SoftLayer Technologies, Inc.
Infrastructure as a Service (IaaS)

Report on SoftLayer Technologies, Inc.'s Infrastructure as a Service (IaaS) System
Relevant to the Security and Availability Principles

For the period May 1, 2017 to April 30, 2018

Prepared in Accordance with:
AT-C 205 pursuant to *TSP section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria, issued March 2016)*

Table of Contents

I. Report of Independent Accountants 1

II. Management of SoftLayer Technologies, Inc.'s Assertion 2

III. SoftLayer Technologies, Inc,'s Description of its Infrastructure as a Service (IaaS) System 3

IV. Attachment A - AICPA Trust Services Principles and Criteria 11

Report of Independent Accountants

To the Management of SoftLayer Technologies, Inc.:

We have examined the accompanying management assertion of SoftLayer Technologies, Inc. titled "Management of SoftLayer Technologies, Inc.'s Assertion" ("assertion") that SoftLayer Technologies, Inc. maintained effective controls over the SoftLayer Technologies, Inc. Infrastructure as a Service (IaaS) system ("system") that were suitably designed and operating effectively throughout the period May 1, 2017 to April 30, 2018 to provide reasonable assurance that SoftLayer Technologies, Inc.'s commitments and system requirements were achieved based on the criteria relevant to the security and availability principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*AICPA, Trust Services Principles and Criteria, issued March 2016*) ("applicable trust services criteria") and included as Attachment A. SoftLayer Technologies, Inc. management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes (1) obtaining an understanding of SoftLayer Technologies, Inc.'s relevant controls over the security and availability of the SoftLayer Technologies, Inc. IaaS system, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become ineffective.

In our opinion, management's assertion referred to above is fairly stated, in all material respects.

PricewaterhouseCoopers LLP

July 30, 2018

PricewaterhouseCoopers LLP, PricewaterhouseCoopers Center, 300 Madison Avenue, New York, NY 10017
T: (646) 471 3000, F: (813) 286 6000, www.pwc.com/us

SoftLayer Technologies, Inc.
14001 North Dallas Parkway,
Suite M100
Dallas, Texas 75240

Management of SoftLayer Technologies, Inc.'s Assertion

Based on our evaluation, we confirm to the best of our knowledge and belief that SoftLayer Technologies, Inc. maintained effective controls over the SoftLayer Technologies, Inc. Infrastructure as a Service (IaaS) system ("system") that were suitably designed and operating effectively throughout the period May 1, 2017 to April 30, 2018 to provide reasonable assurance that SoftLayer Technologies, Inc. 's commitments and system requirements were achieved based on the criteria relevant to the security and availability principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria, issued March 2016)* ("applicable trust services criteria") and included as Attachment A. Our attached description of the system identifies the aspects of the system covered by our assertion.

SoftLayer Technologies, Inc.

III. SoftLayer Technologies, Inc.'s Description of its Infrastructure as a Service (IaaS) System

A. System Overview

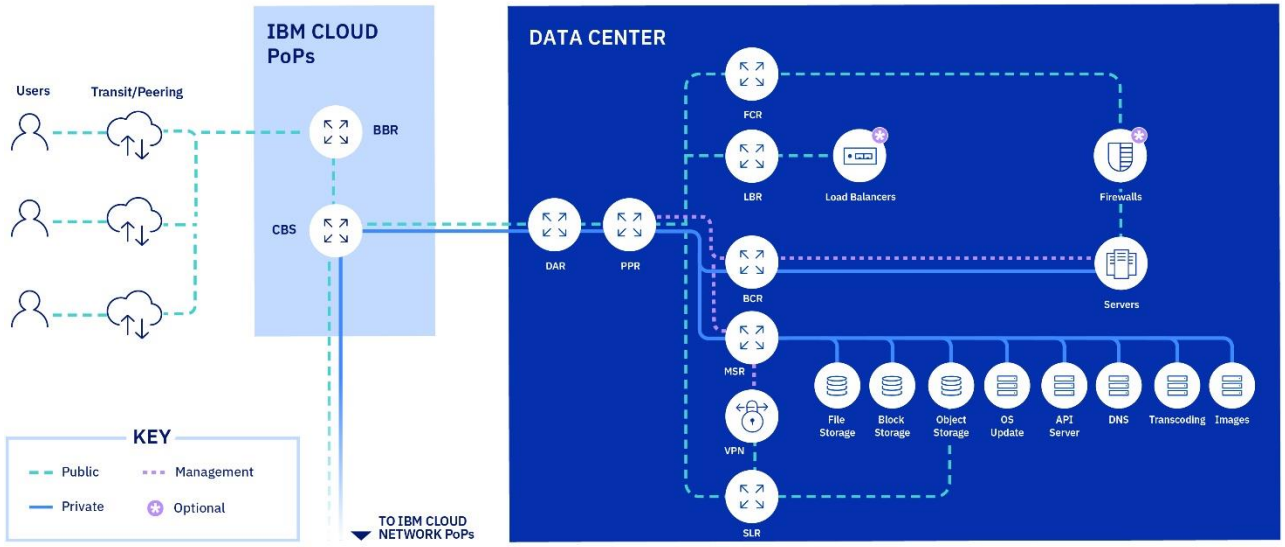
Background

SoftLayer Technologies, Inc., also referred to as "IBM SoftLayer," "SoftLayer," or "Bluemix IaaS," an IBM Company, provides on-demand cloud infrastructure as a service (IaaS) to its customers, allowing them to create scalable bare metal server, virtual server, or hybrid computing environments, via SoftLayer's Customer Portal, leveraging global data centers and points of presence (PoP).

SoftLayer's IaaS is built using a Network-Within-A-Network topology that provides remote access to allow customers the ability to build and manage computing environments remotely. SoftLayer's "Network-Within-A-Network" configuration includes three (3) network interfaces. Public, private, and management traffic travel across separate network interfaces, segregating and securing traffic while streamlining management functions.

- Public Network - Network traffic from anywhere in the world will connect to the closest network PoP, and it will travel directly across the network to its data center, minimizing the number of network hops and handoffs between providers.
- Private Network - Provides a connection to the customer's servers (bare metal or virtual) in SoftLayer data centers around the world. Data can be moved between servers through the private network; and customers can utilize various services, update and patch servers, software repositories, and backend services, without interfering with public network traffic.
- Management Network - Each server within the SoftLayer IaaS is connected to the management network. This out-of-band management network, accessible via VPN, allows access to each server for maintenance and administration, independent of its CPU and regardless of its firmware or operating system.

Public, Private and Management Network Diagram:



SoftLayer delivers its IaaS through the Internal Management System (IMS) system, which is an internally developed customer relationship management (CRM) system used to track customers' hardware and services. IMS allows customers to manage their cloud environments. Customer capabilities include management of system and network devices provisioned by the customer, account management, ordering and deployment, and customer support.

IMS has two components: IMS, as viewed by internal employees, and the Customer Portal, as available to users of SoftLayer's IaaS. The Customer Portal allows customers to:

- Create and manage tickets for incident response and resolution
- Review account information
- View information and certain configuration data regarding their purchased solutions
- Perform functions such as OS reloads, and access RescueLayer
- Maintain customer provisioned firewall and DNS configurations that affect their bare metal servers
- Purchase or upgrade services to initiate the automated provisioning process for new systems

Customers build their environments using virtual servers and/or bare metal servers.

- Virtual servers are computing "instances" that are complete computing environments that include a full hardware and software stack accessed and controlled over the Internet. The computing resources can be scaled on demand, adding or resizing instances as needed, but without having to purchase physical systems. Public and private virtual nodes are available.
- Bare metal servers are dedicated physical servers. Bare metal servers allow direct access to physical hardware to support high demand and processor-intensive workloads.

SoftLayer personnel also have access to IMS to set up and configure purchased solutions, assist in troubleshooting technical issues, and respond to customer requests.

Boundaries of the System

This report covers the services managed by SoftLayer, including global data center physical locations, the IMS portal and the supporting infrastructure devices. Additionally, this report includes network devices that are managed by SoftLayer supporting the IMS portal and infrastructure including hypervisors, and network devices that support customer environments but are not provisioned/managed by customers within the SoftLayer IaaS. The report includes supporting services to the virtual and bare metal services, such as storage. These devices can be locally attached, accessible by API (such as Public Cloud Object Store), or accessible via a storage area network. Cloud Object Storage is an IaaS service with devices locally attached, residing in the SoftLayer control row. The SoftLayer IMS system provides the underpinning for user and storage instance provisioning. The Cloud Object Storage Bluemix provisioning path including the COS Broker are not included within the IaaS system boundary.

The Storage Area Network (SAN) is architecture to attach remote computer storage devices to servers in such a way that, to the operating system, the devices appear as locally attached. Within each customer environment, servers, VMs and other systems/devices are managed by SoftLayer's customers and are not included within the boundaries of the system. This report does not extend to the workloads (data, files, information) sent by SoftLayer IaaS customers to the SoftLayer IaaS system. The integrity and conformity with regulatory requirements of such data are solely the responsibility of the applicable SoftLayer IaaS customer. Additionally, this report does not extend to business process controls, automated application controls, or key reports.

The accompanying description includes only those controls directly impacting SoftLayer's IaaS and customers' hosting environments utilizing SoftLayer's IaaS, and does not include controls over other services. SoftLayer also provides enterprise-class tools to help mitigate potential security risks and ensure availability. Tools provided by SoftLayer include, but are not limited to, load balancing, intrusion detection and prevention, standard and dedicated hardware firewalls, anti-virus, anti-spyware, anti-malware, VeriSign® and GeoTrust® SSL Certificates. This report does not extend to controls over SoftLayer's other services and tools.

Components, infrastructure, network devices, software, and data center locations within the scope of the system:

<table>
<tr><th>Service Offering</th><th>Data Center / Hardware Locations</th><th>Network</th><th>Operating System Infrastructure</th><th>System Software</th><th>Applications</th><th>Customer Data</th></tr>
<tr><td rowspan="3">IBM SoftLayer IaaS</td><td rowspan="3">41 data centers (See Infrastructure section below)</td><td>Customer provisioned and managed network devices, firewalls and VPNs are solely the responsibility of the customer and are not within the boundaries of the system.</td><td colspan="3" rowspan="2">Customer environments (including the development and maintenance) provisioned and managed using the Customer Portal, including OS, system software, and applications are solely the responsibility of the customer and are not within the boundaries of the system.</td><td rowspan="3">Customer data is solely the responsibility of the customer and is not within the boundaries of the system.</td></tr>
<tr><td>Network devices supporting customer managed environments and managed by SoftLayer are within boundaries of the system including:
Routers, Switches, Firewalls, VPNs</td></tr>
<tr><td>Network devices directly in support of the IMS portal are within the boundaries of the system including:
Routers, Switches, Firewalls, VPNs</td><td>Operating systems directly in support of the IMS portal are within boundaries of the system including:
Linux, UNIX, Windows, CentOS</td><td>System software directly in support of the IMS portal are within boundaries of the system including:
Radius, Citrix, Active Directory</td><td>Internal Management System (IMS)/ Customer Portal</td></tr>
</table>

B. System Components

Infrastructure

SoftLayer provides Infrastructure as a Service (IaaS) using multiple telecom service providers for backbone connectivity and multiple co-location management providers for data center facility management. Refer to the table below for a list of data center vendors that provide facility management services in the SoftLayer facilities included within the scope of this report.

Facility *	Physical Location	Facility Manager
AMS01	Amsterdam, Netherlands	Digital Realty
AMS03	Almere, Netherlands	KPN
CHE01	Chennai, India	TATA
DAL01	Dallas, TX	Flexential
DAL02	Dallas, TX	SoftLayer
DAL05	Dallas, TX	Digital Realty
DAL06	Dallas, TX	SoftLayer
DAL07	Plano, TX	SoftLayer
DAL08	Richardson, TX	Digital Realty
DAL09	Richardson, TX	Digital Realty
DAL10	Irving, TX	QTS
DAL12	Richardson, TX	Digital Realty
DAL13	Carrollton, TX	Cyrus One
FRA02	Frankfurt, Germany	Zenium Technology
HKG02	Hong Kong, China	Digital Realty
HOU02	Houston, TX	SoftLayer
LON02	Chessington, London	Digital Realty
LON04	Farnborough, UK	Ark Data Centres
LON06	Slough, UK	Zenium Technology

Facility *	Physical Location	Facility Manager
MEL01	Melbourne, Australia	Digital Realty
MEX01	Queretaro, Mexico	Alestra
MIL01	Milan, Italy	DATA4
MON01	Montreal, Canada	COLO-D
OSL01	Oslo, Norway	EVRY
PAR01	Paris, France	Global Switch
SAO01	Sao Paulo, Brazil	Ascenty
SEA01	Tukwila, WA	Internap
SEO01	South Korea	SK C&C
SJC01	Santa Clara, CA	Digital Realty
SJC03	Santa Clara, CA	Digital Realty
SJC04	Santa Clara, CA	Infomart
SNG01	Jurong East, Singapore	Digital Realty
SYD01	Sydney, Australia	Global Switch
SYD04	Erskine Park, Australia	Digital Realty
TOK02	Tokyo, Japan	@Tokyo
TOR01	Ontario (Markham), Canada	Digital Realty
WDC01	Chantilly, VA	Digital Realty
WDC03	Ashburn, VA	Digital Realty
WDC04	Ashburn, VA	Digital Realty
WDC06	Ashburn, VA	Sabey
WDC07	Ashburn, VA	Raging Wire

* Note: Only those data centers that were operational and hosting customer servers for at least six (6) months are considered in scope for this report.

Customers with bare metal, virtual, or hybrid environments can access the servers remotely (electronically) from anywhere in the world. Certain facilities (i.e., DAL02, DAL07 and HOU02) house both co-location servers and Infrastructure as a Service (IaaS) related servers. Co-location customers do not have logical or physical access to the SoftLayer Infrastructure as a Service (IaaS) system. As such, co-location cages housing customers' servers are not included within the boundaries of the system.

Software

SoftLayer IaaS customers are solely responsible for customer owned and managed software and applications as these components are not within the boundaries of the system. SoftLayer IaaS does not maintain responsibility for customer software and applications that SoftLayer IaaS customers run on their bare metal, virtual, or hybrid environment; the software and applications are the responsibility of SoftLayer IaaS customers.

For components of the environment managed by SoftLayer IaaS, software systems are managed centrally by SoftLayer using consistent controls and processes. SoftLayer manages the Customer Portal (IMS), IMS infrastructure and operating systems, network devices supporting IMS and certain network devices supporting customer environments within the SoftLayer environment.

People

Key SoftLayer positions of authority and responsibility are documented in a formal organizational chart via IBM's BluePages, which evidences key organizational structures and reporting lines. The organizational chart is reviewed by HR and updated periodically for accuracy by managers.

Within the organization, roles and responsibilities are defined and communicated. SoftLayer leverages participation from multiple organizational levels, sites, locations, geographies and organizations are involved, as required, to perform the day-to-day oversight of service delivery related functions, matters, responsibilities and issues. Functional roles may be combined within management positions to deliver services in a cost effective manner.

The SoftLayer IaaS teams are diverse teams of development and operations professionals, which maintain and follow IBM's industry leading processes, standards and procedures in the execution of their work. Security and availability requirements are generated from senior management. These requirements are distributed to the operational management leaders. These leaders are responsible for the implementation and monitoring of security controls.

The General Manager of Cloud Infrastructure Services oversees daily operations and reports to the Senior Vice President IBM Watson & Cloud Platform. Supporting the GM are Tribe Leaders, Directors and Vice Presidents that manage and perform the daily operations of SoftLayer. These core competencies have been established to provide full capabilities to serve customers worldwide. Functional and administrative responsibilities are broadly defined and communicated through organizational charts, which are reviewed and updated regularly.

Procedures

Customers are provided and required to agree to a Cloud Service Agreement (CSA) during the ordering process. The CSA acts as the formal contract and usage policy for customer users of the SoftLayer IaaS system. The CSA documents the contractual obligations of SoftLayer and the customers using SoftLayer IaaS. Any updates to the CSA are communicated to the existing customers through the Customer Portal.

The policies and procedures are a series of documents, which are used to describe the controls implemented within the SoftLayer IaaS system. The purpose of the policies and procedures is to describe the environment and define the practices performed on behalf of the customer. The policies and procedures include diagrams and descriptions of the network, infrastructure, environment and SoftLayer's commitments. These policies and procedures are available to all SoftLayer employees that support the SoftLayer IaaS system. Additionally, each of the policies and procedures are reviewed by SoftLayer management on a periodic basis, per the defined policy.

Data

The integrity and conformity with regulatory requirements of workloads sent to the SoftLayer IaaS system are solely the responsibility of SoftLayer IaaS customers. SoftLayer IaaS does not maintain responsibility for the data SoftLayer IaaS customers store on their bare metal, virtual, or hybrid environment. The data is the responsibility of SoftLayer IaaS customers.

Attachment A - AICPA Trust Services Principles and Criteria

This attachment includes the Trust Services Criteria included in the scope of the engagement relevant to the security and availability principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*AICPA, Trust Services Principles and Criteria, issued March 2016*) ("applicable trust services criteria").

Criteria

Ref	Criteria
CC1.0	**Common Criteria Related to Organization and Management**
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security and availability.
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security and availability.
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities.
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security and availability.
CC2.0	**Common Criteria Related to Communications**
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.
CC2.2	The entity's security and availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and availability of the system, is provided to personnel to carry out their responsibilities.

CC2.5	Internal and external users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security and availability are communicated to those users in a timely manner.
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**
CC3.1	The entity (1) identifies potential threats that could impair system security and availability commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.
CC4.0	**Common Criteria Related to Monitoring of Controls**
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability.
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security and availability.

CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and availability.
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and availability.
CC5.6	Logical access security measures have been implemented to protect against security and availability threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security and availability.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security and availability.
CC6.0	**Common Criteria Related to System Operations**
CC6.1	Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security and availability.
CC6.2	Security and availability incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.
CC7.0	**Common Criteria Related to Change Management**
CC7.1	The entity's commitments and system requirements, as they relate to security and availability, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security and availability.
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security and availability.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security and availability commitments and system requirements.
Additional Criteria for Availability	

A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.