Extol Corporation Sdn Bhd

Electronic Banking Confirmation ("EBC") Platform

System Organisation Controls (SOC) 3 Report

For the Period from September 1, 2020 to February 28, 2021

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITORS’ REPORT

Deloitte PLT (LLP0010145-LCA)
Chartered Accountants (AF0080)
Level 16, Menara LGB
1 Jalan Wan Kadir
Taman Tun Dr. Ismail
60000 Kuala Lumpur

P.O. Box 10093
50704 Kuala Lumpur
Malaysia

Tel: +60 3 7610 8888
Fax: +60 3 7726 8986
myaaa@deloitte.com
www.deloitte.com/my

1 Independent Service Auditors' Report

Extol Corporation Sdn Bhd

1-40-1, Menara Bangkok Bank
Berjaya Central Park
No. 105, Jalan Ampang
50450 Kuala Lumpur

Scope

We have examined the attached description of the system of Extol Corporation Sdn Bhd (the "Service Organization" or "Extol") related to its Electronic Banking Confirmation ("EBC") Platform (also known as eConfirm Platform) and description of IP Server One Solutions Sdn Bhd (the "Sub-Service Organization" or "IPS") scope of services related to its data center hosting and infrastructure monitoring services for the period September 1, 2020 to February 28, 2021 ('the Description') based on the criteria for a description of a Service Organization's system set forth in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 3® Report ("description criteria"), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period September 1, 2020 to February 28, 2021, to provide reasonable assurance that Extol service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and processing integrity ("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 Extol, to achieve Extol's service commitments and system requirements based on the applicable trust services criteria. The description presents Extol's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Extol'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

The Service Organization 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 the Service Organization's service commitments and system requirements were achieved. The Service Organization has provided the accompanying assertion titled "Management Assertion of Extol

Corporation Sdn Bhd." ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. The Service Organization 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.

Sub-Service Organization's Responsibilities

The Sub-Service Organization is responsible for providing its data center hosting and infrastructure monitoring services and for operating effective controls in relation to Extol's EBC Platform to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved. The Sub-Service Organization has provided the accompanying assertion titled "MANAGEMENT ASSERTION OF IP SERVER ONE SOLUTIONS SDN BHD ("IPS")" ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. The Sub-Service Organization 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 Independence and Quality Control

We are independent of the Company in accordance with the By-Laws (on Professional Ethics, Conduct and Practice) of the Malaysian Institute of Accountants ("By-Laws") and the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (including International Independence Standards) ("IESBA Code") and we have fulfilled our other ethical responsibilities in accordance with the By-Laws and the IESBA Code.

In accordance with International Standards on Quality Control 1 *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements* as adopted by the Malaysian Institute of Accountants, Deloitte PLT maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of the design and operating effectiveness of the controls stated in the Description based on our examination. Our examination was conducted in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, as adopted by the Malaysian Institute of Accountants. That standard requires 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 and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

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

- Obtaining an understanding of the system and service organizations's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Extol'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 Extol'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. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, 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 Extol'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.

Intended users

This report is intended solely for customers who have used Extol's EBC platform during some or all of the period September 1, 2020, to February 28, 2021, and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by customers themselves.

Opinion

In our opinion, management's assertion that the controls within the Extol's and IPS were effective throughout the period September 1, 2020 to February 28, 2021, to provide reasonable assurance that Extol's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

August 30, 2021

Deloitte PLT

SECTION 2

SERVICE ORGANISATION’S STATEMENT

2 Service Organisation's Statement

2.1 Management Assertion Provided by Extol

We are responsible for designing, implementing, operating, and maintaining effective controls within Extol Corporation Sdn Bhd ("Service Organization" or "Extol") related to its Electronic Banking Confirmation ("EBC") Platform (also known as eConfirm Platform), throughout the period September 1, 2020, to February 28, 2021, to provide reasonable assurance that EBC Platform's service commitments and system requirements relevant to security, availability, processing integrity, and confidentiality were achieved. Our description of the boundaries of the system is presented 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 September 1, 2020, to February 28, 2021, to provide reasonable assurance that EBC Platform's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity and confidentiality ("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). EBC Platform'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 in Section 4.

Extol uses IP Server One Solutions Sdn Bhd ("subservice organization" or "IPS") for its data center hosting and infrastructure monitoring services. Extol Description includes a description of IPS' services used by Extol, including the controls of Extol and the controls designed by Extol and operated by IPS that are necessary, along with controls for EBC Platform, to achieve Extol's service commitments and system requirements based on the applicable trust services criteria.

This assertion and the Description of the EBC Platform indicate that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Extol to achieve its service commitments and system requirements related to EBC Platform based on the applicable trust services criteria. The accompanying Description of the EBC Platform presents the complementary user entity controls assumed in the design of Extol's controls.

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 September 1, 2020, to February 28, 2021, to provide reasonable assurance that EBC Platform's service commitments and system requirements were achieved based on the applicable trust services criteria.

2.2 Management Assertion Provided by IPS

IP Server One Solutions Sdn Bhd ("IPS") provides data centre hosting and infrastructure monitoring services to Extol Corporation Sdn Bhd ("Extol"). The services provided by IPS ("IPS' scope of services") are part of Extol's EBC Platform.

IPS' scope of services are intended to provide users with information about IPS' services provided to Extol's EBC Platform that may be useful when assessing the risks arising from interactions with Extol's system, particularly information about controls operated by IPS 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 and Availability.

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 IPS' controls which were designed by Extol, were effective throughout the period September 1, 2020 to February 28, 2021, to provide reasonable assurance that Extol's service commitments and system requirements were achieved based on the applicable trust services criteria.

SECTION 3

SERVICE ORGANISATION’S SYSTEM DESCRIPTION

3 Description of the System

Company Background

Extol Corporation Sdn Bhd ("Extol") is a fully owned subsidiary of AppAsia Berhad, which is a public listed company on Bursa Malaysia ACE market since 2006.

Established since 1984, Extol is an information technology ("IT") solutions provider specializing in IT security, secured enterprise application, digital platform solution and managed cloud services. In 2018, Extol was selected by Malaysian Institute of Accountants ("MIA") to develop the Industry-Wide Electronic Banking Confirmation ("EBC") Platform or also known as eConfirm Platform.

The EBC platform was launched on 26 June 2021 by Extol and MIA. It can be accessible through the internet with a public domain name http://eConfirm.my.

Description of Services Provided

The EBC Platform is an online system to facilitate the audit process for the auditors and banks operating in Malaysia as required under the International Standards on Auditing (ISA) 505 External Confirmations.

Under ISA 505, reliable audit evidence can be obtained in documentary form from a third party, e.g. a bank, whether on paper, electronically or in another medium. Many bank confirmation request letters are sent to banks annually by auditors for confirmation of their clients' bank and arrangements.

EBC Platform is an efficient and secure way to request bank confirmations without the risk of fraud going undetected, i.e. through electronic confirmation. This electronic platform enhances the security of the bank confirmation process whereby it verifies organizations and users, ensures confirmations are only sent and received by registered auditors and banks, reduces risks of fraud related to the bank confirmation process, enhances efficiency in the bank confirmation process, saves valuable time and effort that can be diverted to other higher value-added work.

Infrastructure and Software

The primary infrastructure and software used to provide EBC Platform include the following systems:

Production Application	Business Function Description	Operating System Platform	Physical Location
Proxmox VE	Server virtualization management platform.	Debian-based Linux distribution	CJ1 Data Center, Cyberjaya
FreeIPA Directory	Identity management system.	CentOS Linux	CJ1 Data Center, Cyberjaya
Web Application Servers	Front-end and back-end facing web application.	CentOS Linux	CJ1 Data Center, Cyberjaya
Scheduling Servers	To perform scheduled batch processing tasks.	CentOS Linux	CJ1 Data Center, Cyberjaya
Postgres Database	Database server.	CentOS Linux	CJ1 Data Center, Cyberjaya

Production Application	Business Function Description	Operating System Platform	Physical Location
Redis	Caching server.	CentOS Linux	CJ1 Data Center, Cyberjaya
GlusterFS File Server	Highly available replicated file storage cluster	CentOS Linux	CJ1 Data Center, Cyberjaya
Crypto Server	To perform user authentication, encryption and decryption for sensitive data and files before the storage.	CentOS Linux	CJ1 Data Center, Cyberjaya
Payment Server	To integrate with external payment gateway.	CentOS Linux	CJ1 Data Center, Cyberjaya
Vault Server	To store sensitive encryption key information.	CentOS Linux	CJ1 Data Center, Cyberjaya
Firewall/IPS	To filter incoming and outgoing traffic based on predefined firewall policy.	Fortigate	CJ1 Data Center, Cyberjaya
TICK Stack Monitoring System	Provide 24x7 real time monitoring and alerts related to availability, capacity, performance of infrastructure hardware and system services. It monitors loads, memory usage, CPU, disk space, network performance etc.; and instantly alerts IT operations for failure via instant messaging system and email.	CentOS Linux	CJ1 Data Center, Cyberjaya
VPN	To control access the production environment based on user access rights matrix.	Fortigate	CJ1 Data Center, Cyberjaya
AlienVault OSSIM	Security information and event management system (SIEM) to monitor security event activity and vulnerability assessment.	Debian-based Linux distribution	CJ1 Data Center, Cyberjaya
JIRA	To record incident and case management.	CentOS Linux	Operation office at Megan Avenue 1, Kuala Lumpur

People

The present team involved in EBC Platform includes the following departments and roles:

- Executive Director: Provides overall lead, general oversight, and strategic planning and direction.
- Research and Development Department: Responsible for software research, development, enhancement and maintenance.
- System Support Department: Responsible for software installation, system configuration, IT operations, system backup and maintenance of system infrastructure, hardware and software.

- Service and Compliance Department: Responsible for servicing customers by providing product and service information, including training, issues reporting and escalation; ensure regularly scheduled audits relating to defined policies, procedures and standards; provides continuous improvement feedback; and assesses legal and regulatory requirements.

Policies and Procedures

Formal policies and procedures exist that describe computer operations, change control, and data communication standards. All teams are expected to adhere to the Extol policies and procedures that define how services should be delivered. The policies and procedures are located in Extol files repository in softcopy and hardcopy. Policies include the following:

- Information Security Policies and Standards (which encompasses all eighteen (18) families of ISO/IEC 27001:2013 Information Security Management System (ISMS))
- Termination of Employment Policy
- Data Protection Policy

Data

EBC Platform does not process or store any sensitive personal data. The followings are the data stored and processed on the EBC Platform:

Data	Data Description
User Data	Auditors' and Banks' general user information for verification purpose
Encrypted authorisation files	Authorisation files are encrypted by the users before uploading to the EBC Platform as attachment which can only be decrypted by authorised recipients
Encrypted confirmation files	Confirmation files are encrypted by the users before uploading to the EBC Platform as attachment which can only be decrypted by authorised recipients
Company Information	General company information and application activity logs related to the confirmation requests used for verification purpose

Sub-Service Organization

EBC Platform utilizes the data centre hosting and infrastructure monitoring services located at CJ1 Data Center, Cyberjaya, provided by IP Server One Solutions Sdn Bhd ("IPS"). Physical accesses to the servers are restricted via card access. Approvals are provided by data centre management before staff are granted with the card access. Physical accesses to the servers are removed upon the staff's last working day. Access cards are returned to the data centre manager as part of the staff's exit procedure.

The data centre operation team meets on periodically to review and discuss operational matters, which includes reviewing the current data centre access list to ensure it remains relevant. Visitors, including customers, are required to register themselves through Extol IT support team in IPS' visitor portal and approved by the data centre manager before being allowed access to the premises. Visitors must be escorted at all time at the premises.

Sub-Service Organization has implemented environmental controls such as fire suppressions systems, generators, UPS, raised flooring, cooling and temperature and humidity detectors. These environmental controls are serviced periodically to ensure optimal working condition.

Trust Service Criteria Not Applicable to the in-Scope System

All criteria within the security, availability, processing integrity and confidentiality categories are applicable to the EBC Platform except for privacy category because EBC Platform does not process or store sensitive personal data in its environment.

RELEVANT ASPECTS OF EBC PLATFORM CONTROL ENVIRONMENT. RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION SYSTEMS AND MONITORING.

1. **Control Environment.** Sets the tone for the Extol organization, influencing the control consciousness of employees and management. It is the foundation for all other components of internal control, providing service organization discipline and structure.
2. **Policies and Procedures.** The policies, procedures and related execution (automated and manual) that help make sure that Extol Management's directives are carried out.
3. **Information and Communication.** Systems, both automated and manual, that support the identification, capture, and exchange of Extol information in a form and timeframe that enable our employees and management to carry out their responsibilities.
4. **Monitoring.** The ongoing processes that assesses the quality of internal control performance over time.
5. **Risk Assessment.** Our identification and analysis of relevant risk to the achievement of our objectives or impact to our company, partners or customers, forming a basis for determining how the risks can be most effectively managed.

Control Environment

The internal control objectives related to EBC Platform are to provide reasonable, but not absolute, assurance that controls are suitably designed and operating effectively to meet our risk appetite. This means that assets are protected from unauthorized use or disposition, that transactions are executed in accordance with management's authorization and client instructions, and that customer data is secure.

Management has established and maintains controls designed to monitor compliance with established Extol policies and procedures. The remainder of this subsection discusses the "tone at the top" as set by Extol's management; the integrity, ethical values, and competence of Extol employees; the policies and procedures to guide controlled execution by our employees and management; the risk management process and monitoring; and the roles of significant control groups. The internal control structure is established and refreshed based on Extol's assessment of inherent and residual risk faced by organization.

Integrity and Ethical Values

Extol believes that the effectiveness of controls correlates with the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Extol's control environment, affecting the design, administration, and monitoring of its service organization components. Integrity and ethical behavior are the product of Extol's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Commitment to Competence

Extol's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. This includes management's consideration of the competency levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Management’s Philosophy and Operating Style

Extol's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, confidential and privacy-related data, accounting functions, and personnel.

Organizational Structure

Extol's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. This organizational structure is based, in part, on the size and the nature of the service organization’s activities. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility.

Governance and Oversight: Human Resource Procedures and Practices

Human Resource procedures and practices are enforced with a high level of efficiency, integrity, and ethical standards. Evidenced by its proven track record for hiring and retaining top-quality personnel who ensure the service organization is operating at maximum efficiency. Extol's human resources procedures and practices relate to employee hiring, orientation, training, evaluation, promotion, compensation, and disciplinary activities.

Risk Assessment

Extol's risk assessment process identifies and manages risks that could potentially affect Extol's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Extol identifies the underlying sources of risk, measures the impact on the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Extol and its Sub-Service organization, IPS, that provides data centre hosting and infrastructure monitoring services. Extol management has implemented various measures designed to manage these risks.

Information System

Information should be made available with minimal disruption to staff and the public as required by the business process. The integrity of this information will be maintained. Confidentiality of information not limited to research, third parties, personal and electronic communications data will be assured.

Information security education, awareness and training will be made available to staff. All breaches of information security, actual or suspected, will be reported to, and investigated by the relevant authorities not limited to System Administration and Incident Response.

Policies and Procedures

Extol has the following security procedures and policies in place as following:

1. ECSB-POL-01 Information Security Policies and Standards
2. ECSB-POL-03 Data Protection Policy
3. ECSB-P02 Internal Audit Procedure
4. ECSB-P03 Management Review Procedure
5. ECSB-P05 Risk Management Procedure
6. ECSB-P06 ISMS Security Measurement Effectiveness
7. ECSB-P08 User Access Management Procedure
8. ECSB-P09 Backup and Media Handling Procedure
9. ECSB-P10 Maintenance of Asset Procedure
10. ECSB-P11 Operational Change Management & Capacity Planning Procedure
11. ECSB-P12 Fault Logs Procedure
12. ECSB-P13 Security Incident Management Procedure
13. ECSB-P14 System Security Monitoring
14. ECSB-P16 Server Deployment & Remote Access Procedure
15. ECSB-P17 Research and Development
16. ECSB-P18 Information Classification & Handling
17. ECSB-P19 Business Continuity Planning
18. ECSB-P20 Supplier Agreement Management
19. ECSB-P29 Yearly Performance Review
20. ECSB-P22 Recruitment and Placement
21. ECSB-P30 Disciplinary Procedure
22. ECSB-P34 Audit Firm Activation Procedure
23. ECSB-P35 Bank Creation Procedure
24. ECSB-P36 Server Deployment & Remote Access Procedure
25. ECSB-P38 Service Desk Incident Management Procedure
26. ECSB-P39 Disaster Recovery Plan & Procedure
27. ECSB-P40 Company Key Revocation Procedure
28. ECSB-P41 Browser Security Review Procedure

Communication System

Extol maintains an extensive set of controls to manage effective communication internally (with personnel) and externally (with customers, partners, and other specific entities). A description that delineates the EBC Platform is available to external users via the EBC Platform's website. A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority. Reporting relationships and organizational structures are reviewed periodically by management.

Extol’s roles and responsibilities are defined in written job descriptions and communicated to personnel. Management reviews the job descriptions periodically and makes updates, if necessary. Employees are required to review, sign and accept the employee handbook and agreement upon hire. Newly hired employees are required to undergo information security training upon hire and annually thereafter. Policies and procedures are documented for significant processes and are available on the entity's intranet.

Customer responsibilities are documented in contracts, and general guidelines are outlined and communicated via the EBC Platform's website. Internal and Sub-Service organization processes are monitored through service level management procedures to ensure compliance with service level commitments and agreements. Security and privacy commitments are communicated to external users via the EBC Platform's website.

Ticketing System

JIRA is a web-based ticketing application system that provides internal staff with the ability to submit technical issues, security incidents or requests for system changes to accounted personnel. To ensure that only authorized requests are accepted, each user is assigned a unique user ID and required to set a confidential password prior to being granted access. The team associated with the queue receives notification that a new request has been submitted to the queue. The request is assigned to the appropriate team member, who attempts to resolve the request. If additional information is required, the requestor is contacted via the ticket, and the request is put on hold until the information is received thus creating a continual journal of dialogue and actions.

Logical Security

Extol has established an information asset listing based on the requirements of ISMS. Assets are classified based on criticality in accordance with the EBC Platform. The asset listing is reviewed on a yearly basis. The information classification procedure to identify the criticality of the information related to the EBC platform. This procedure is reviewed on a yearly basis.

Network segmentation has been implemented for the EBC Platform Infrastructure. The web application and database servers are separated into different subnets to reduce the risk of direct access to the servers using VLAN. Web servers are placed in the DMZ. All ports are configured and restricted according to the required services of servers by following predefined server deployment guide as established in the Server Deployment Procedure. Internal vulnerability assessments are performed monthly to detect any open ports and associated vulnerabilities.

The firewall is configured to restrict the access of traffic to production environment. The remote access to the firewall is restricted only to the following conditions:

a. Trusted IP source from internal network
b. Authorised MAC address
c. 2-factor authentication with hard token for VPN access

The firewall ruleset to the EBC environment has been documented, backed up on a monthly basis and configured accordingly to restrict traffic/access to the network. The ruleset contains a lockdown rule as to deny all access unless specifically permitted.

Only authorised users are granted access to critical servers and network infrastructure in production environment as per User Access Matrix. Login process into every server in the production environment is controlled by identity management systems.

User credentials used to access EBC platform meets the applicable password policy requirements in the IT Security Policy such as expiration, length, complexity and history. Authentication of users are performed at the backend application server and concurrent user ID logins are disabled. Users are forced to create password and change credentials when accessing the platform for the first time.

VPN is established to restrict users into the EBC system production environment. Access to VPN is only granted to authorised personnel, upon approval by management. Users also require a hard token that provides a 2-factor authentication number in order to be granted access.

The EBC Platform has a self-service password reset function. One Time Password (“OTP”) is randomly generated and will expire after 10 minutes.

The super users for the EBC Platform and its supporting infrastructure are held by the Executive Director or approved designate. Other elevated access IDs (read, write, user administration) are restricted to authorised personnel through designated channels based on job responsibilities. Requests for new access, or modifications to existing access to infrastructure-related assets are appropriately approved prior to access provisioning, based on the User Access Management Procedures. Access privileges to the IT Infrastructure are reviewed on an annual basis to determine if access rights are commensurate to the user’s job duties. Access is modified based on the results of the reviews.

The EBC Platform separates the login domains and functions of the banks and auditors. Banks and auditors’ users are assigned with separate roles and functions within the system by authorised personnel from the respective Banks and Auditors. Bank users are required to provide authorised IP addresses to be whitelisted.

Monitoring

Extol management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Extol management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored.

COMPLEMENTARY USER ENTITY CONTROL CONSIDERATIONS (CUECs')

1. User entities are responsible for understanding and complying with their contractual obligations to Extol.
2. User entities are responsible for ensuring the supervision, management and control of the use of Extol services by their personnel.
3. User entities are responsible for developing their own disaster recovery and business continuity plans that address their inability to access or utilize Extol services.
4. User entities are responsible for immediately notifying Extol of any actual or suspected information security breaches, including compromised user accounts, including those used for integration and secure file transfers.
5. User entities are responsible for establishing and adhering to security procedures to prevent the unauthorized personnel, vendors and contractors as well as changes to technical or administrative contact information.
6. User entities are responsible for notifying Extol of terminated employees with access to the Extol data centre within a timely manner.
7. User entities are responsible for creating and communicating specific escalation procedures for problems with their services and for notifying Extol of changes to their escalation procedures.
8. User entities are responsible for maintaining a list of authorized customer contacts with the ability to initiate changes to subscribed services.
9. User entities are responsible for obtaining appropriate approval of customer-requested changes to their environment(s).
10. User entities are responsible for providing updated information for their designated to liaised contact and billing contact personnel.
11. User entities are responsible for obtaining appropriate approval of security-related emergency changes.
12. User entities are responsible for monitoring their user accounts and administrative activity on business user system at Extol.
13. User entities are responsible for creating, maintaining and disseminating their own Information Security Policy.

SECTION 4

Principal Service Commitments and System Requirements

4 Principal Service Commitments and System Requirements

Extol makes service commitments to its customers and has established system requirements as part of its EBC Platform. Some of these commitments are principal to the performance of the service and relate to applicable trust services criteria. Extol 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 Extol’s service commitments and system requirements are achieved.