A-LIGN

A-LIGN.com

Type 1 SOC 2

Prepared for:
iM Critical

Year:
2025

REPORT ON IM CRITICAL'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN OF ITS CONTROLS RELEVANT TO SECURITY AND AVAILABILITY

Pursuant to Reporting on System and Organization Controls 2 (SOC 2)
Type 1 examination performed under AT-C 105 and AT-C 205

September 9, 2025

Table of Contents

SECTION 1

ASSERTION OF IM CRITICAL MANAGEMENT

ASSERTION OF IM CRITICAL MANAGEMENT

September 17, 2025

We have prepared the accompanying description of iM Critical's ('the Company') Data Center Services System titled "iM Critical's Description of Its Data Center Services System as of September 9, 2025" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the Data Center Services System that may be useful when assessing the risks arising from interactions with iM Critical's system, particularly information about system controls that iM Critical has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The description indicates that complementary user entity controls that are suitably designed are necessary to achieve iM Critical's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of iM Critical's controls.

We confirm, to the best of our knowledge and belief, that:

a. the description presents iM Critical's Data Center Services System that was designed and implemented as of September 9, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of September 9, 2025, to provide reasonable assurance that iM Critical's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the user entities applied the complementary controls assumed in the design of iM Critical's controls as of that date.

Jonathan Cox

Jonathan Cox
CISO
iM Critical

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: iM Critical

Scope

We have examined iM Critical's accompanying description of its Data Center Services System titled "iM Critical's Description of Its Data Center Services System as of September 9, 2025" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design of controls stated in the description as of September 9, 2025, to provide reasonable assurance that iM Critical's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at iM Critical, to achieve iM Critical's service commitments and system requirements based on the applicable trust services criteria. The description presents iM Critical's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of iM Critical's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

iM Critical is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that iM Critical's service commitments and system requirements were achieved. iM Critical has provided the accompanying assertion titled "Assertion of iM Critical Management" (assertion) about the description and the suitability of the design of controls stated therein. iM Critical is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description 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 our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

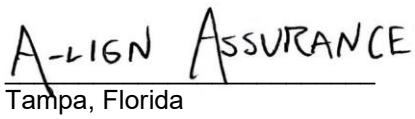
a. the description presents iM Critical's Data Center Services System that was designed and implemented as of September 9, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of September 9, 2025, to provide reasonable assurance that iM Critical's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the user entities applied the complementary controls assumed in the design of iM Critical's controls as of that date.

Restricted Use

This report is intended solely for the information and use of iM Critical, user entities of iM Critical's Data Center Services System as of September 9, 2025, business partners of iM Critical subject to risks arising from interactions with the Data Center Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.



Tampa, Florida
September 17, 2025

SECTION 3

IM CRITICAL'S DESCRIPTION OF ITS DATA CENTER SERVICES SYSTEM AS OF SEPTEMBER 9, 2025

OVERVIEW OF OPERATIONS

Company Background

iM Critical is a data center and managed infrastructure provider focused on delivering high-performance, secure, and resilient services to enterprises across regulated industries. Founded with the mission to bring innovation and agility to the infrastructure layer, iM Critical operates multiple purpose-built data centers with a focus on supporting hybrid, edge, and high-density computing needs.

The company's Miami Data Center, located at 100 NE 80th Terrace, Miami, Florida, is a newly launched, purpose-built facility spanning approximately 100,000 square feet, with ~5 MW of critical load capacity and modular growth to 40 MW. The facility supports collocation, managed infrastructure, and high-density compute workloads including HPC and AI/ML training, with direct access to subsea cables, carrier hotels, and major cloud providers.

iM Critical serves a broad range of industries, including:

- Financial Services
- Healthcare and Life Sciences
- Government and Public Sector
- Legal and Professional Services
- Technology and Media
- Educational Institutions

The company's data centers, and managed infrastructure solutions are backed by 24/7 on-site NOC/SOC operations, robust physical and logical security, and commitment to performance, sustainability, and compliance.

Description of Services Provided

iM Critical provides the Data Center Services System. iM Critical provides colocation, high-density compute hosting, and managed infrastructure services to enterprise clients and public sector organizations throughout the United States. Services are delivered from purpose-built data centers, including the newly constructed Miami Data Center, which serves as a hub for cloud, AI, HPC, and latency-sensitive workloads.

The Miami Data Center delivers the following core services:

- **Colocation services:** High-density cabinets and cages (up to 75 kW per rack), with customizable power, cooling, and security configurations
- **Managed infrastructure:** Support for private and hybrid cloud architectures, including managed bare metal, virtual machines, and storage
- **Connectivity solutions:** Carrier-neutral cross-connects, IP transit, metro rings, direct access to subsea cables and public clouds
- **Security services:** On-site SOC services, intrusion detection and response, managed firewalls, and physical security controls
- **Remote hands and NOC services:** 24/7 operational support, equipment installation, monitoring, and troubleshooting

Services are designed to support regulated and security-sensitive use cases, including HIPAA, GLBA, CJIS, and SOC 2-compliant deployments.

Customer infrastructure and data hosted at iM Critical facilities are accessible through secure, authenticated methods including direct cross-connects, Virtual Private Network (VPN), Transport Layer Security (TLS)-encrypted sessions, and customer-dedicated private network links. iM Critical's operations team collaborates with customers to ensure that uptime service level agreements SLAs, access controls, data privacy requirements, and incident response procedures are met or exceeded.

Principal Service Commitments and System Requirements

iM Critical designs and operates its Miami Data Center to meet high standards for availability, security, privacy, and performance. These objectives are guided by SLAs, industry best practices, regulatory compliance obligations, and the specific needs of iM Critical's enterprise and public sector clients.

The Data Center Services System's service commitments include:

- **High Availability and Resilience**: The facility is designed with concurrently maintainable power and cooling infrastructure, N+1 redundancy, dual utility feeds, and storm-hardened construction to ensure continuous operation during adverse conditions. Systems are monitored 24/7 by on-site NOC personnel.
- **Security and Access Control**: Physical security measures include perimeter fencing, access control zones, multifactor authentication (MFA) (including biometric readers), 24/7 on-site guards, and video surveillance. Logical access is managed through Role-Based Access Control (RBAC), Active Directory (AD) authentication, MFA, and documented access provisioning procedures.
- **Data Protection**: iM Critical uses encryption to protect customer data in transit and at rest (where applicable in managed service environments). Secure communication channels include TLS, VPN, and dedicated cross-connects. No unauthorized logical access is granted to client systems or data without prior authorization.
- **Compliance Alignment**: iM Critical's system policies and procedures are aligned with the requirements of SOC 2 Trust Services Criteria (Security, and Availability).
- **Operational Transparency**: Service commitments, including uptime SLAs, escalation procedures, and change management policies, are detailed in customer contracts and reviewed during onboarding. Customers are provided with change notifications, access logs, and operational reports as defined by their agreements.

System requirements supporting these commitments include:

- Documented security and operational policies accessible to staff via internal systems
- Defined change management and incident response procedures
- Periodic vulnerability scans and third-party penetration tests
- Regular capacity and utilization reviews for critical infrastructure (power, cooling, bandwidth)
- Formal onboarding, training, and background screening for employees with privileged access

iM Critical's system of controls supports customers' ability to meet their own risk management, security, and audit obligations when colocating or hosting systems within the Miami Data Center.

Components of the System

Infrastructure

The infrastructure supporting iM Critical's Data Center Services System includes physical, power, cooling, and network systems designed to support high-density and mission-critical workloads:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Electric UPS Systems	Power Redundancy	Provides clean, uninterruptible power during utility outages
Diesel Generators (N+1)	Backup Power	Ensures continued operations during sustained power loss
Computer Room Air Handlers (CRAH) Units with Hot/Cold Aisles	Heating, Ventilation, and Air Conditioning (HVAC) / Cooling	Regulates temperature and humidity to protect equipment

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Biometric and Card Access Readers	Physical Security	Controls and monitors facility access
Structured Cabling and Fiber Plant	Network Interconnect	Enables internal and external cross-connects and diverse fiber entry
Closed-circuit television (CCTV) and Monitoring Sensors	Environmental and Security	Monitors physical space, logs entries, and provides visual surveillance

Software

While the Miami Data Center is primarily an infrastructure facility, the Data Center Services System uses a suite of software tools for infrastructure management, monitoring, and security:

Primary Software		
Software	**Operating System**	**Purpose**
Data Center Infrastructure Mgmt.	Windows	Monitors power, temperature, environmental health, and capacity
Building Management System (BMS)	Embedded / Proprietary	Controls and automates lighting, HVAC, and facility environment
Access Control Platform	Proprietary	Manages access provisioning, authentication, and physical logs

People

The Miami Data Center is supported by iM Critical's personnel organized across several core operational disciplines:

- **Facilities and Engineering**: Maintains building infrastructure, power, HVAC, and monitors critical systems. Engineers are on-site 24/7 for immediate response and preventative maintenance.
- **Network and Connectivity Team**: Manages interconnects, carrier relations, Border Gateway Protocol (BGP) peering, and fiber plant infrastructure.
- **Security Operations Center (SOC)**: Monitors alerts, reviews access logs, responds to incidents, and manages intrusion detection systems.
- **Network Operations Center (NOC)/ Technical Operations**: Provides customer support, remote hands, equipment installation assistance, and monitors uptime and SLAs.
- **Compliance and Risk Team**: Maintains SOC 2 controls, coordinates audits, and supports customer compliance initiatives.
- **Support Staff**: Administrative and customer experience staff manage contracts, scheduling, and customer communications.

Data

iM Critical's Miami facility is primarily a collocation and infrastructure provider and does not process or store end-customer data directly. However, the system components generate and manage operational data, including:

- Access control logs (badge, biometric, PIN access attempts)
- Video surveillance footage (CCTV with retention per policy)
- Network telemetry (traffic patterns, port activity, bandwidth utilization)
- Infrastructure logs (power consumption, cooling status, system health)
- Incident and change management records (tickets, resolutions, audit trails)

Data relevant to facility operations is stored securely and retained in accordance with iM Critical's internal data retention policies and customer contractual requirements.

Processes, Policies and Procedures

iM Critical maintains formal, documented policies and procedures that govern the secure and reliable operation of its Miami Data Center. These policies span physical security, logical access, data communications, infrastructure management, and operational practices. Policies are reviewed annually and updated as necessary by leadership and compliance personnel.

Physical Security

The Miami Data Center employs a multi-layered physical security model designed to control and monitor access to the facility and protect client equipment and infrastructure. Controls include:

- **Perimeter Protection**: The facility is enclosed by a gated perimeter with access controlled via secure entry points.
- **Access Control Systems**: Entry is granted through a combination of key card and biometric hand geometry readers. Doors are zoned and monitored by an access control list system.
- **24/7 On-Site Security**: Security personnel monitor ingress/egress and perform regular patrols. A staffed reception area controls visitor access.
- **Visitor Management**: Visitors present government-issued ID, sign in, and be escorted by authorized personnel. Temporary visitor badges do not permit unescorted access.
- **Surveillance**: High-definition CCTV cameras cover critical areas, including entrances, data halls, mechanical rooms, and exterior perimeters, with footage retained per policy.
- **Access Reviews**: Quarterly and semi-annual reviews of employee and vendor access are conducted. Access cards are tracked and deactivated promptly upon termination.

Logical Access

Logical access to internal systems that support operations at the Miami facility is governed by:

- **RBAC**: System access is granted based on least privilege and specific job roles.
- **Authentication**: Staff access is authenticated using AD credentials. Remote access requires MFA using token-based systems.
- **Access Provisioning and Revocation**: User accounts are created via HR onboarding workflows and terminated via automated access deletion requests. Daily termination reports are reviewed by IT.
- **Privileged Access Monitoring**: Elevated access roles are reviewed by the Chief Information Security Officer (CISO) and relevant stakeholders on a quarterly basis.
- **Password Policies**: Strong password requirements are enforced across systems, with automatic lockouts and session timeouts after periods of inactivity.

Computer Operations - Backups

At the time of this report, iM Critical is in the process of finalizing the implementation of backup controls at the Miami Data Center. These controls are expected to be fully operational within 30 to 60 days as part of the integration with a contracted Managed Services Provider (MSP). Once implemented, the backup process will include:

- **Infrastructure Data**: Regular backups of infrastructure configurations, monitoring logs, and system state data to ensure recoverability of operational environments.
- **Media Security**: Physical backup infrastructure will reside in restricted-access areas. Optional off-site backup services will be managed by a certified third-party provider under formal agreements, with activity logged and reviewed.
- **Access Restrictions**: Access to backup systems and stored media will be strictly limited to authorized personnel, with access governed by documented role-based access controls.

Computer Operations - Availability

iM Critical's Miami Data Center was constructed with N+1 redundancy for power, cooling, and network infrastructure. Operational availability controls and monitoring procedures are in the final stages of deployment and are expected to be fully in place within 30 to 60 days. These include:

- **Monitoring and Alerting**: Implementation of real-time monitoring for temperature, power, and connectivity metrics, integrated into a centralized alerting platform.
- **Patch Management**: A structured patch management process is being formalized to ensure timely updates to infrastructure systems, incorporating risk-based scheduling and post-deployment validation.
- **Incident Response**: An incident response framework, aligned to industry best practices, is under development and will be used to document, assess, and respond to IT incidents affecting infrastructure availability.

Change Control

A documented change management process is being implemented in collaboration with the MSP. This process will govern infrastructure, system, and security changes, and is expected to be fully operational within the next 60 days. The process will include:

- **Change Requests**: Changes will be initiated and tracked through a centralized platform, with approvals and rollback plans defined prior to implementation.
- **Testing and Validation**: Changes with production impact will be tested in a controlled environment where feasible, and validated for operational impact prior to deployment.
- **Version Control**: Configuration and code changes will be maintained in version-controlled repositories to support traceability and rapid rollback in the event of failure.

Data Communications

Data communication and perimeter security controls at the Miami Data Center are currently in deployment and scheduled for completion within 30 to 60 days. The planned capabilities include:

- **Firewalls**: Firewall appliances will be configured to permit only approved traffic flows, following least-privilege principles.
- **NAT and IP Segmentation**: Internal addressing schemes will be protected using Network Address Translation (NAT), along with segmentation of administrative and customer infrastructure.
- **VPN Access**: Remote administrative access will require MFA and secure VPN tunnels with logging and timeout controls.
- **Penetration Testing**: Annual third-party penetration tests are planned beginning in the current audit period, simulating both internal and external threat scenarios.
- **Vulnerability Scanning**: Quarterly vulnerability assessments will be conducted by a third-party provider, with remediation tracked and rescans scheduled as-needed.

Boundaries of the System

The scope of this report includes the Data Center Services System performed in the Miami, Florida facilities.

Included in Scope

The following components and services fall within the boundaries of the system for this assessment:

- **Physical infrastructure and facility operations:**
  - Power, cooling, physical security, fire suppression, and building controls
  - Biometric and card-based access systems
  - CCTV and environmental monitoring systems
- **Logical infrastructure and supporting systems:**
  - Access control platforms (physical and logical)
  - Network segmentation and perimeter security systems
  - Managed network services provided by iM Critical
  - Centralized monitoring, ticketing, and change management systems
- **Personnel and operational support:**
  The system includes personnel and functions that support the secure and continuous operation of the Miami Data Center:
  - Facilities and Engineering Staff: iM Critical personnel are responsible for maintaining critical infrastructure systems such as power, cooling, and physical security. These staff are currently on-site and provide day-to-day oversight of environmental systems and building operations.
  - MSP-Provided NOC and SOC Services: NOC and SOC services will be delivered by a contracted MSP. The MSP is scheduled to be fully integrated within 30 to 60 days of this report and will assume responsibility for 24/7 monitoring, alert response, incident triage, and security event management. The MSP will maintain a dedicated on-site presence at the Miami facility.
  - Support and Compliance Functions: iM Critical's internal support teams provide customer onboarding, ticketing system administration, and compliance oversight. These roles coordinate with the MSP to ensure that operational controls are aligned with SLAs and regulatory requirements.
- **Data relevant to facility operations**
  - Access logs, surveillance footage, environmental sensor data, and system alerts
  - Monitoring data and incident/change management records
  - Configuration data for core infrastructure systems

Excluded from Scope

The following elements are outside the system boundaries for this SOC 2 engagement:

- Customer-owned systems and data:
  - iM Critical provides colocation and infrastructure hosting services; it does not access or manage the data, applications, or virtual environments deployed by customers unless under separate managed service agreements (which are currently outside the scope of this report).
  - Clients are responsible for the security, access control, and compliance of their own systems hosted within the facility.
- Other iM Critical facilities:
  - This assessment does not include iM Critical data centers in other geographic locations or corporate office environments outside of Miami.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

The control environment at iM Critical is grounded in a commitment to ethical behavior and operational integrity. These values guide the organization's approach to delivering secure and reliable infrastructure services from the Miami Data Center. Ethical expectations are set through formal policy and reinforced through culture and daily operations.

Control activities include:

- iM Critical maintains documented policy statements and an employee handbook outlining expected standards of conduct.
- Employees sign an acknowledgment of receipt and understanding of the handbook, including confidentiality obligations.
- A confidentiality statement, which covers customer data and internal proprietary information, is included as part of onboarding.
- Background checks are conducted on employees prior to hire.

Commitment to Competence

iM Critical defines competence as the combination of knowledge, skills, and experience required to effectively carry out assigned duties. Position descriptions are aligned with these expectations, and ongoing training supports staff development.

Control activities include:

- Job descriptions and role definitions incorporate required qualifications and skill levels.
- Technical and compliance training is provided based on role, and ongoing training is scheduled as operational requirements evolve.

Management's Philosophy and Operating Style

The organization's management team maintains a proactive approach to operational risk, compliance, and information security. They remain engaged with industry standards and emerging threats and prioritize accountability and transparency in decision-making.
Control activities include:

- Management is briefed on regulatory and industry developments affecting colocation and infrastructure services.
- Executive meetings are conducted regularly to discuss operations, risk posture, and planned initiatives across business units.

Organizational Structure and Assignment of Authority and Responsibility

iM Critical's organizational structure is designed to support the delivery of secure, high-availability infrastructure services. Responsibilities are clearly assigned and communicated, especially within the facilities, engineering, compliance, and MSP coordination functions.

Control activities include:

- A current organizational chart defines roles and lines of reporting and is made available to staff.
- Authority and responsibilities are communicated as part of onboarding and through team leadership.

Human Resources Policies and Practices

iM Critical emphasizes ethical conduct and professional growth. Human resources (HR) policies are designed to recruit, evaluate, retain, and appropriately offboard personnel in a secure and consistent manner.

Control activities include:

- New hires complete orientation and acknowledge receipt of key policies and confidentiality agreements on Day 1.
- Formal annual performance evaluations are conducted for each employee.
- A documented termination checklist governs employee offboarding to ensure systems and access are secured appropriately.

Risk Assessment Process

iM Critical maintains a formal risk assessment process designed to identify and manage risks that could impact the delivery of secure and continuous data center operations. The organization's leadership and compliance staff work collaboratively to evaluate environmental, strategic, and compliance risks relevant to the Miami Data Center.

Identified risks include:

- Operational risk: Personnel turnover, infrastructure changes, or environmental disruptions
- Strategic risk: Evolving client technology requirements and emerging threats
- Compliance risk: Shifts in data protection regulations or industry certifications

A centralized Risk Register is used to track, assess, and monitor identified risks. Mitigation strategies are documented and reviewed on a recurring basis. This process is expected to further mature as iM Critical completes the onboarding of its MSP partner, which will contribute to both operational risk oversight and incident response capabilities.

Integration with Risk Assessment

Risks related to the system's ability to meet service commitments and system requirements are identified based on the unique characteristics of the Miami Data Center, including physical and environmental controls, third-party dependencies, and operational limitations.

iM Critical's management team maps each identified risk to applicable SOC 2 Trust Services Criteria and implements control activities designed to provide reasonable assurance that these criteria are met. Risk-based design decisions are reviewed periodically as infrastructure, customer demands, and regulatory environments evolve.

Information and Communications Systems

iM Critical emphasizes consistent, transparent communication across teams and systems. Internal communication occurs through a combination of policy distribution, meetings, and informal escalation channels. System and infrastructure monitoring tools are used to capture relevant data on environmental performance and physical access.

Control activities include:

- Operational and engineering meetings are held weekly to address issues, review metrics, and coordinate tasks.
- Biannual town hall meetings are held across geographic locations to communicate strategic initiatives and reinforce company values.
- Updates to policies and procedures are communicated via email and acknowledged through management workflows.
- Monitoring platforms and system logs support internal decision-making and infrastructure adjustments.

Monitoring Controls

Management performs continuous monitoring activities to assess the design and operating effectiveness of controls across the Miami Data Center environment. This includes oversight of on-site systems, as well as processes that will be assumed by the MSP within 30 to 60 days.

Control activities include:

- Quality assurance monitoring is conducted regularly across infrastructure and operational systems.
- Monitoring findings are used to guide corrective actions through department meetings or direct follow-up.
- A Risk Register is maintained to document findings, remediation efforts, and corrective action plans.
- Escalation procedures are in place for risks rated as high-impact, and risk-related topics are reviewed annually by senior leadership.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the last 12 months.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the last 12 months.

Criteria Not Applicable to the System

All Common Criteria/Security and Availability criteria were applicable to the iM Critical Data Center Services System.

Subservice Organizations

No subservice organizations were included in the scope of this assessment.

COMPLEMENTARY USER ENTITY CONTROLS

The effectiveness of certain controls at iM Critical depends on user entities (i.e., colocation customers) implementing their own controls. These Complementary User Entity Controls (CUECs) are necessary to achieve the Trust Services Criteria for systems hosted in the Miami Data Center.

Customers of iM Critical retain full responsibility for the security, integrity, and availability of their own systems, including physical assets hosted in their leased spaces, logical access to operating systems and applications, and data stored or processed on those systems.

User entities are responsible for implementing the following controls to complement the controls provided by iM Critical:

1. **Physical Security of Customer-Owned Equipment:**
    - Customers ensure their racks and equipment are physically secured within their assigned cages or cabinets using locks or other protective enclosures.
    - Customers should control access to their assigned spaces by limiting and approving personnel who are authorized to work within the data center.
2. **Logical Access Controls:**
    - Customers are responsible for managing user accounts, passwords, MFA, and remote access to their own systems and applications.
    - Customers should review user access regularly and follow secure provisioning and deprovisioning procedures.
3. **System Hardening and Patch Management:**
    - Customers configure, secure, and maintain the operating systems, middleware, and applications running on their hosted equipment.
    - Regular patching and updates of software under the customer's control are the responsibility of the customer.
4. **Data Protection and Encryption:**
    - Customers ensure the confidentiality and integrity of their data through the use of encryption, both at rest and in transit, when applicable.
    - Data classification and retention policies are defined and enforced by the customer.
5. **Monitoring and Logging:**
    - Customers should enable logging and system monitoring on their own devices and infrastructure to detect suspicious or unauthorized activity.
    - Customers are responsible for reviewing and responding to events generated from their systems.
6. **Backup and Recovery:**
    - Unless contracted separately, customers are responsible for backing up their own systems and data and verifying that recovery procedures meet business needs.
    - Customers should test backup integrity and document recovery procedures.
7. **Compliance with Legal and Regulatory Requirements:**
    - Customers are responsible for identifying and complying with any legal, regulatory, or contractual obligations that apply to the data or systems they host in the Miami Data Center.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (applies to Security and Availability)
The Common Criteria apply across all Trust Services Categories included in this assessment. These criteria include foundational control principles such as logical access, change management, risk assessment, system operations, and incident response. iM Critical has implemented controls aligned with these principles to protect the Miami Data Center's infrastructure and ensure service reliability.

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Core values are communicated from executive management to personnel through policies, procedures, the code of conduct and the employee handbook. An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures. Upon hire, personnel are required to acknowledge the employee handbook and code of conduct. Prior to employment, personnel are required to complete a background check. Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis. Performance and conduct evaluations are performed for personnel on an annual basis. Sanction policies, which include probation, suspension and termination, are in place for employee misconduct. An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner. Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner. Upon hire, personnel are required to sign a confidentiality agreement.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Performance and conduct evaluations are performed for personnel on an annual basis. Executive management roles and responsibilities are documented and reviewed annually. Executive management defines and documents the skills and expertise needed among its members. Executive management evaluates the skills and expertise of its members annually. Executive management maintains independence from those that operate the key controls implemented within the environment. Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Executive management evaluates the skills and competencies of those that operate the internal controls implemented within the environment annually.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.
		Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Executive management maintains independence from those that operate the key controls implemented within the environment.
		A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.
		Executive management reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.
		Executive management reviews job descriptions annually and makes updates, if necessary.
		Executive management has established proper segregations of duties for key job functions and roles within the organization.
		Roles and responsibilities defined in written job descriptions consider and address specific requirements relevant to the system.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Prior to employment, personnel are required to complete a background check.
		Performance and conduct evaluations are performed for personnel on an annual basis.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel. The entity evaluates the competencies and experience of candidates prior to hiring. The entity evaluates the competencies and experience of third-parties prior to working with them. Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process. The entity has a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives. Employees are required to attend continued training annually that relates to their job role and responsibilities. Executive management has created a training program for its employees. As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations and performs disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities. Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Upon hire, personnel are required to acknowledge the employee handbook and code of conduct. Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis. Performance and conduct evaluations are performed for personnel on an annual basis. Sanction policies, which include probation, suspension and termination, are in place for employee misconduct. A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet. Executive management reviews job descriptions annually and makes updates, if necessary. Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel. As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations and performs disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities. Executive management has established performance measures, including the incentives and rewards for exceeding expectations, as it relates to job roles and responsibilities. Executive management reviews the job requirements and responsibilities documented within job descriptions annually and makes updates, if necessary.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented and made available to personnel through the entity's intranet. Data flow diagrams, process flowcharts, narratives and procedures manuals are documented and maintained by management to identify the relevant internal and external information sources of the system. Data entered into the system, processed by the system and output from the system is protected from unauthorized access. Data entered into the system is reviewed for completeness and accuracy.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Core values are communicated from executive management to personnel through policies, procedures, the code of conduct and the employee handbook. Upon hire, personnel are required to acknowledge the employee handbook and code of conduct. Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis. An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner. Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet. Employees are required to attend continued training annually that relates to their job role and responsibilities. Organizational and information security policies and procedures are documented and made available to personnel through the entity's intranet. The entity's policies and procedures, code of conduct and employee handbook are made available to personnel through the entity's intranet. Upon hire, personnel are required to complete information security awareness training. Current employees are required to complete information security awareness training annually. Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Changes to job roles and responsibilities are communicated to personnel through the entity's intranet. Documented escalation procedures for reporting system failures, incidents, concerns, and other complaints are in place and made available to personnel through the entity's intranet. The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's intranet. The information security policies and procedures that communicate the system commitments and requirements of external users are provided to external users prior to allowing them access to the system. Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities. Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner. Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner. Documented escalation procedures for reporting system failures, incidents, concerns, and other complaints are in place and made available to personnel through the entity's intranet. The entity's third-party agreement delineates the boundaries of the system and describes relevant system components. The entity's third-party agreement communicates the system commitments and requirements of third-parties. The entity's third-party agreement outlines and communicates the terms, conditions and responsibilities of third-parties. The entity's contractor agreement outlines and communicates the terms, conditions and responsibilities of external users. Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Changes to commitments, requirements and responsibilities are communicated to third-parties, external users, and customers via mass notifications. Executive management meets annually with operational management to discuss the results of assessments performed by third-parties. Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment. A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority. Organizational and information security policies and procedures are documented and made available to personnel through the entity's intranet. The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics. Executive management has documented objectives that are specific, measurable, attainable, relevant and time-bound (SMART). Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved. Executive management reviews policies, procedures and other control documents for alignment to the entity's objectives on an annual basis. Executive management reviews and addresses repeated control failures. Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure. Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities. The entity has defined the desired level of performance and operation in order to achieve the established entity objectives. Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies. Business plans and budgets align with the entity's strategies and objectives. Entity strategies, objectives and budgets are assessed on an annual basis. The entity's internal controls environment takes into consideration affecting laws, regulations, standards, and legislatures.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Applicable law, regulation, standard and legislature requirements are identified and integrated into the entity's strategies and objectives. Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process. A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties. Documented policies and procedures are in place to guide personnel when performing a risk assessment. Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. The entity's risk assessment process includes: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks for each identified vulnerability Identified risks are rated using a risk evaluation process and ratings are approved by management.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process. For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities. The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management. As part of the annual risk assessment, management reviews the potential threats and vulnerabilities arising from its customers, vendors and third-parties. Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations. Identified fraud risks are reviewed and addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk As part of management's assessment of fraud risks, management considers key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	As part of management's assessment of fraud risks, management considers how personnel could engage in or justify fraudulent activities. As part of management's assessment of fraud risks, management considers threats and vulnerabilities that arise from the use of IT. Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment. A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties. Changes to the regulatory, economic and physical environment in which the entity operates are considered and evaluated as part of the annual comprehensive risk assessment. Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment. Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment. Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment. Changes in vendor and third-party relationships are considered and evaluated as part of the annual comprehensive risk assessment. Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Monitoring Activities		
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Performance and conduct evaluations are performed for personnel on an annual basis. Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment. A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties. Organizational and information security policies and procedures are documented and made available to personnel through the entity's intranet. Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis. On an annual basis, management reviews the controls implemented within the environment for compliance and operational effectiveness and identifies potential control gaps and weaknesses. A data backup restoration test is performed on quarterly basis. Vulnerability scans are performed annually and remedial actions are taken where necessary. A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment, and identified vulnerabilities are addressed and tracked to resolution. Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment. The monitoring software is configured to alert IT personnel when thresholds have been exceeded.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Monitoring Activities		
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment. Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities. Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process. The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management. Senior management assesses the results of the compliance, control and risk assessments performed on the environment. Senior management is made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed. Vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment are communicated to those parties responsible for taking corrective actions. Vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment are documented, investigated, and addressed. Vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment are addressed by those parties responsible for taking corrective actions. Management tracks whether vulnerabilities, deviations and control failures/gaps identified as part of the evaluations performed are addressed in a timely manner.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Executive management maintains independence from those that operate the key controls implemented within the environment. Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment. Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities. Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process. As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations and control gaps. Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed. Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities. Prior to the development and implementation of internal controls into the environment, management considers the complexity, nature, and scope of its operations. Management has documented the relevant controls in place for each key business or operational process. Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls. Business continuity and disaster recovery plans are developed and updated on an annual basis. Business continuity and disaster recovery plans are tested on an annual basis. An analysis of incompatible operational duties is performed on at least an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over	Organizational and information security policies and procedures are documented and made available to personnel through the entity's intranet.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**
	technology to support the achievement of objectives.	Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls. Management has documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes. Management has documented the controls implemented around the entity's technology infrastructure. Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing. As part of the risk assessment process, the use of technology in business processes is evaluated by management. The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Authentication of access • Protecting the entity's assets from external threats Management has established controls around the acquisition, development and maintenance of the entity's technology infrastructure.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet. Organizational and information security policies and procedures are documented and made available to personnel through the entity's intranet. Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities. Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls. The organizational and information security policies and procedures detail the day-to-day activities to be performed by personnel. Management has implemented controls that are built into the organizational and information security policies and procedures. Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment. Process owners and management operate the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures. Process owners and management investigate and troubleshoot control failures. The effectiveness of the internal controls implemented within the environment is evaluated annually.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	An inventory of system assets and components is maintained to classify and manage the information assets. Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Privileged access to sensitive resources is restricted to authorized personnel. Network user access is restricted via role-based security privileges defined within the access control system. Network administrative access is restricted to authorized personnel. Network users are authenticated via individually-assigned user accounts and passwords. The network is configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Network audit logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events Network audit logs are maintained for review when needed. Production server user access is restricted via role-based security privileges defined within the access control system. Production server administrative access is restricted to authorized personnel.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Production server users are authenticated via individually-assigned user accounts and passwords. Production servers are configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity Production server account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Production server audit logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events Production server audit logs are maintained for review when needed. VPN user access is restricted via role-based security privileges defined within the access control system. The ability to administer VPN access is restricted to authorized personnel. Users are authenticated via username and password prior to being granted remote access to the environment. The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel. Data coming into the environment is secured and monitored through the use of firewalls and an IPS. Server certificate-based authentication is used as part of the Secure Sockets Layer (SSL) / TLS encryption with a trusted certificate authority. Passwords and production data is stored in an encrypted format using software supporting the Advanced Encryption Standard (AES).

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Encryption keys are protected during generation, storage, use, and destruction. Logical access to systems is approved and granted to personnel as a component of the hiring process. Logical and physical access to systems is revoked from personnel as a component of the termination process. Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Privileged access to sensitive resources is restricted to authorized personnel. Logical access to systems is approved and granted to personnel as a component of the hiring process. Logical and physical access to systems is revoked from personnel as a component of the termination process. Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	An analysis of incompatible operational duties is performed on at least an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place. Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Privileged access to sensitive resources is restricted to authorized personnel. Network user access is restricted via role-based security privileges defined within the access control system. Production server user access is restricted via role-based security privileges defined within the access control system. Logical access to systems is approved and granted to personnel as a component of the hiring process. Logical and physical access to systems is revoked from personnel as a component of the termination process. Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Logical and physical access to systems is revoked from personnel as a component of the termination process. A video surveillance system is in place with footage retained for 161 days. Visitors to the office facility and server room / data center are required to sign a visitor log prior upon arrival.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	This criterion is the responsibility of the user entities. Refer to the "Complementary User Entity Controls" section above for controls managed by the user entities.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	VPN user access is restricted via role-based security privileges defined within the access control system. Users are authenticated via username and password prior to being granted remote access to the environment. Server certificate-based authentication is used as part of the SSL / TLS encryption with a trusted certificate authority. Passwords and production data is stored in an encrypted format using software supporting the AES. NAT functionality is utilized to manage internal IP addresses. VPN, SSL/TLS and other encryption technologies are used for defined points of connectivity. Transmission of digital output beyond the boundary of the system is encrypted. Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session. A firewall is in place to filter unauthorized inbound network traffic from the Internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. An IPS is utilized to analyze network events and report possible or actual network security breaches. The IPS is configured to notify personnel upon intrusion prevention.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations and servers on a daily basis. Use of removable media is prohibited by policy and system configuration except when authorized by management. Users are authenticated via username and password prior to being granted remote access to the environment. Server certificate-based authentication is used as part of the SSL / TLS encryption with a trusted certificate authority. Passwords and production data is stored in an encrypted format using software supporting the AES. NAT functionality is utilized to manage internal IP addresses. VPN, SSL/TLS and other encryption technologies are used for defined points of connectivity. Transmission of digital output beyond the boundary of the system is encrypted. Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session. A firewall is in place to filter unauthorized inbound network traffic from the Internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. An IPS is utilized to analyze network events and report possible or actual network security breaches. The IPS is configured to notify personnel upon intrusion prevention. Use of removable media is prohibited by policy and system configuration except when authorized by management. Backup media is stored in an encrypted format. Mobile devices are protected through the use of secured, encrypted connections.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Production data is backed up and replicated to an offsite facility as-needed. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations and servers on a daily basis. The ability to install applications and software on workstations is restricted to authorized personnel. The ability to implement new Access Control Lists (ACLs) is restricted to authorized and appropriate users. Documented change control policies and procedures are in place to guide personnel in the change management process. The monitoring software is configured to alert IT personnel when thresholds have been exceeded.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. Vulnerability scans are performed annually and remedial actions are taken where necessary. A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment, and identified vulnerabilities are addressed and tracked to resolution. A firewall is in place to filter unauthorized inbound network traffic from the Internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. An IPS is utilized to analyze network events and report possible or actual network security breaches. The IPS is configured to notify personnel upon intrusion prevention. Use of removable media is prohibited by policy and system configuration except when authorized by management. Management defined configuration standards in the information security policies and procedures. The monitoring software is configured to alert IT personnel when thresholds have been exceeded. Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Network audit logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events Network audit logs are maintained for review when needed. Production server account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Production server audit logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events Production server audit logs are maintained for review when needed. A video surveillance system is in place with footage retained for 161 days. Visitors to the office facility and server room / data center are required to sign a visitor log prior upon arrival. A firewall is in place to filter unauthorized inbound network traffic from the Internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. An IPS is utilized to analyze network events and report possible or actual network security breaches. The IPS is configured to notify personnel upon intrusion prevention.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations and servers on a daily basis. Use of removable media is prohibited by policy and system configuration except when authorized by management. The monitoring software is configured to alert IT personnel when thresholds have been exceeded. Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. The incident response and escalation procedures are reviewed at least annually for effectiveness. The incident response policies and procedures define the classification of incidents based on its severity. Resolution of incidents is documented within the ticket and communicated to affected users. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Identified incidents are reviewed, monitored and investigated by an incident response team. Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users. Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes. The incident response and escalation procedures are reviewed at least annually for effectiveness. The incident response policies and procedures define the classification of incidents based on its severity. Resolution of incidents is documented within the ticket and communicated to affected users. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented. The actions taken to address identified security incidents are documented and communicated to affected parties. Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents. Critical security incidents that result in a service operation disruption are communicated to those affected through creation of an incident ticket. Remediation actions taken for security incidents are documented within the ticket and communicated to affected users.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The risks associated with identified vulnerabilities are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk A data backup restoration test is performed on quarterly basis. Business continuity and disaster recovery plans are developed and updated on an annual basis. Business continuity and disaster recovery plans are tested on an annual basis. Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes. A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. Change management requests are opened for incidents that require permanent fixes. The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations A business continuity and disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. The business continuity and disaster recovery plan and procedures are updated based on disaster recovery plan test results.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Change Management		
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The ability to implement new ACLs is restricted to authorized and appropriate users. Documented change control policies and procedures are in place to guide personnel in the change management process. The change management process has defined the following roles and assignments: • Authorization of change requests - Owner or business unit manager • Development - Application Design and Support Department • Testing - Quality Assurance Department • Implementation - Software Change Management Group System changes are communicated to both affected internal and external users. System patches updates follow the standard change management process. System patches updates are performed on a configured schedule. Information security policies and procedures document the baseline requirements for configuration of IT systems and tools. Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Mitigation		
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. Identified risks are rated using a risk evaluation process and ratings are approved by management. Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process. Documented policies and procedures are in place to guide personnel in performing risk assessment and risk mitigation activities. The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability. Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties. Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. Identified risks are rated using a risk evaluation process and ratings are approved by management.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Mitigation		
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment. The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability. Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances. Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process. Identified third-party risks are rated using a risk evaluation process and ratings are approved by management. The entity's third-party agreement outlines and communicates: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements. Management has assigned responsibility and accountability for the management of risks associated with third-parties to appropriate personnel. Management has established exception handling procedures for services provided by third-parties. The entity has documented procedures for addressing issues identified with third-parties. The entity has documented procedures for terminating third-party relationships.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY		
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. The monitoring software is configured to alert IT personnel when thresholds have been exceeded. Processing capacity is monitored 24x7x365. Future processing demand is forecasted and compared to scheduled capacity on an annual basis. Future processing demand forecasts are reviewed and approved by management on an annual basis. The change management process is followed when a change is made to a system as a result of capacity constraint.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Environmental threats that could impair the availability of the system are considered and identified as a part of the risk assessment process. Risks relating to environmental threats identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk A centralized environmental monitoring system is in place to monitor facilities housing production systems and send automated alerts to personnel if pre-defined thresholds are exceeded. Temperature and humidity sensor systems are in place in the facility that notifies operations support personnel via email of readings outside of the defined parameters. The pre-action dry pipe fire suppression systems are tested and inspected by a third-party on an annual basis. The UPS units are tested and inspected by a third-party on a semi-annual basis. The generators are tested on a semi-annual basis. Preventive maintenance inspections and service is performed on the generators by a third-party on a semi-annual basis. The HVAC units are inspected and maintained by a third-party on a monthly basis. Alerts generated from the centralized environmental monitoring system are sent to operations support personnel that are responsible for investigating and resolving the alerts.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY		
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Alerts generated from the temperature and humidity sensor systems are sent to operations support personnel that are responsible for investigating and resolving the alerts. Environmental protection policies and procedures are documented and maintained. The environmental protection policies and procedures practices are reviewed annually. Full backups of certain application and database components are performed on a monthly basis and incremental backups are performed on a daily basis. When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure. Production data is backed up and replicated to an offsite facility as-needed. Redundant architecture is in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable. The disaster recovery plan includes moving the business operations and supporting systems to a different site. A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations. The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A data backup restoration test is performed on quarterly basis. Business continuity and disaster recovery plans are developed and updated on an annual basis. Business continuity and disaster recovery plans are tested on an annual basis. A business continuity and disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY		
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**
		A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations. The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE's examination of the controls of iM Critical was limited to the Trust Services Criteria, related criteria and control activities specified by the management of iM Critical and did not encompass all aspects of iM Critical's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization
- Determine whether the criteria are relevant to the user entity's assertions
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria