HOGAN ASSESSMENT SYSTEMS

SOC 2® TYPE 2 REPORT ON THE SECURITY AND AVAILABILITY TRUST SERVICES PRINCIPLES

January 1, 2017 to December 31, 2017

Hogan Assessment Link Online
Personality Assessment System

CONTENTS

SECTION I – INDEPENDENT SERVICE AUDITORS' REPORT

Hogan Assessment Systems
Tulsa, Oklahoma

Scope

We have examined Hogan Assessment Systems' (Hogan or Service Organization) attached description of its Hogan Assessment Link Online Personality Assessment System (system) throughout the period January 1, 2017 to December 31, 2017, (description) based on the criteria set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria) and the suitability of the design and operating effectiveness of controls included in the description throughout the period January 1, 2017 to December 31, 2017, to meet the criteria for the security and availability principles set forth in Trust Services Principles (TSP) section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*) (applicable trust services criteria), throughout the period January 1, 2017 to December 31, 2017.

The Service Organization uses a data center subservice organization for hosting of its production systems and a software development subservice organization for application development services. The description includes only the controls of the Service Organization and excludes controls of the subservice organizations. The description also indicates that certain applicable trust services criteria can be achieved only if complementary subservice organization controls assumed in the design of the Service Organization's controls are suitably designed and operating effectively, along with the related controls at the Service Organization. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service organization's responsibilities

The Service Organization has provided its assertion about the fairness of the presentation of the description based on the description criteria and suitability of design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. The Service Organization is responsible for preparing the description and assertion; including the completeness, accuracy, and method of presentation of the description and the assertion; providing the services covered by the description; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting the controls to meet the applicable trust services criteria; and specifying the controls that meet the applicable trust services criteria and stating them in the description.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, 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 fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period January 1, 2017 to December 31, 2017. 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 the Service Organization's system and the suitability of the design and operating effectiveness of the controls involves:

- performing procedures to obtain evidence about whether the description is fairly presented based on the description criteria and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period January 1, 2017 to December 31, 2017,
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively,
- testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met, and
- evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization in its assertion.

Inherent limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls is subject to the risks that the system may change or that controls at a service organization may become ineffective or fail.

Description of tests of controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section III of this report.

Opinion

In our opinion, in all material respects, based on the description and the applicable trust services criteria:

a. The description fairly presents the system that was designed and implemented throughout the period January 1, 2017 to December 31, 2017.
b. The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period January 1, 2017 to December 31, 2017, and the subservice organizations applied the types of controls expected to be implemented at the subservice organizations throughout the period January 1, 2017 to December 31, 2017.

c. The controls tested operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period January 1, 2017 to December 31, 2017, if the controls expected to be implemented at the subservice organizations were also operating effectively throughout the period January 1, 2017 to December 31, 2017.

Intended users and purpose

This report, including the description of tests of controls and results thereof in Section III, is intended solely for the information and use of the Service Organization, user entities of the Service Organization's system during the period January 1, 2017 to December 31, 2017, and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- the nature of the service provided by Hogan,
- how the Service Organization's system interacts with user entities, subservice organizations, or other parties,
- internal control and its limitations,
- the applicable trust services criteria, and
- the risks that may threaten the achievement of the applicable trust services criteria 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.

Tulsa, Oklahoma
February 26, 2018

Section II – Management's Assertion and Hogan's Description of the System

Management's Assertion

HOGAN
11 S Greenwood | Tulsa OK 74120
hoganassessments.com

We have prepared the attached description of Hogan Assessment Systems' (Hogan or Service Organization) Hogan Assessment Link Online Personality Assessment System (system) throughout the period January 1, 2017 to December 31, 2017 (description), based on the criteria in items (a)(i)—(ii) below, which are the criteria for a description of a service organization's system in paragraphs 1.26—.27 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria). The description is intended to provide users with information about the Service Organization's system, particularly system controls intended to meet the criteria for the security and availability principles set forth in Trust Services Principles (TSP) section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*) (applicable trust services criteria).

The Service Organization uses a data center subservice organization for hosting of its production systems and a software development subservice organization for application development services. The description includes only the controls and related control objectives of the Service Organization and excludes the control objectives and related controls of these subservice organizations. The description also indicates that the applicable trust services criteria can be achieved only if complementary subservice organization controls assumed in the design of the Service Organization's controls are suitably designed and operating effectively, along with the related controls at the Service Organization.

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

a. the description fairly presents the system throughout the period January 1, 2017 to December 31, 2017, based on the following description criteria:

i. The description contains the following information:

(1) The types of services provided,

(2) The components of the system used to provide the services, which are as follows:

a) Infrastructure. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks),

(b) Software. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities),

(c) People. The personnel involved in the governance, operation, and use of the system (developers, operators, entity users, vendor personnel, and managers),

(d) Procedures. The automated and manual procedures, and

(e) Data. Transaction streams, files, databases, tables, and output used or processed by the system.

(3) The boundaries or aspects of the system covered by the description,

(4) For information provided to, or received from, subservice organizations or other parties:

(a) how such information is provided or received and the role of the subservice organization and other parties, and

(b) the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

(6) For the subservice organization utilized:

(a) the nature of the services provided by the subservice organization, and

(b) each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at the carved-out subservice organization to meet those criteria.

(7) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons, and

(8) Relevant details of changes to the service organization's system during the period covered by the description.

ii. The description does not omit or distort information relevant to the Service Organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. the controls stated in the description were suitably designed throughout the period January 1, 2017 to December 31, 2017, to meet the applicable trust services criteria.

c. the controls stated in the description operated effectively throughout the period January 1, 2017 to December 31, 2017, to meet the applicable trust services criteria.

Sincerely,

Chris Kingham
Chief Operating Officer

Overview of Operations

Business Description

For 30+ years, Hogan Assessment Systems (Hogan) has been the industry leader in personality assessment. Founded in research and propelled by a strict adherence to empirical and scientific evidence, Hogan's solutions bring greater objectivity, science, and insight to talent management initiatives. Hogan's reputation for excellence is supported by technical and professional expertise, diverse experience and practical perspective, and creative solutions to organizational issues.

Hogan continues to meet its vision of developing and distributing state-of-the-art personality assessment tools and leadership development programs to enhance the effectiveness of both individuals and organizations. Hogan consultants use a combination of science and practical experience to help organizations manage a wide range of human resource issues, and Hogan supports its assessment and development programs via ongoing research and continuous improvement.

Hogan provides organizations with valid and reliable assessment tools and professional consulting expertise. Hogan's personality, values, and cognitive-based assessment tools are the results of over 54 cumulative years of research and refinement. Over half of the Fortune 500 companies use Hogan's assessments for employee selection and/or development purposes.

Currently, over 3,000 test publishers exist within the United States alone. Hogan is proud to distinguish itself within the growing assessment industry along the following dimensions: Predictive, Effective, Defensible, and Validated.

Products and Services

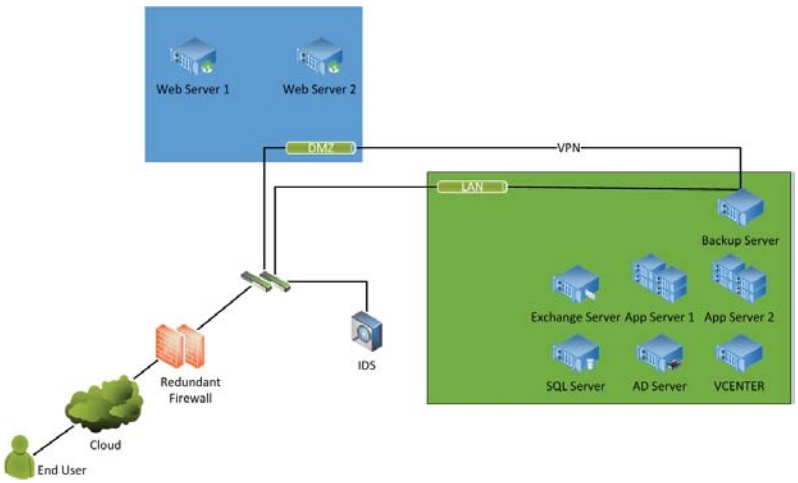
The world's most powerful companies depend on Hogan, and for good reason: Hogan provides hard-hitting solutions to problems that every business, big or small, must overcome to be successful. Hogan helps its clients decide which candidate is best suited for the job, and how to build strong, effective teams. Hogan helps clients develop high potential managers into executive-level leadership and how to maximize productivity across the organization.

Hogan's core products consist of personality assessments paired with specific reports tailored to the unique needs of your business, along with personal support from our team of consultants. Hogan does not just administer tests. Hogan works with clients to identify needs and design long-term solutions.

Components of Systems Providing Services
Hogan maintains an information security program that is consistent with industry standards, which includes appropriate administrative, physical and technical safeguards to a) maintain the security and availability of data; b) protect against anticipated threats or hazards to the security and availability of data; and c) protect against security incidents.

Infrastructure

Systems: Hogan production systems are deployed in a Tier III data center (located in Tulsa, Oklahoma) and utilize clustered web servers and clustered database servers in the production environment. The Hogan network has been designed and built with two firewalls in place, a primary firewall and a failover firewall. The network has been fully tested and no connectivity is lost during failover. Hogan utilizes development, testing, and production environments.



Data Center: Hogan utilizes a colocation data center in Tulsa, Oklahoma, to house production and testing systems. The data center provider, TierPoint, utilizes the carrier-class levels of security, redundancy and connectivity. TierPoint provides 99.9999% up-time and has an external examination of its controls performed annually. Hogan owns and manages the servers and storage.

Disaster Recovery: Hogan has a fully documented disaster recovery plan, which is tested annually. Backups are stored locally, and in a separate data center 100 miles away. Configured as a warm site, business continuity would be maintained by activating the standby platform in the event of a disaster.

Availability: Hogan maintains a standard service level of 99.8% website availability, as calculated on a monthly basis, excluding scheduled maintenance.

Backups: Hourly incremental and daily full backups are completed on production servers. Backups are stored remotely at a Tier III data center.

Change Management: Hogan follows a structured change management process to minimize service interruptions and client impact. Requested changes are reviewed and categorized as either service impacting or an enhancement. Enhancements are placed in the development queue and scheduled to be included in one of the standard Thursday evening maintenance windows.

Online Platforms

Hogan's assessments and reports are accessed from, and processed by, two primary platforms: Hogan Assessment Link Online (HALO) and the Participant Portal:

HALO: This is the primary Hogan and client administrative portal. For Hogan clients, HALO provides the ability to select assessments, report options, as well as create, manage, and track participants. Hogan personnel use HALO to create, administer, and support client accounts, as well as manage data and other systems information.

Participant Portal: This is the online platform participants use to take the Hogan Assessments. Participants are generally client job candidates or current employees, depending on the Hogan reports being purchased.

Client Support

Hogan maintains appropriate processes to provide service support and issue resolution from 8:00am to 5:00pm, Central US Time, Monday through Friday. Hogan can be reached at 877-670-0637 or support@hoganassessments.com.

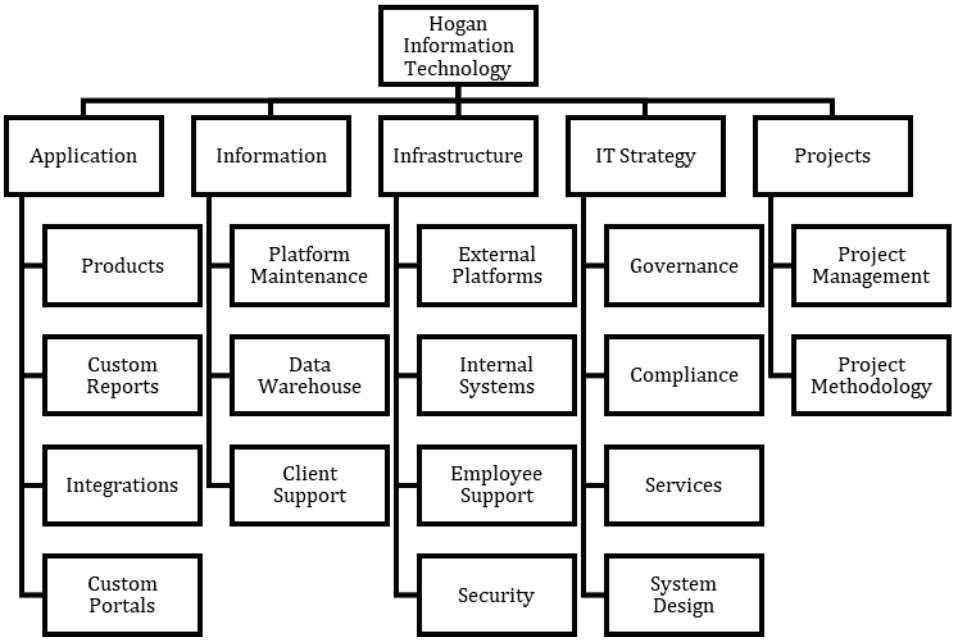
System and Application Development Life Cycle

Hogan has developed an Integrated System Methodology (ISM) approach for system and application development. The ISM is meant to provide a uniform approach to managing information systems while providing sufficient flexibility to choose the techniques and tools best suited for a specific task. It is to be used as a guideline to those involved in information system planning, systems analysis, security, design and development, acquisition, implementation, maintenance, and conversion. Each model defines the deliverables that are to be produced during the process as well as the tasks to be performed and who is to perform them. It also defines what should be created and what tasks are likely to be executed to create the deliverable. This has been developed by taking the best concepts from several System Development Life Cycle (SDLC) process frameworks, including Waterfall, Agile, and SCRUM among others.

Standard SDLC phases may include requirements gathering, analysis, design, development, testing, deployment, and maintenance. Depending on the specific need or change, some of these phases may be combined, repeated, eliminated, or otherwise modified. The Hogan SDLC is not meant to be all-inclusive or rigid in terms of content, but rather a guideline to use based on the requirements, complexity, urgency and flexibility of an individual project.

People

Hogan Information Technology (IT) personnel are organized into functional teams representing application support, application development, project management, client support, infrastructure management, security and compliance, and governance. A functional organization chart is on the following page.



Data

Maintaining the security and availability of client data is one of Hogan's highest responsibilities. To fulfill this responsibility, Hogan has several policies which cover the collection, processing, storage, and access of data from both clients and participants.

Before Hogan will receive data from a client, a legal agreement must be in place. This could be in the form of a Master Services Agreement, Statement of Work, Standard Contractual Clauses, or other legal agreement. These agreements establish the baseline for the transfer of data in a safe and secure manner. Additionally, users of HALO must agree to an online Terms of Services, while Participants must agree to an assessment-focused Informed Consent.

Encryption of data is an essential means of ensuring information is not intercepted as it is transferred from source to destination. Hogan has established an encryption policy to provide guidelines on the standards and methods to be used for transmission and storage of data.

Additionally, Hogan has implemented information labeling and handling guidelines in a data classification policy. Sensitivity level definitions were created as guidelines and to emphasize common sense steps that one can take to protect Hogan Confidential information (e.g., Hogan Confidential information should not be left unattended in conference rooms).

Hogan information is categorized into two main classifications:

- Hogan Public – Hogan Public information is information that has been declared public knowledge by the head of the department which created the document or a member of executive management and can freely be given to anyone without damage to Hogan Systems.
- Hogan Confidential – Hogan Confidential contains information not specifically designated as Public. It is understood that some information is more sensitive than other information and should be protected in a more secure manner. Therefore, Hogan Confidential information must be further classified by sensitivity as:
  - ✓ Internal Use Only,
  - ✓ Proprietary,

- ✓ Highly Confidential, or
- ✓ Third-Party Confidential.

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring

Control Environment

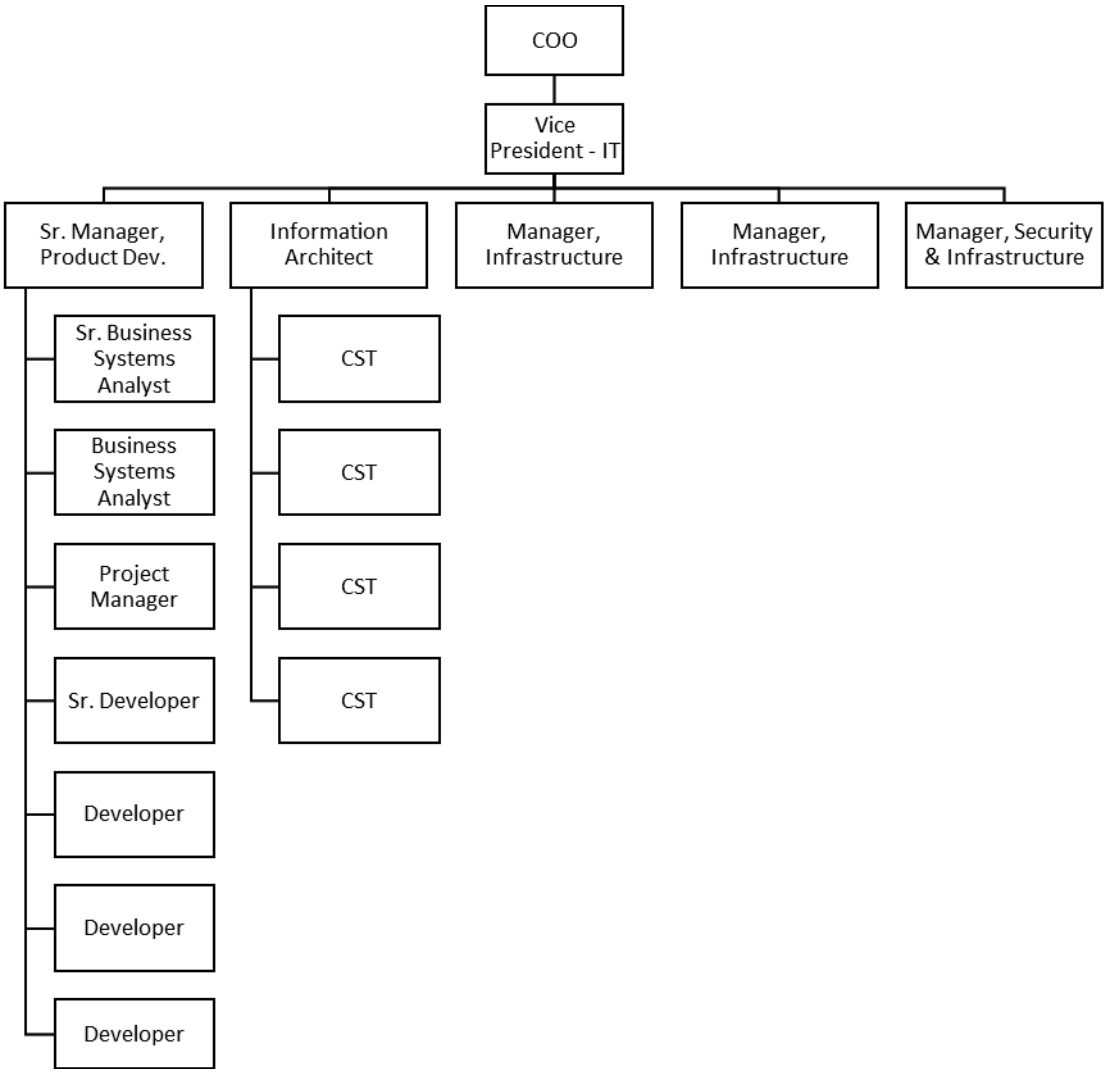
The control environment sets the tone of the organization, influencing the control consciousness of its people. It is the foundation for the other components of internal control, providing discipline and structure. The control environment has a pervasive influence on the structure of business activities, establishment of objectives, and assessment of risks. It influences control activities, information and communication systems, and monitoring procedures. The control environment is influenced by an entity's history and managerial culture. Effectively controlled entities strive to have competent personnel, instill an enterprise-wide attitude of integrity and control consciousness, and set a positive corporate direction. These entities establish appropriate controls that foster shared values and teamwork in pursuit of the organization's objectives.

Integrity and Ethical Values

Hogan maintains a safe and cooperative working environment and expects employees to have high standards of performance, integrity, productivity, and professionalism. Hogan employs an IT Code of Conduct which IT employees must agree to on an annual basis. While managers are responsible for understanding, communicating, and enforcing Hogan policies, this does not override or diminish an employee's individual responsibility to be aware of and adhere to these policies. Management monitors behavior closely and exceptions to these values lead to immediate corrective action as defined by Human Resources (HR) policies and procedures. Employees found to have violated any ethical policy may be subject to disciplinary action, up to and including termination.

Organization Structure

Hogan's IT organization structure provides the framework within which its activities for achieving company-wide objectives are planned, executed, controlled, and monitored. The chart on the following page shows the current structure of the IT organization.



Information Security Program Oversight Committee

The purpose of the Hogan Information Security Program Oversight Committee (ISPOC) is to serve as a governance body to ensure Hogan establishes and maintains an effective information security program. Hogan ISPOC follows best practice standards as defined by organizations such as the International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), and the American Institute of Certified Public Accountants (AICPA).

Hogan ISPOC is responsible for reviewing and recommending policies, standards, guidelines, controls, control procedures, and controls tests which provide the framework for protecting classified information. In addition, the committee is responsible for providing governance to ensure the appropriate artifacts are collected and archived with the objective of providing auditable proof Hogan diligently protects classified data.

Human Resources Practices

Hogan's HR policies and practices relate to hiring, orienting, training, evaluating, counseling, promoting and compensating personnel. Hogan has hiring practices designed to ensure new employees are qualified

for their job responsibilities. Written job descriptions, which thoroughly define the role and associated responsibilities, are maintained by the Director of HR, which are reviewed annually and revised as necessary.

Candidates pass through an interview process to assess their qualifications related to the expected responsibility of the position. Hogan conducts pre-employment reference checks, as well as background investigations relating to past employment history and criminal activity in accordance with the Fair Credit Reporting Act.

The Hogan Employee Handbook (Handbook) is provided to employees upon hire, and again as the document is updated. In addition to common employment information, the Handbook discusses security, acceptable use of systems, confidentiality, ethics, and other relevant topics. New employees are required to sign an acknowledgment that they will abide by Company policies, as well as a separate confidentiality agreement.

Managers and direct reports create performance review plans which align with objectives and accountabilities of the business and department. On a periodic basis, but no less than twice a year, managers and employees discuss the plan to ensure objectives are being met, gaps are identified, and new objectives are set (as applicable).

Business Planning
Each year Hogan undertakes a multi-month exercise to plan for the upcoming year. This initiative includes setting goals, objectives, strategies, and tactics from both an organization-wide and department-level perspective. Activities include reviewing the organization structure, reporting structures, product releases, research and development, system capacity planning, marketing strategies, and more. Employees throughout the Company are included in the business planning process, and the Hogan Board of Directors approves the final plan.

Risk Assessment
Hogan's risk management framework has been designed to assist executive management and stakeholders in identifying risks that have a significant likelihood and that could impact Hogan's efforts to meet strategic goals and objectives. The framework, which provides for continuous review and improvement, has been implemented around business processes and functions of the organization that have been identified with input from stakeholders and subject matter experts. Risk treatment decisions are made with the assistance of the ISPOC.

Information and Communication
Information and communication is an integral component of Hogan's internal control system. Hogan is committed to the communication of relevant information to stakeholders. Hogan communicates its commitments through various methods, including master agreements, terms and conditions, informed consent, and multiple user manuals and training guides. Additionally, proposed system changes which may affect client access or functionality are communicated prior to implementation. Changes made to systems are communicated through ongoing mechanisms such as client care meetings and support cases logged in the client support ticket tracking system.

Incident Response Management
Hogan utilizes a formal incident management policy, which outlines the process and exceptions for investigating and reporting security incidents. Incidents should be immediately reported to the Hogan Support team, or Hogan Consultant assigned to client. Support or the Consultant will notify the Vice President (VP) of IT and the Infrastructure Manager. An analysis of the incident will be performed to

determine scope and impact. Appropriate notifications to senior leadership will be made. As applicable, client notifications will be made within 24 hours.

Policies and Procedures

Hogan has documented policies and procedures to support the operations and controls over its environments. Specific examples include the following:

- Acceptable Encryption Policy,
- Acceptable Use Policy,
- Authentication Policy,
- Business Continuity Plan (BCP),
- Change Management Policy,
- Data Backup Policy,
- Data Classification Policy,
- Disaster Recovery Plan (DRP),
- Equipment Disposal Policy,
- Guest Access Policy,
- Hogan Data Retention and Research Policy,
- Incident Management Policy,
- Information Security Awareness Training Policy,
- IT Code of Conduct,
- Mobile Device Policy,
- Network Device Security Policy,
- Password Policy,
- Patch Management Policy,
- Policy Management and Maintenance Policy,
- Remote Access Policy,
- Risk Management Policy,
- Secure Configuration Management Policy, and
- System Development Life Cycle (SDLC) Policy.

Physical Security

Hogan utilizes a colocation data center in Tulsa, Oklahoma, to house production and testing systems. Entry points at the data center are controlled by card and biometric readers to be sure that only authorized personnel can gain entry. Hardware is secured with state-of-the-art cage and cabinet design. Security alarms are integrated with local emergency response units, so that help can be summoned instantly if needed.

The Hogan corporate office is secured with an access control card system, security cameras, and monitored alarm system. Visitors cannot enter the office without intervention by a Hogan employee, after which point they are escorted to their point of contact.

Logical Security

Logical access to Hogan's systems, applications, and data is limited to properly authorized individuals, and user rights are kept to a minimum based on job responsibility. System administrators, at the direction of management, control network and server passwords. User account authentication to the network is managed via Microsoft Active Directory. System passwords are managed by the Systems Administrators who follow a password policy approved by management.

Monitoring

Hogan utilizes a third-party to perform annual web application penetration testing on core platforms to ensure an adequate security posture. Additionally, quarterly vulnerability scans are performed to identify adversarial entry points and appropriate mitigation strategies.

Hogan's network based intrusion detection system (IDS) analyzes traffic in real-time as it travels across the network. If an attack is detected, based on pattern, frequency, or anomaly then an alert is triggered. Hogan conducts quarterly vulnerability assessments against externally facing internet protocol (IP) addresses, critical internal systems, and engages an in-depth web application vulnerability scan. Additionally, penetration testing is performed annually to insure vulnerabilities are identified and mitigated as appropriate.

Subservice Organizations and Vendor Management

Hogan uses the following subservice organizations:

- TierPoint – a third-party data center providing colocation services related to security, redundancy and connectivity.
- Cityon Systems (Cityon) – third-party developers providing system development services.

Hogan relies on controls at these subservice organizations, in conjunction with controls at Hogan, to achieve the following Trust Services Principle criteria:

- Common Criteria 5.1 – Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.

  Hogan expects controls related to preventing and detecting unauthorized logical access to Hogan's data to have been implemented at each subservice organization.

- Common Criteria 5.5 – Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel.

  Hogan expects controls related to preventing and detecting unauthorized physical access to Hogan's data and equipment to have been implemented at TierPoint.

- Common Criteria 7.4 – Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented in accordance with security and availability commitments and requirements.

  Hogan expects controls related to developing, documenting, and testing of changes to have been implemented at Cityon.

- Availability Criteria 1.2 – Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.

  Hogan expects controls related to maintaining the physical environment and connectivity to systems to have been implemented by TierPoint.

In order to ensure these controls have been implemented and are operating effectively, Hogan has implemented a vendor management policy that requires vendors to be risk rated. On an annual basis, Hogan evaluates high-risk vendors through review of Service Organization Control reports, other independent reports when available, and reports provided by the vendor. Vendor performance is also monitored during the year through daily, weekly, and monthly management activities.

Trust Services Criteria and Related Controls

Although the trust services criteria and related controls are presented in Section III, "Trust Services Security and Availability Principles, Criteria, Related Controls, and Tests of Controls," they are an integral part of Hogan's system description.

Section III – Trust Services Security and Availability Principles, Criteria, Related Controls and Tests of Controls

The relevant control environment elements at Hogan have the collective effect of establishing, enhancing, or mitigating the effectiveness of specific controls. In planning the nature, timing, and extent of our testing of controls, we considered the aspects of Hogan's control environment, risk assessment processes, information and communication, and management monitoring of procedures and performed the procedures we considered necessary.

On the pages that follow, the description of the applicable Trust Services Criteria and the controls to meet the criteria have been specified by, and are the responsibility of Hogan. The Testing Performed by HoganTaylor LLP (HT) and the Results of Tests are the responsibility of the service auditor.