Deloitte.

Extol Corporation Sdn Bhd

System and Organisation Controls 3 (SOC 3) Report

Report on the Electronic Banking Confirmation ("EBC") System relevant to Security, Availability, Confidentiality and Processing Integrity

For the Period from January 1, 2023, to December 31, 2023

Independent Service Auditors' Assurance Report

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

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

Scope

We have examined Extol Corporation Sdn Bhd (known as the "Service Organisation" or "Extol") accompanying assertion titled "Service Organisation Statement" in Section 2, that the controls within Extol's Electronic Banking Confirmation ("EBC") Platform services were effective throughout for the period January 1, 2023 to December 31, 2023 to provide reasonable assurance that Extol's service commitments and system requirements were achieved based on trust services criteria relevant to security, availability, confidentiality, and processing integrity ("applicable trust services criteria") as set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy.

Service Organisation's Responsibilities

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 the Extol's service commitments and system requirements were achieved. Extol has provided the accompanying assertion about the effectiveness of controls within the system. Extol is responsible for selecting, and identifying in its statement, the applicable trust service criteria and for having a reasonable basis for its statement by performing assessment of the effectiveness of controls within the system..

Service Auditor's Independence and Quality Management

We are independent of the Service Organisation in accordance with the *By-Laws (on Professional Ethics, Conduct and Practice)* of the Malaysian Institute of Accountants ("By-Laws") and the International Ethics 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.

The firm applies Malaysian Standard on Quality Management 1 ("ISQM-1"), Quality Management for Firms that Perform Audits or Reviews of Historical Financial Statements, or Other Assurance or Related Services Engagements, which requires the firm to design, implement and operate a system of quality management including 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, based on our examination on Extol 's statements that controls within the system were effective throughout the period to provide reasonable assurance that the service organisation's service

commitments and system requirements were achieved based on the applicable trust services criteria. 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. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether Extol's statements 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 involves the following:

- Obtaining an understanding of the system and the service organisation'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.

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.

Opinion

In our opinion, management's statement that the controls within the Extol's Electronic Banking Confirmation ("EBC") Platform services were effective throughout the period January 1, 2023 to December 31, 2023, 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.

DELOITTE PLT (LLP0010145-LCA)
Chartered Accountants (AF0080)
May 9, 2024

Assertion of Extol Corporation Sdn Bhd Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Extol Corporation Sdn Bhd (Extol) Electronic Banking Confirmation ("EBC") System (system) throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Extol'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, in AICPA Trust Services Criteria. fn 1 Our description of the boundaries of the system is presented in attachment A 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 January 1, 2023 to December 31, 2023, to provide reasonable assurance that Extol's service commitments and system requirements were achieved based on the applicable trust services criteria. Extols'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 attachment B.

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 January 1,2023 to December 31, 2023, to provide reasonable assurance that Extol's service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A – Extol & EBC System Overview

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 Organisations 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 Centre, Cyberjaya
FreeIPA Directory	Identity management system.	CentOS Linux	CJ1 Data Centre, Cyberjaya
Web Application Servers	Front-end and back-end facing web application.	CentOS Linux	CJ1 Data Centre, Cyberjaya
Scheduling Servers	To perform scheduled batch processing tasks.	CentOS Linux	CJ1 Data Centre, Cyberjaya
Postgres Database	Database server.	CentOS Linux	CJ1 Data Centre, Cyberjaya
Redis	Caching server.	CentOS Linux	CJ1 Data Centre, Cyberjaya
GlusterFS File Server	Highly available replicated file storage cluster	CentOS Linux	CJ1 Data Centre, Cyberjaya
Crypto Server	To perform user authentication, encryption and decryption for sensitive data and files before the storage.	CentOS Linux	CJ1 Data Centre, Cyberjaya
Payment Server	To integrate with external payment gateway.	CentOS Linux	CJ1 Data Centre, Cyberjaya
Vault Server	To store sensitive encryption key information.	CentOS Linux	CJ1 Data Centre, Cyberjaya
Firewall/IPS	To filter incoming and outgoing traffic based on predefined firewall policy.	Fortigate	CJ1 Data Centre, 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	CentOS Linux	CJ1 Data Centre, Cyberjaya

Production Application	Business Function Description	Operating System Platform	Physical Location
	alerts IT operations for failure via instant messaging system and email.		
VPN	To control access the production environment based on user access rights matrix.	Fortigate	CJ1 Data Centre, Cyberjaya
AlienVault OSSIM	Security information and event management system (SIEM) to monitor security event activity and vulnerability assessment.	Debian-based Linux distribution	CJ1 Data Centre, Cyberjaya
JIRA	To record incident and case management.	CentOS Linux	Operation office at Megan Avenue 1, Kuala Lumpur

People

The 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 following 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 Organisation

EBC Platform utilizes the data centre hosting and infrastructure monitoring services located at CJ1 Data Centre, 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. The server racks are protected with a secure passcode which is held by authorised personnel.

All visitors are required to register themselves through Extol IT support team in IPS visitor portal and approved by the data centre management before being allowed access to the premises. Visitors must be escorted at all times at the premises.

Sub-Service Organisation 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.

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 unauthorised use or disposition, that transactions are executed in accordance with management's authorization and client instructions, and that customer data is secure.

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 Organisation 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.

Organisational Structure

Extol's Organisational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. This Organisational structure is based, in part, on the size and the nature of the service Organisation's activities. Management believes establishing a relevant Organisational 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 Organisation 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 Organisations. 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 Organisation, 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 Organisation, 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.

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 describes the EBC Platform is available to external users via the EBC Platform's website. A documented Organisational chart is in place to communicate Organisational structures, lines of reporting, and areas of authority. Reporting relationships and Organisational 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 Organisation 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 authorised 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. Other than that, External Vulnerability Assessments are performed on all critical servers within production environment on an annual basis. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum.

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 15 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.

Attachment B: Principal Service Commitments and System Requirements

Extol designs its processes and procedures related to the EBC Platform to meet its objectives for its services. Those objectives are based on the service commitments that Extol makes to its customers, business partners, and vendors, and the operational and compliance requirements that Extol has established for the services. Service commitments are declarations made by management to its customers regarding the performance of the EBC Platform. Service commitments are set forth in standardized contracts, service level agreements, and in the description of the service offering provided online and include the following:

- Commitments regarding the security and availability of the system and confidentiality of information processed by the system in accordance with contractual stipulations.
- Commitments regarding customer interactions as described in the master service agreement, service level agreement, and the system reference document.
- Commitments to support customer compliance with the security-related requirements of the bank regulators.

Extol establishes operational requirements that support the achievement of security commitments, relevant operational and compliance requirements, applicable laws and regulations, and other system requirements. These include system requirements (both functional and non-functional) derived from service commitments, published documentation of system functionality, and other descriptions of the system.

Such requirements are communicated in Extol's system policies and procedures, system design documentation, and contracts with customers.

Extol has adopted the ISMS Manual as the basis for its organization-wide information security policies. In addition to these policies, standard operating procedures have been developed and documented on how to carry out specific manual and automated processes required in the operation and development of the EBC Platform. System requirements include the following:

• Data, personnel, devices, systems, and facilities are identified and managed.
• Extol management understands and manages the cybersecurity risk to organizational operations.
• Extol’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
• Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
• Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.
• Security policies, processes, and procedures are maintained and used to manage protection of information systems and assets.
• Maintenance and repairs of information system components are performed consistent with policies and procedures.
• Technical security solutions are managed to help ensure the security and resilience of systems and assets.
• Anomalous activity is detected and the potential impact of events is understood.

• The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
• Detection processes and procedures are maintained and tested to help ensure awareness of anomalous events.
• Response processes and procedures are executed and maintained to help ensure response to detected cybersecurity incidents.
• Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
• Recovery processes and procedures are executed and maintained to help ensure restoration of systems or assets affected by cybersecurity incidents.

About Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more. Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

About Deloitte Malaysia

In Malaysia, services are provided by Deloitte PLT (LLP0010145-LCA) (AF0080), a limited liability partnership established under Malaysian law, and its affiliates.