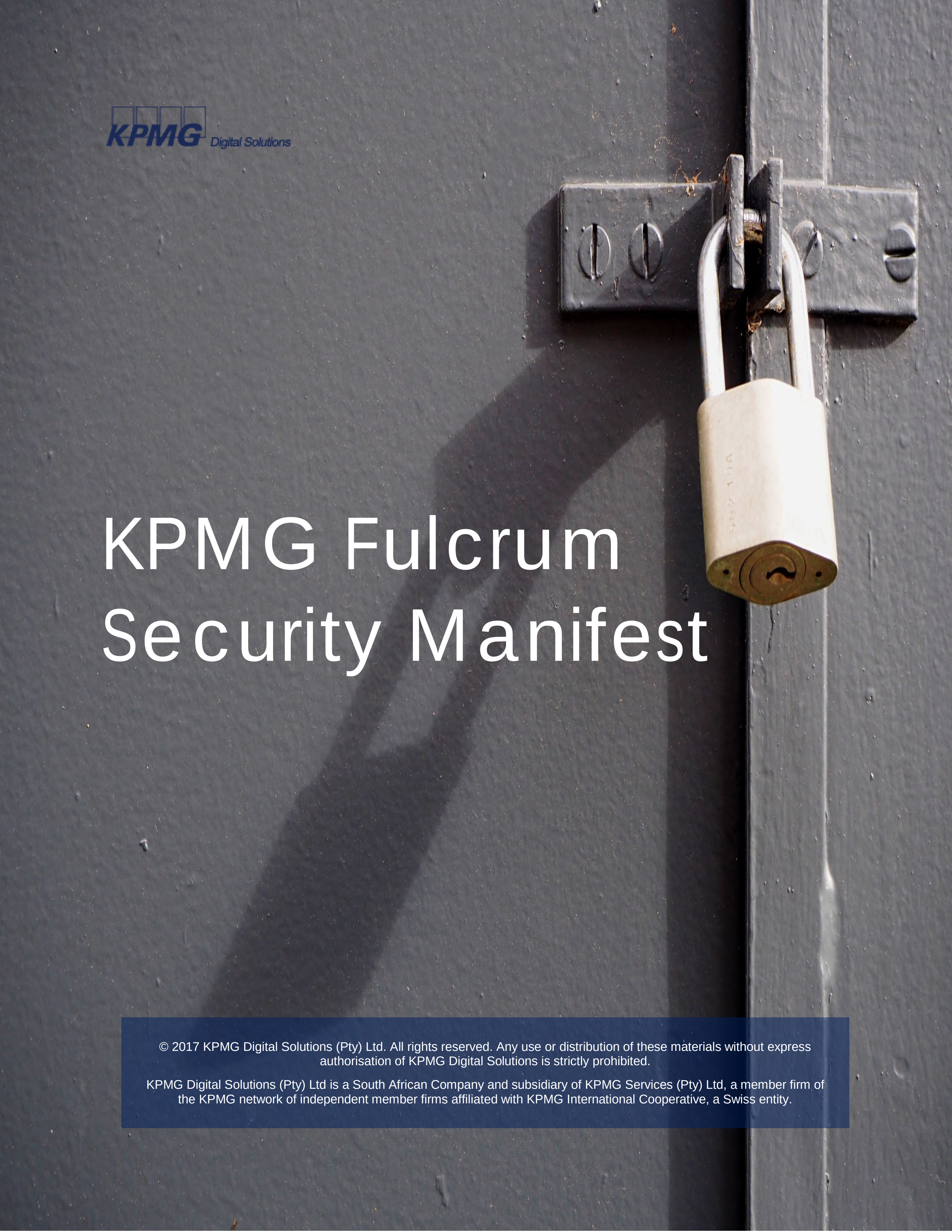

KPMG Digital Solutions

KPMG Fulcrum Security Manifest

KPMG DIGITAL SOLUTIONS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of KPMG Digital Solutions.

KPMG Digital Solutions may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from KPMG Digital Solutions, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by KPMG Digital Solutions. KPMG Digital Solutions cannot guarantee their accuracy and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

KPMG Services (Pty) Ltd is a South African Company and subsidiary of KPMG Services (Pty) Ltd, a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Introduction

KPMG Fulcrum is an innovative digital solution leveraging the power of the Cloud to help you change the way you see your business and your professional service provider. Fulcrum makes it simpler to access professional services and related apps quickly, conveniently and in the format you want whilst also giving you a unique approach to furthering your own digital ambitions by providing a platform on which to deploy and host your own apps.

We do all this while ensuring that you receive the data security and privacy, control and transparency you need to protect the information you or your employees put on the platform.

To make this possible, we apply very strict policies and processes to ensure that your data is secure – and protecting it remains a key focus for our team. At KPMG Digital, we are sensitive to the fact that our clients in many industries are bound by extensive regulations regarding the use, transmission and storage of data. Therefore, we're committed to being transparent about our approach to security so that you have peace of mind when trusting us with your company's sensitive information.

KPMG Fulcrum Security Features

Authentication / Authorisation:

- Users are able to self-provision accounts only on approved client domains.
- Password and user account management is strictly enforced according to KPMG Global Security Standards.

Enrolment and subscription:

- KPMG Fulcrum is designed to provide multi-factor authentication at the user level, where clients require this to be enforced.
- Access to all parts of KPMG Fulcrum are role-based access and easily manageable by client administrators from the secure client control panel.

Encryption:

- All data is encrypted at rest and in transit.

Service Continuity, Reliability

- Databases are replicated on a real-time basis with fail-over controls in place in the event that a primary data link becomes unavailable.
- Daily backups are performed as an additional control.

Log and Data Retention

- Logging of all critical transactions and user activity.
- Client data is hosted, archived and destroyed in accordance with data retention policies and privacy regulations.
- Clients have access to their own data and can request to export this at any time for storage on their own infrastructure.

Application Security

Given that KPMG Fulcrum operates as an Enterprise App Store that may include applications provided by third parties, we implement strict practices and that include the accreditation of applications deployed in our App Store. Some of the controls applied to all apps available on KPMG Fulcrum include:

- Applications and interfaces (APIs) are designed, developed and deployed in accordance with OWASP and adhere to applicable legal, statutory or regulatory compliance obligations.
- We use open and published APIs to ensure the broadest support for interoperability between components and to facilitate migrating applications.
- Data input and output integrity routines are implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data or misuse.
- Where data is exchanged between one or more apps, system interfaces, jurisdictions or external platforms, we apply strict technical measures and processes to prevent improper disclosure, alteration or destruction of client data.

Data Security

Each client's data is hosted on KPMG Digital's shared infrastructure and segregated logically by KPMG Fulcrum.

We maintain an inventory of and data flows for data that is resident (permanently or temporarily) within KPMG Fulcrum's geographically distributed applications and infrastructure to ascertain any regulatory, statutory or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data.

Production data is not replicated or used in non-production environments and we have applied security mechanisms to prevent data leakage.

All data is designated with stewardship, with assigned responsibilities defined, documented and communicated.

All unstructured data is available to clients and can be provided to them upon request in an industry-standard format (e.g., .doc, .xls, or .pdf) in order to facilitate processing outside of KPMG Fulcrum.

All data is transmitted using strong encryption. This includes data transmitted between clients and KPMG Fulcrum. KPMG Fulcrum implements the latest recommended secure cipher-suites to encrypt all traffic in transit, including use of TLS 1.2 protocols, AES256 encryption and SHA2 signatures. We monitor the changing cryptographic landscape and upgrade our cipher suite choices as the landscape changes, while also balancing the need for compatibility with older clients.

Data at rest on our production network is similarly encrypted.

Data Requests

Not unlike other Cloud-based Service Providers, we receive requests from users and government agencies to disclose or delete data other than in the ordinary operation and provision of our services. Our Data Request Policy addresses those issues and clearly outlines our policies and procedures for responding to such requests for customer data.

Secure Development Approach

Our Software Development Life Cycle (SDLC) has been designed to incorporate security into our development process – from the ground up. At the outset of each development effort, our teams assess the security risks according to our security schema. Before completion of the design phase, we undertake an assessment to qualify the security risk of the software that is intended to be deployed onto KPMG Fulcrum – whether this is a change, an integration or a new app. This risk analysis leverages the OWASP Top 10 to categorise every project as High, Medium or Low risk. Based on this analysis, we apply a set of requirements that must be met before the resulting product may be released to production.

All code is checked into a version-controlled repository. Code changes are subject to peer review and continuous integration testing. Any defects identified in this process are reviewed and followed to resolution before deployment to production.

Identity and Access Management

User access policies, procedures and have been implemented for ensuring appropriate identity, entitlement and access management for all users who have access to KPMG Fulcrum, whether as Fulcrum Administrators, Company Administrators or end users. These policies, procedures, processes and measures incorporate the following:

- Procedures and supporting roles and responsibilities for provisioning and de-provisioning user accounts
- Segmentation of access to sessions and data in our multi-tenant architecture
- Identity trust verification and service-to-service application (API) and information processing interoperability
- Account credential lifecycle management from instantiation through revocation
- Account credential and/or identity store minimisation or re-use across our apps
- Authentication, authorisation, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets)
- Permissions and supporting capabilities for client controls over authentication, authorisation, and accounting (AAA) rules for access to data and sessions on KPMG Fulcrum by their own personnel
- Adherence to applicable legal, statutory, or regulatory compliance requirements
- Segregation of duties across the shopping cart functionality with appropriate access controls to protect authoriser accounts

Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.

Provisioning user access to data is authorised by the management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, we inform our clients of this user access, especially if client data is used as part the service and/or our client has some shared responsibility over implementation of control.

User access is authorised and revalidated for entitlement appropriateness, at planned intervals.

Timely de-provisioning (revocation or modification) of user access to data is implemented as per established policies and procedures (where necessary this is modified to meet stricter controls required by our clients) and based on the user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Clients have access to a log of these changes.

Infrastructure Security

In order to deliver always-on, secure and scalable performance for KPMG Fulcrum, we work very closely with KPMG International (KPMGI) and Microsoft to leverage the full force of the Azure Cloud. The KPMG Cloud Central Project, managed by KPMGI delivers a secure, managed IaaS production hosting solution on Microsoft Azure. KPMGI has implemented a wide variety of security controls for the core infrastructure services. Control domains include boundary protection, perimeter, secure hosting, communication security, access control, security operations and operations management.

Microsoft offers state-of-the-art physical protection for the servers and related infrastructure that comprise the operating environment for KPMG Fulcrum. More information on how Microsoft manages security of the Azure platform is available at:

https://www.microsoft.com/en-us/TrustCenter/Security/AzureSecurity

Key Security Features

The following key controls exist to protect the KPMG Fulcrum infrastructure:

3rd Party Attestation:

- KPMGI maintains ISO27001 certification and undergoes annual SOC reviews

Network Security Groups (NSGs):

- Network Security Groups (NSGs) – stateful firewalls -control traffic (ingress and egress) on our Azure VNET.
- Implicit rules are disabled as they open access to the Internet and other VNETs. Explicit rules are defined instead. KPMGI worked with Microsoft to develop a custom solution (due to the removal of the implicit rules) to ensure some of the Microsoft services could be configured for proxy access.

Internet Access:

- Direct internet access (public endpoints) for individual VMs is not permitted. Internet related traffic is routed through forward and reverse proxy servers in the perimeter zone.

Isolation / Filtering:

- The KPMGI IaaS Azure infrastructure adheres to KPMG Global hosting zoning standards and applicable infrastructure controls.
- Symantec Endpoint Protection is installed on all servers.

Authentication / Authorisation:

- Identity services include separate forests for development, test, and production environments.
- Managed devices: authentication via SSO (where this is required by individual clients, otherwise the KPMG Fulcrum security layer handles sign-on).
- The Layer 7 handles authentication and authorisation to KPMG Fulcrum.

Enrolment and subscription:

- Multi Factor Authentication is enabled for Azure Account, Subscription and Operations. Access is limited to key personnel.

Encryption:

- BitLocker is the Windows Server component to encrypt local Disks (VHDs). All VHDs in production are encrypted.
- The Core Services leverages encryption. For example: Only HTTPS, SSH, DFSR, RDP, Kerberos, etc.

Key Vault:

- Key Vault encrypts keys and secrets (such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords) by using keys that are protected by in FIPS 140-2 Level 2 validated HSMs (hardware security modules).
- Keys are stored in a secure server on a segregated network with very limited access. Keys are never stored on the local system, but are delivered at process start time and retained only in memory while in use.
- Key Vault is designed so that Microsoft does not see or extract keys.

Logging and Monitoring:

- Monitoring uses gateways to SCOM and includes Azure Security Center monitoring.
- Palo Alto Network (PAN) devices monitor traffic (inbound and outbound).

Organisational Security

We have established an Information Security Management Program (ISMP) aimed at ensuring that our clients have the highest confidence that their data is protected – both by our systems and by our people. This program includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorised access, disclosure, alteration and destruction and covers the following areas:

- Risk management
- Security policy
- Organisation of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance

Polices and standards

Information security policies and procedures are in place and are readily available for review by all impacted personnel and external stakeholders. Information security policies are authorised by leadership and supported by a strategic business plan and our ISMP inclusive of defined information security roles and responsibilities for business leadership. Security documents include, but are not limited to:

- Information Security
- Classification, labelling, handling and destruction of information assets
- Acceptable Use of Information Systems
- Secure development, acquisition, configuration and maintenance of systems
- Systems Development Life Cycle (SDLC)
- Change Management
- Use of encryption
- Classification and handling of security incidents
- Business continuity and disaster recovery

Personnel Security

All employees, contractors and third parties are subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.

Employment agreements incorporate provisions and terms for adherence to established information governance and security policies and are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources and assets.

Our security awareness training program for all contractors, third-party users and employees covers a variety of topics, including:

- Data Security
- Acceptable Use of IT Systems and Data
- Protection Against Malicious Software

- Data Privacy
- Account Management
- Incident and Problem Management

We measure compliance to policies rigorously and require every employee to complete an annual declaration covering policy compliance, awareness, confidentiality and adherence to privacy standards.

A formal disciplinary or sanction policy exists for employees who have violated security policies and procedures.

Controls exist to mitigate and contain data security risks through proper separation of duties, role-based access and least-privilege access for all personnel across supply chain (internal, contractors, consultants, third party application providers, etc).

Change Control

We have implemented a strict program to systematically monitor and evaluate all software development to ensure that standards of quality and security baselines are being met. Quality evaluation and acceptance criteria for information systems, upgrades and new versions are rigorously applied, and tests of the system(s) are carried out both during development and prior to acceptance to maintain security.

Our application architects have clear oversight capacity in the quality testing process, with the final product being certified as "fit for purpose" and "right first time" prior to release. We have also incorporated technical security reviews (i.e., vulnerability assessments and penetration testing) to remediate any vulnerabilities that pose an unreasonable business risk or risk to our clients prior to release.

Supporting IT governance and service management-related business processes have been implemented for managing the risks associated with applying changes to business-critical or client-impacting apps and system-system interface designs and configurations, as well as infrastructure network and systems components. Technical measures operate to provide assurance that, prior to deployment, all changes directly correspond to a registered change request, business-critical risk analysis, validation of expected outcome in staged environment, pre-authorisation and notification to clients (where relevant) as per agreement (SLA).

Workstation Security

All workstations issued to employees are configured by KPMG to comply with global standards for security. These standards require all workstations to be properly configured, kept updated, run monitoring software and be tracked by KPMG’s endpoint management solution. KPMG’s default configuration sets up workstations to encrypt data, have strong passwords and lock when idle. Workstations run up-to-date monitoring software to report potential malware and unauthorised software and mobile storage devices.

Incident Management

We have implemented process to ensure that all affected clients are made aware of security incidents through electronic methods (e.g. portals).

Audit and Assurance

We perform annual internal assessments of conformance and effectiveness of its policies, procedures and supporting measures and metrics.

Independent reviews and assessments are performed at least annually, to ensure our ongoing compliance with established policies, procedures and known contractual, statutory, or regulatory compliance obligations.

Third-party service providers are required to demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in third-party contracts. Third-party reports, records and services undergo audit and review at planned intervals to govern and maintain compliance with the service delivery agreements.