SYSTEM AND ORGANIZATION CONTROLS (SOC) FOR SERVICE ORGANIZATIONS SOC 3®

AUDITWERX
A DIVISION OF
CARR, RIGGS & INGRAM CAPITAL, LLC
AUDITWERX.COM

GENERAL USE REPORT ON

F12.NET, INC.'S

DESCRIPTION OF ITS MANAGED IT SUPPORT SERVICES RELEVANT TO SECURITY, AVAILABILITY, CONFIDENTIALITY, AND PRIVACY

THROUGHOUT THE PERIOD

NOVEMBER 1, 2022 to DECEMBER 31, 2023

TABLE OF CONTENTS

SECTION 1: INDEPENDENT SERVICE AUDITOR’S REPORT

AUDITWERX
A DIVISION OF
CARR, RIGGS & INGRAM CAPITAL, LLC

Auditwerx
3000 Bayport Drive
Suite 500
Tampa, FL 33607

866.446.4038
Auditwerx.com

INDEPENDENT SERVICE AUDITOR'S REPORT

To: F12.net, Inc

Scope

We have examined F12.net, Inc.'s ("F12.net") accompanying assertion titled "F12.net's Assertion" ("assertion") that the controls within F12.net's Managed IT Support Services ("System") were effective throughout the period November 1, 2022 to December 31, 2023, to provide reasonable assurance that F12.net's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy ("applicable trust services criteria") set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria.*

F12.net's Responsibilities

F12.net 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 F12.net's service commitments and system requirements were achieved. F12.net has also provided the accompanying assertion about the effectiveness of controls within the System. When preparing its assertion, F12.net is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for it assertion by performing an assessment of the effectiveness of the controls within the System.

Auditwerx's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the System were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA and in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other Than Audits or Reviews of Historical Financial Information*, set out in the CPA *Canada Handbook – Assurance*. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the System and the service organization’s service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve F12.net’s service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the System were effective to achieve F12.net’s service commitments and system requirements based on the applicable trust services criteria.

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

Service Auditor’s Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal controls, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness 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.

Opinion

In our opinion, management’s assertion that the controls within F12.net’s Managed IT Support Services were effective throughout the period November 1, 2022 to December 31, 2023, to provide reasonable assurance that F12.net’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Auditwerx, LLC

Auditwerx, LLC, a Division of Carr, Riggs & Ingram Capital, LLC
Tampa, Florida

March 12, 2024

SECTION 2: F12.NET, INC.'S ASSERTION

F12.NET, INC.'S ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within F12.net, Inc.'s ("F12.net") Managed IT Support Services ("System") throughout the period November 1, 2022 to December 31, 2023, to provide reasonable assurance that F12.net's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy ("applicable trust services criteria") set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is in Section 3 and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the System throughout the period November 1, 2022 to December 31, 2023, to provide reasonable assurance that F12.net's service commitments and system requirements were achieved based on the trust services criteria. F12.net's objectives for the System in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented within the description of the boundaries of the System in Section 3.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the System were effective throughout the period November 1, 2022 to December 31, 2023, to provide reasonable assurance that F12.net's service commitments and system requirements were achieved based on the applicable trust services criteria.

By: /S/ Calvin Engen

Calvin Engen
Chief Technology Officer

March 12, 2024

SECTION 3: F12.NET, INC.'S DESCRIPTION OF ITS MANAGED IT SUPPORT SERVICES

COMPANY OVERVIEW

F12.net, Inc. (“F12.net” or the “Company”) was started in 1996 and incorporated in Alberta, Canada.

F12.net was built by uniting IT consulting firms across Canada around a shared vision – to combat risk and complexity by continuously crafting business technology platforms that empower business leaders to focus and thrive.

SERVICES OVERVIEW

F12.net provides businesses and not-for-profits with managed IT services for flat monthly fees, from point solutions to full-stack, hardware-inclusive subscription IT.

F12.net’s point solutions include Disaster-Recovery-as-a-Service (“F12 Rescue”), sovereign cloud hosting (“F12 Cloud”), and managed cyber security (“F12 Secure”). Many of F12’s clients are enrolled in comprehensive managed IT programs that bundle together infrastructure management, data backup, helpdesk services, and cybersecurity (“F12 Select”).

F12.net’s premier subscription IT program (“F12 Infinite”) provides infrastructure-as-a-service and takes on the responsibility of uptime, data security, backup and recovery, and hardware asset management. It also includes on-site support and an end-user platform that allows users to connect with support technicians at the click of a key.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

F12.net designs its processes and procedures related to the Managed IT Support Services (“System”) to meet its objectives. Those objectives are based on the service commitments F12.net makes to user entities, the laws and regulations governing the provision of the services, and the financial, operational and compliance requirements that F12.net has established for the services.

Security, availability, confidentiality, and privacy commitments to user entities are documented and communicated in Service Agreements, other customer agreements and in the description of the service offering provided online. Security, availability, confidentiality, and privacy commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the System permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Uptime availability of production systems
- Use of encryption technologies to protect confidential data at rest and in transit
- Protection of personal information regarding the collection, use, retention, disclosure, and disposal of personal information.

F12.net establishes operational requirements that support the achievement of security, availability, confidentiality, and privacy commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in system policies and procedures, system design documentation, and customer agreements. Information security policies define an organization-wide approach to protecting systems and data. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition, policies define how to carry out specific manual and automated processes required in the operation and development of the System.

SCOPE OF THE DESCRIPTION

This description addresses only F12.net's System provided to user entities and excludes other services provided by F12.net. The description is intended solely for the information and use of F12.net, user entities of F12.net's System during some or all of the period November 1, 2022 to December 31, 2023, business partners of F12.net subject to risks arising from interactions with the System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators to help them understand the controls that are likely to be relevant to meeting the applicable trust services criteria.

The scope of this report did not include the employees, locations, policies or procedures related to Dynamix or 365 IT.

F12.net uses EXA Infrastructure ("EXA"), a subservice organization, for co-location hosting services at 151 Front St. In addition, F12.net also uses BlackPoint Cyber, a subservice organization, for providing security incident event management (SIEM) and network monitoring services.

The description includes only the related controls of F12.net and excludes the controls carved out to the subservice organizations.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The System description is comprised of the following components:

- *Infrastructure* – The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization uses to provide the services.
- *Software* – The application programs, the IT system software that supports those application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop and laptop applications.

- *People* – The personnel involved in governance, management, operations, and security, as well as information about the users of the system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- *Data* – The types of data used by the system, transaction streams, files, databases, tables and output used or processed by the system.
- *Procedures* – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered and through which reports and other information are prepared.

Infrastructure

F12.net cloud services are hosted in a fully virtualized environment with power redundancy, high-performance shared storage area network (SAN) storage, redundant hypervisor hosts, and redundant networking paths. High availability features at the virtual machine level allow automatic failover and restart of virtual machine hosts in the event of hypervisor host failure.

The F12.net hosted environments are located in secure on-site server rooms in F12.net's Edmonton branch, F12.net's Toronto branch, and the 151 Front Street datacenter in Toronto. The F12 on-site server environments include the following security features:

- Triple factor authentication
- Video surveillance and 24x7x365 monitored security system
- Redundant, modular 90-160kVA uninterruptible power supply (UPS) with diesel generator backup
- Automated encrypted backups replicated between geo-redundant datacenter regions, DC East and DC West

Physical and Logical Access Controls

During business hours, visitors and personnel must pass the reception desk area to enter the F12.net regional centers. Key fob access is required to enter other secured entry doors, garages, and staff entrances. Visitors must be escorted by an F12.net employee when visiting facilities where sensitive systems and system components are maintained and operated. Security cameras are in place at facility entrances and at the main access to the datacenter. The front door entrances are locked, and access is granted by monitored access through F12.net personnel.

Access to the F12.net server room inside of the facility requires a face scanner and key fob access. Upon entrance to the server room, a secure passcode must be entered on a keypad to ensure that access has been authorized. If the secured code is not entered within 30 seconds, contact is made with the alarm company.

For internal employee access to Active Directory (AD), user account setup is communicated via email (with role level) and set up individually for each system. The request is sent from the individual's manager to Team Omega (Internal IT Team), who then performs the setup of the access.

External access by employees is permitted via AD user id and password through remote desktop connection or secured virtual private network (VPN) connections, which are secured via a Rivest-Shamir-Adleman (RSA)-encrypted 2048-bit secure sockets layer (SSL) certificate from F12.net. External access to F12.net systems require multi-factor authentication. External client servers can be accessed either with the above process or through N-Central, provided the individual is F12.net tech level or higher.

Access to the F12.net AD is disabled or removed upon notification of termination from HR to the security administrators. Once the security administrators are notified, access to the network and application is disabled within 24 hours.

Role-based access is in place for internal AD, client data applications (CRM), and client hardware support applications. Users logon to AD, CRM, or client support applications using an AD User ID and password. Password complexity standards are established to enforce control over access control software passwords. Master passwords are stored within F12.net's internal password manager, which is monitored and only accessible by the CEO, CTO, and C&S Team. Privileged user access is reviewed by the Compliance & Security Manager quarterly. For disabling access for internal employees, the employee's manager sends a request through F12.net Connect, and the Omega Team disables AD access and other application access.

Initial client administrator access is granted by F12.net and it is the responsibility of the client administrator to maintain and monitor the administrator access thereafter. Client administrators should ensure access is granted only to authorized personnel and that access is granted, modified, or removed timely when there are changes to personnel status.

Software

Software utilized to manage and support F12.net's IT environment includes systems built on modern Microsoft Windows Server platforms, Ubuntu Linux platforms, and is virtualized using VMWare vSphere 7.x. Also included in the software stack are the following products:

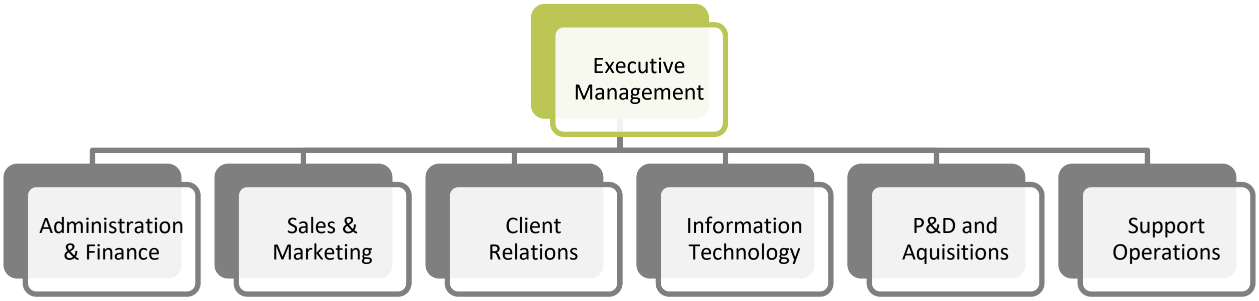
- Microsoft SQL Server 2016 and 2019, Standard and Enterprise Editions
- Microsoft Azure DevOps
- Visual Studio 2019
- Help Desk ticketing: F12 ConnectWise
- Backup and recovery tools: Cove Data Protection, Veeam Backup and Replication
- System monitoring tools: N-Central, PRTG, Zabbix, VMware vRealize Log Insight, VMware Operations Manager, VMTurbo, WatchGuard WSM, WatchGuard Dimension

The F12 Connect application is used for internal and external communication for creating and managing service tickets. The application is an intermediary between the client's ticket request and the internal ticketing system, F12 ConnectWise

People

F12.net employs dedicated team members to handle major product functions, including operations and support. The IT Team monitors the environment and manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep F12.net and its data secure.

F12.net is led by the Executive Management team, who assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments. Such assignments commonly relate to achieving corporate objectives, oversight of operating functions, and compliance with applicable regulatory requirements. Open dialogue and individual initiative are encouraged as fundamental parts of F12.net’s goal to deliver client service.



Executive Management is responsible for developing and establishing organizational goals, strategic vision, organizational direction, client strategy, market positioning, and Company growth. The department consists of the Chief Executive Officer (CEO), Chief Financial Officer (CFO), the Chief of Staff, Chief Marketing Officer (CMO), Chief Technology Officer (CTO), and Chief Operating Officer (COO).

Administration & Finance is responsible for the F12.net administration and finance. This department oversees administration functions Company-wide. Specifically, the department is responsible for accounting functions, purchasing, warehouse management, facilities management, and legal. This department reports to the Chief Financial Officer.

Sales & Marketing is responsible for client acquisition and marketing. This department is charged with developing new business opportunities. Marketing is responsible for brand recognition and client awareness. This department reports to the Chief Revenue Officer.

Client Relations is responsible for client engagement. This department is responsible for nurturing and maturing existing client relationships and developing and advancing each client’s technology strategy. This department reports to the Chief Operating Officer.

Information Technology is responsible for F12.net’s network infrastructure and the F12.net IT datacenter facility. This department also manages governance, compliance, risk, deployment, planning, and implementation of internal IT systems, maintenance, reporting, managed service allocation and billing, inventory, and Company IT initiatives. This department reports to the Chief Technology Officer.

P&D and Acquisitions is responsible for F12.net's people and development of staff, along with acquisitions of businesses to complement F12.net. This department handles the human resources of F12.net, from recruitment and professional development of the Networkers of F12. This department reports to the Chief of Staff.

Support Operations is responsible for F12.net's service delivery. This department monitors and proactively maintains client networks and provides remote and on-site technical support services. This department also manages the deployment and onboarding of clients. This is measured through a number of key performance indicators (KPIs), service level agreements (SLAs), and client surveys to ensure high client satisfaction. This department reports to the Chief Operating Officer.

Data

F12.net leverages several technologies to house data. Predominately, SQL 2016 or higher is used for internal applications. Each application communicates to a common production database. SharePoint is used as a central portal for department-specific documentation as well as F12.net's policies and procedures.

Most data that F12.net stores are name, address, client number, and phone number. F12.net deems this to be sensitive, however, low-level sensitive. F12.net stores employees' social security numbers (SSN), which are considered mid-level confidential and sensitive. F12.net also collects credit card and electronic funds transfer (EFT) information, considered the top level of sensitive data. This information is highly restricted, encrypted, and audited regularly.

Procedures

F12.net employs a set of procedures in order to obtain the stated objectives to enforce service security and change management control with proper segregation of duties among divisions. The definition and execution of these procedures are performed by the trained, qualified, experienced members of the F12.net Executive Team.

- Information Security Policies
    - Change Management Policy and Procedure
    - Data Classification
    - Data Protection and Confidentiality Policy
    - DC Host Setup Policy
    - Development Procedures and Policy
    - Disaster Recovery Plan
    - Incident Management Policy and Procedure
    - IT Security Policy and Procedure
    - Privacy Policy and Statement
    - Risk Assessment Policy

Policies and procedures are communicated to employees upon hire (new employee orientation) via security awareness programs, emails, and the Company intranet. Additionally, a quarterly risk assessment related to security threats and strategy is performed and reviewed annually by F12.net's Confidentiality Security Team. Based on the results of the assessment, the Cloud and Security (C&S) Team issues an executive report which specifies high-level risks and suggests risk-mitigating controls as well as the cost of the implementation. The report is then reviewed by the CTO and Executive Team as required.

Change Management Controls

System change requests are reviewed and approved in the following order:

- F12.net application change – approval by CTO or Director of Innovation
- Client infrastructure IMAC (Adds, Installs, Moves, Changes) – approval by point of contact
- Client configuration (client request) change – approval by client
- F12.net datacenter environment infrastructure or firewall change – approval by client
- F12.net internal firewall changes – initiated by event or system

F12.net application change releases contain a scope document reviewed by the CTO or Director of Innovation. The F12.net Senior Information Systems Developer performs code review and Quality Assurance (QA) testing. Lastly, F12.net has three separate environments – development, application build (staging), quality assurance, and production. The Information Systems Developer and the C&S department have access to the last three environments. Changes are moved from the staging server to Production.

Patching for F12.net servers is facilitated through the Remote Monitoring and Management (RMM) tool, N-Able N-Central. F12.net configured N-Able N-Central to scan for critical patch updates provided by Microsoft, and the Solutions Team is responsible for reviewing the patching status for each monitored server on a weekly basis to ensure patches are applied successfully.

Network Security and Data Communications Controls

External points of connectivity are protected by a firewall complex. For internal firewalls, firewall rules within WatchGuard limit user access to authorized connections. F12.net internal branch operations and C&S are monitored and actioned for security events 24x7. For external client firewalls, firewall rules are in place to prevent malicious attempts to connect. Authorized clients can access their devices via a specific port and an authorized user account. Secured file transfer protocol (SFTP) connections are used to transfer client data to and from F12.net's datacenter. EndPoint Detection and Response (EPDR) is installed on workstations, laptops, and servers. EPDR is modelled after a zero trust which means no process or application is permitted to be run unless approved. Laptops must be connected to the F12.net network environment to receive updates, and an alert is received by Team Omega on a daily basis. Issues are reviewed and remediated (ConnectWise ticket) as necessary.

Backup and Recovery Controls

Daily virtual full system backups are performed using the Veeam virtual backup system. Backups are monitored for success or failure using the Veeam system, and alerts are sent to C&S. If the job is a complete failure, the job is rerun. If another activity is required, a ticket is opened in ConnectWise. F12.net datacenters have failover for one another in the event of the loss of either facility to permit the resumption of operations in the event of the loss of the Edmonton facility. Business continuity and disaster recovery plans are tested annually. Client data replication testing (sample of population) is performed at a minimum on a monthly basis.

Privacy

A privacy notice outlines how personal information is collected, used, retained, disclosed, and disposed of per the Company's commitments. The Privacy Officer is responsible for the privacy policies and procedures. The privacy notice is reviewed annually and updated as needed.

The privacy notice outlines the purposes for which personal information is collected, used, retained, and disclosed to those whose information is processed, processed, or used. Personal information is collected only for the purposes outlined in the privacy notice. The use of the website and services is considered consent and acknowledgement of the privacy notice.

F12.net retains personal information for only as long as necessary to fulfill the stated purposes or required by law or regulation and disposes of the information in a timely manner.

Third parties and vendors are utilized to provide services as part of the system description. However, these third parties and vendors do not have access to personal information.