | **FTB Requirement** | **Solution Recommendations** |
| Network Threat Mitigation | Internal Firewall | Firewalls must be used behind the network DMZ to isolate disparate network segments and restrict traffic to that which is specifically authorized.  Separate production and non-production environments to prevent unauthorized access to changes to information assets.  Apply defense-in-depth technical measures and techniques for detection and timely response to network-based attacks. |  |
| Network Threat Mitigation | Defense in Depth | Implement technical measures and apply defense-in-depth techniques for detection and timely response to network-based attacks. |  |
| Network Threat Mitigation | Network Access Control | Provide Network Access Control. |  |
| Network Threat Mitigation | Secure Presentation Layer | Presentation layers must be designed to separate user inputs from program control functions, and must include error identification and handling for unexpected user inputs in compliance with secure coding standards and the OWASP Top Ten Secure Coding practices. |  |
| Trusted Platform | OS Compliance | Build OS images for servers from approved baseline, secure configurations.  Boot Protection: Created bootable instances of operating systems that are encrypted.  Follow principle of least privilege (Give users the minimum privileges they need to carry out their tasks).  Avoid SMTP open relay, which can be used to spread spam. |  |
| Trusted Platform | Antivirus / Malware Management | Use a reputable and up-to-date antivirus, malware, and antispam solutions on instances.  Provide a solution to prevent the installation of untrusted software. |  |
| Trusted Platform | Application Whitelisting | Provide default restricted application whitelisting capability, allowing only specifically allowed IPs, on Internet facing systems. |  |
| Trusted Platform | Vulnerability Scanning | With security patches being released daily, Cloud service provider security practices must include procedures for both frequent (at least weekly) and periodic, vulnerability scanning to validate security patches; timely detect and remediate vulnerabilities; and to provide assurance that vulnerabilities have not been introduced after the implementation of significant changes.  Provide customers with a dashboard report of total open vulnerabilities at severity levels 5, 4, and 3. |  |
| Encryption | TLS Termination | Under end-to-end data protection principles, TLS encrypted traffic must be terminated on the target servers/services. |  |
| Encryption | Key Management | **Separation of Duties** – This means that different people control different procedures so that no one person controls multiple procedures. When it comes to encryption key management, the person who manages encryption keys should not be the same person who has access to the encrypted data.  **Dual Control** – This means that at least two or more people control a single process. In encryption key management, this means at least two people should be needed to authenticate the access of an encryption key, so that no one single person has access to an encryption key.  **Split Knowledge** – This prevents any one person from knowing the complete value of an encryption key or passcode. Two or more people should know parts of the value, and all must be present to create or re-create the encryption key or passcode. While split knowledge is not needed to create data encryption keys on the Cloud Provider, it is needed for the generation of master keys which are needed to protect data encryption keys. |  |
| Data Loss Prevention | Web Security Services | All data used and stored in a cloud environment must be protected in compliance with The Bank Information Classification & Handling Standard.  The FTB Access Management Standard requires that the data must be secured based on least privilege access controlusing role-based access requirements.  Monitored for inappropriate access, copying, and dataexfiltration. |  |

### Internet Layer Controls

|  |  |  |  |
| --- | --- | --- | --- |
| Domain | Control | Requirement | Solution Recommendation |
| Network Threat Mitigation | Distributed Denial of Service | All external facing Internet connectivity must be protected from DDoS attacks using Akamai Prolexic. |  |
| Network Threat Mitigation | WAF/NGF | Traffic must be actively inspected at the application layer to block exploit vulnerabilities such as SQL Injection, Cross-Site Scripting and other prevalent application layer attacks. |  |
| Network Threat Mitigation | Reverse Proxy | Reverse proxy servers must be employed to isolate Bank Web servers from direct Internet access and hide their Web server topology and characteristics. |  |
| Threat Mitigation | Forward Proxies | Provide a secure means to access third party services, such as content services and vendor patch downloads. |  |
| Trusted Platform | Malicious Code Protection | Provide protection against the introduction of software that may disrupt normal operations. Such protection must include prevention, detection, and correction.  Provide protection against such threats as malicious software, viruses, worms, trojan horses, key-loggers, adware, spyware, and ramsomware.  Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.  Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code. |  |
| Trusted Platform | Bastion Host | Bastion hosts services must be limited to those necessary to support approved network functionality. Such hosts must run current operating systems at current patch levels. |  |
| Network Threat Mitigation | External Firewall | For critical services, external firewalls must be configured for high availability. |  |
| Network Threat Mitigation | External Firewall | External firewalls must be restrictively configured to prevent all traffic, both inbound and outbound, except that which is specifically required, documented, and approved.  The Bank prohibits the use of default policy configrations and vendor provided default accounts and/or passwords. |  |
| Network Threat Mitigation | External Firewall | Production and non-production environments shall be separated to prevent unauthorized access to changes to information assets.  Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties. |  |
| Network Threat Mitigation | External Firewall | A dedicated grid/cluster is required for all PCI-DSS environments. |  |
| Data Protection | Web Services Security | All data used and stored in a cloud environment must be protected in compliance with the FTB Information Classification & Handling Standard, and the FTB Access Management Standard requiring that the data must be secured based on least privilege access control, role-based access requirements, and monitored for inappropriate access, copying, and exfiltration. |  |
| Encryption | SSL Acceleration | FTB does not use SSL acceleration. However, all Internetworking should use Secure HTTP.  Under end-to-end data protection principles, TLS encrypted traffic must be terminated on the target servers/services.  Akamai FastDNS should be used for DNS resolution. |  |

### Service Layer Controls

|  |  |  |  |
| --- | --- | --- | --- |
| **Domain** | **Control** | **Requirement** | **Solution Recommendation** |
| IAM | Authentication | Existing user accounts must be used and provisioned for Cloud access in lieu of creating new accounts for current users. New accounts must conform to Bank naming standards for login accounts. This requirement will apply except in those cases in which a unique account is required in the Cloud environment. |  |
| IAM | Authentication | Each user and process must be assigned a unique identifier that does not duplicate any current or previously used identifier. All identifiers must be given a name that enables ready traceability to a responsible ID holder or process name. |  |
| IAM | Federation | Access to off-premise cloud platforms will be authenticated on-premise and the identity assertion will be passed to the off-premise cloud service.   * Web Services * Management/Administration Console / Power Shell * API Access |  |
| IAM | Authentication | User login authentication must be password based in compliance with current Bank password standards, or key-based where such functionality is available. |  |
| IAM | Authentication | Cloud service provider personnel must not have any access to the resources, applications, services, or data that the Bank builds or manages and maintains the CSP environment. |  |
| IAM | Authentication | Multi-factor authentication techniques must be implemented for remote user access to cloud services and functionality. |  |
| IAM | Elevated Privilege | Elevated privileges must be restricted.  No user or process may have normally elevated privileges without a clearly proven and approved need. Approval for such privilege must be received from Bank Risk, Compliance, and Information Security.  "Break Glass" procedures must be established to enable elevated privilege on an emergency basis, governed by the Bank Problem Management Procedures and Protocols. |  |
| IAM | Provisioning | Provisioning of accounts and access must comply with Bank Information Security service level and operating level agreements. User accounts must not be re-used. |  |
| IAM | De-Provisioning | Terminated/Obsolete accounts must be disabled immediately on notification. The account must be retained in a disabeld state for forensic purposes for a period of at least 90-days. User accounts must not be re-used. |  |
| Trusted Platform | Asset Lifecycle Management | Provide the capability for the bank to adopt and use Asset Lifecycle Management (ALM) tools and processes to manage cloud assets, and maintain the same in the face of dynamic cloud scaling. |  |
| Trusted Platform | Configuration Management | Server builds should be based on established and pre-approved baseline security configurations with automated configuration validation on build and on a regular schedule thereafter. |  |
| Trusted Platform | Performance Management | Performance management and tuning must not negate or impair the operation or performance of information security solutions. |  |
| Data Loss Prevention | Secure Messaging | Provide the capability for all message payloads sent and received to be:  Encrypted both in transit and while stored, and;  Secured with authentication and access control mechanisms. |  |
| Data Loss Prevention | Version Controls | Implement the capability to facilitate version control on storage objects and source code including change records, and the capability to readily revert to a previous version in case of errors or other problems. |  |
| Data Loss Prevention | Backup Recovery | Provide the capability to encrypt backup data at rest using approved as per the Bank Cryptographic Materials and Handling Standard. |  |
| Encryption | Certificate Services | Provide the capability to create, manage and use certificates such as X.509 along with TLS. |  |
| Encryption | Key Management | Certificates must be stored in Venafi for tracking/life cycle purposes (not for issuing/management). |  |
| Encryption | Communica-tions | Provide/enable encryption for all networking; cross-server data movement; inter-application data movement that transfers Confidential and/or Restricted data, as per the FTB Information Classification and Handling Standard. |  |
| Encryption | Storage | Provide the capability for the Bank to encrypt storage to ensure all data on the drive is encrypted so senstivie data stored thereon cannot be accessed by an attacker, or by infrastructure management and support personnel. |  |
| Security Analytics | SIEM | Protect, retain, and manage the lifecycle of audit logs in compliance with applicable legal and regulatory obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach. |  |
| Security Analytics | SIEM | Provide the capability to integrate unaltered and decrypted network and server activity including server builds and configurations with the Bank SIEM. |  |
| Security Analytics | Alerts & Warning | Provide a dedicated resource on all shifts to monitor security as an extension of and in collaboration with the Bank Security Operations Center. |  |
| Security Analytics | Alerts & Warning | Bank Information Security must be notified of security breaches, alerts of policy violations, anomalies, and attacks affecting cloud services used by the Bank.  Bank must have the capability to manage the alerts and alert thresholds for each cloud instance. |  |
| Security Analytics | Forensics | Provide the capability to move hosts to isolated environments for forensic analysis in case of a security breach. |  |
| Business Continuity | Disaster Recovery | FTB cloud infrastructure, applications, and services must be architected and build to enable disaster recovery capability consistent with their FTB Recovery Rating. Application teams must have visibility for how their application / solution is architected and built so they can define required infrastructure, dependencies, and recovery approach. |  |
| Business Continuity | Auto Recovery | Provide the capability to recover an instance automatically, onto new hardware when a problem, hardware failure, or other interruption of service is detected. |  |
| Business Continuity | Auto Recovery | Provide automatic operational failure detection and health checking. |  |
| Business Continuity | Disaster Recovery | Disaster recovery exercises are required to validate recovery plans, application configurations, architectures, and recovery strategies for meeting the recovery expectations of the business without impact or impeding production.  Stand-Alone Exercises: Required prior to production implementation for any new applications / solutions or any existing solutions that have undergone material change such as new or changed infrastructure, process, etc. that impact recovery capability integrity.  Annual Exercise: Ability to participate in an annual exercise that validates the recovery of all applications / solutions that are supported in the cloud environment. |  |

### Compliance Layer Controls

|  |  |  |  |
| --- | --- | --- | --- |
| **Domain** | **Control** | **FTB Requirement** | **Solution Recommendation** |
| Network Threat Mitigation | IDS / IPS | All external network connectivity must be secured using an Intrusion Detection & Prevention solution approved by Bank Information Security with unaltered events and alerts securely generated and integrated with the Bank SIEM solution. |  |
| Trusted Platform | Identity & Access Management | The Provider must establish and regularly test and validate controls to prevent access to customer data by Provider personnel. |  |
| Trusted Platform | Identity & Access Management | Access of users and processes must be managed based on job function roles aligned with the FTB role-based access control program, representing the access requirements of each job function and in compliance with SOX divisions of labor where applicable (financial accounting and reporting functions). Access granted uniquely to individuals or processes/daemons must be limited and approved based on operational need or sensitivity of the function. |  |
| Trusted Platform | HIDS | Provide the ability for the bank to use a Host Intrusion Detection System to detect malicious activity.  Send alarms for each instance and log the malicious activity, especially in high-risk devices, or in those cases in which intrusion detection cannot adquately analyze/interpret the traffic.  Provide the ability for the HIDS to monitor and analyze network traffic, log files and file access on a host.  Unaltered events and alerts must be securely generated and integrated with the Bank SIEM solution. |  |
| Trusted Platform | Encryption | Provide the capability to fully encrypt customer storage. |  |
| Trusted Platform | Software Provisioning | All software must be subject to security scanning and testing by Information Security during development, pre-deployment, and post-deployment.  Static  Dynamic  Licensing  Open Source usage  Escrow  New and significantly changed applications are subject to a pre-production penetration test prior to production distribution. |  |
| Trusted Platform | Software Provisioning | Open source software must be documented, reviewed and approved by Information Security prior to distribution to production. |  |
| Trusted Platform | Software Provisioning | Entitlements access authorization must be implemented in applications to restrict access where there is a business requirement to segment records in a database for more specific control and administration (e.g., White Glove accounts). |  |
| Trusted Platform | Software Provisioning | Developers of internet facing applications are required to complete annual training on secure development practices. |  |
| Trusted Platform | Assurance | Provide customers with an annual detailed SOC 2 report from an independent auditor. |  |
| Data Loss Prevention | FTP | Anonymous FTP must not be used. Outbound anonymous FTP may only be used for serving information classified as public. |  |
| Data Loss Prevention | Rights Management | Safeguard sensitive information by applying protection to documents that persist outside the organization. Controls may include a combination of encryption, identity and authorization policies to secure files.  Provide a solution for labeling, handling, and security of data and objects which contain Bank resources. |  |
| Data Loss Prevention | Data Encryption | Data encryption to be applied at multiple levels (as appropriate, depending on the asset value) to protect sensitive information.  Data in Motion (DIM) – Applying encryption when data is traversing over networks.  Data at Rest (DAR) – Data stored in flat files, Databases, SAN, Desktops, Mobile etc.  Technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.  Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. |  |
| Data Loss Prevention | Data Masking | Production data must not be replicated or used in non-production environments. Otherwise, the non-production environment must be protected as a production-equivalent.  Obscuring or making specific data elements within data stores to ensure that sensitive data is replaced with realistic but not real data. The objective is to not make sensitive information available outside of the authorized environment. (E.g. Production). |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  | |  |

**E n d o f D o c u m e n t**