basware
Now it all just happens™

Basware Corporation

BASWARE NETWORK SOLUTION

INDEPENDENT AUDITOR'S REPORT ON BASWARE CORPORATION DESCRIPTION ON ITS SYSTEM AND THE SUITABILITY OF DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

ISAE 3402 TYPE II REPORT

November 26th, 2025

CONTENTS

SECTION ONE

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT

Service Auditor's Assurance Report

To: Basware Corporation

Scope

We have been engaged to report on the Basware service description of its Basware Network solution (hereinafter also "Basware Network") for processing customers' transactions throughout the period from January 1st, 2025 to September 30th, 2025 and on the design and operation effectiveness of controls related to the control objectives stated in the description.

Basware uses subservice organizations Amazon Web Services (AWS) and Microsoft Azure (Azure) to provide cloud infrastructure services for its Basware Network solution. The Description indicates that complementary subservices organization controls that are suitably designed and operating effectively are necessary, along with controls at Basware, to achieve Basware's control objectives. For its description Basware uses the carve-out method. The description also indicates that certain control objectives specified by Basware can be achieved only if complementary subservice organization controls assumed in the design of Basware's controls are suitably designed and operating effectively, along with the related controls at Basware. We have not evaluated the design or operating effectiveness of such complementary subservice organization controls.

The Description indicates that certain complementary user entity controls must be suitably designed and implemented at user entities for related controls at the service organization to be considered suitably designed to achieve the related control objectives. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Basware's Responsibilities

Basware is responsible for preparing the description and the accompanying statement in Section 2 (Statement) including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on Basware's description and on the design and operation of controls related to the control objectives stated in that description based on our procedures. We conducted our engagement in accordance with the International Standard on Assurance Engagements 3402, '*Assurance Reports on Controls at a Service Organisation*' issued by the International Auditing and Assurance Board. That standard requires that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An

assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organisation.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Our Independence and Quality Control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' *International Code of Ethics for Professional Accountants (including International Independence Standards)* (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies International Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*, which requires the firm to design, implement and operate a system of quality management including documented policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Limitations of Controls at a Service Organisation

Basware's description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in Basware Oy's Statement in Section 2. In our opinion, in all material respects:

(a) The Description fairly presents the Basware Network system as designed and implemented throughout the period from January 1st, 2025 to September 30th, 2025;

(b) The controls related to the control objectives stated in the Description were suitably designed throughout the period from January 1st, 2025 to September 30th, 2025; and

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from January 1st, 2025 to September 30th, 2025.

Description of Tests of Controls

The specific controls tested and the nature, timing and results of those tests are listed in Section 4.

Intended Users and Purpose

This report and the description of tests if controls on section 4 are intended only for user entities who have used the Network solution provided by Basware, and their auditors, who have a sufficient understanding to consider the report and the description along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial statements.

Helsinki, on November 26th, 2025

KPMG Oy Ab

DocuSigned by:
2477B01D945A425...

Jussi Paski
Partner
Authorized Public Accountant

DocuSigned by:
BB057897E6F64C0...

Mika Iivari
Partner
Head of Cyber Advisory

SECTION TWO

basware
Now it all just happens™

STATEMENT BY THE SERVICE ORGANISATION

We have prepared the description of Basware's Network solution solution for processing user entities' transactions at section 3 throughout the period January 1st, 2025 to September 30th, 2025, (description) for user entities of the system during some or all of the period January 1st, 2025 to September 30th, 2025, and their user auditors who have a sufficient understanding to consider the description, along with other information, including information about controls operated by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements

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

a) The accompanying description fairly presents the Basware Network solution made available to user entities during some or all of the period January 1st, 2025 to September 30th, 2025. Basware uses a Amazon Web Services service organization for cloud infrastructure. The description includes only the controls and related control objectives of Basware and excludes the control objectives and related controls of the Amawon Web Services service organization. The criteria used in making this statement were that the accompanying description:

   i) Presents how the system was designed and implemented, including:

   - The types of services provided, including, as appropriate, the classes of transactions processed;
   - The procedures, within both automated and manual systems, by which those transactions were initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports prepared for user entities;
   - The information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information and specific accounts involved in initiating, authorizing, recording, processing and reporting transactions; this includes the correction of incorrect information and how information was transferred to the reports and other information prepared for user entities;
   - How the system captured and addressed significant events and conditions, other than transactions;
   - The process used to prepare reports or other information for user entities
   - Specified control objectives and controls designed to achieve those objectives including, as applicable, complementary subservice organization controls assumed in the design of the service organization's controls
   - Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved solely by controls implemented by ourselves alone; and
   - Other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities and monitoring controls that were relevant to processing and reporting user entities' transactions.

basware
Now it all just happens™

ii) includes relevant details of changes to the service organisation's system during the period from January 1st, 2025 to September 30th, 2025;

iii) does not omit or distort information relevant to the scope of the Basware Network solution system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities and their auditors and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment;

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from January 1st, 2025 to September 30th, 2025. The criteria used in making this statement were that:

i) the risks that threatened achievement of the control objectives stated in the description were identified; and

ii) the identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and

The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from January 1st, 2025 to September 30th, 2025.

South Carolina, on November 26th, 2025

DocuSigned by:
Jason Kurtz
707D40B4166549B...

Jason Kurtz
Chief Executive Officer
Basware Corporation

SECTION THREE

basware
Now it all just happens™

DESCRIPTION OF SERVICES PROVIDED BY BASWARE

1.1 Overview of the Service Organization and the Services Provided

Basware is a global leader in providing Accounts Payable and Invoice Automation Solutions to customers of all sizes globally. Through its Invoice Lifecycle Management SaaS platform ("Cloud Services"), it automates and oversees the entire invoice process, from creation and approval to payment and reconciliation. By replacing fragmented, manual workflows with a unified, AI-powered solution, it ensures accuracy, compliance, and control at every stage, while giving finance teams the visibility they need to make smarter, faster decisions.

Basware aligns with good industry practices and has implemented both a Quality Management System (QMS) and an Information Security Management System (ISMS) that are independently certified to the ISO9001 and ISO27001 standards respectively.

The scope of this report covers the General Information Technology Controls and Application Controls of Basware Network ("System") to the extent that Basware is responsible for operating these controls.

1.2 Principal Service Commitments and System Requirements

Basware designs its processes and procedures related to its Cloud Services to meet its objectives. Those objectives are based on the service commitments to customers, the laws and regulations that govern the provision of the services and the financial, operational and compliance requirements that Basware has established for the services.

Security commitments to customers are documented and communicated in Service Level Agreements (SLAs) and other customer agreements.

Basware establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Basware policies and procedures, system design documents, and contracts with customers. Information security policies define an organization-wide approach to how the System and data are protected. These include policies around how the System 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 to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the System.

1.3 Components of the System

Infrastructure

The system infrastructure is cloud-based and hosted in AWS data centers, which are physically and environmentally access-controlled. AWS provides core infrastructure services including automated backup and recovery, multi-zone replication for high availability. Basware is responsible for application-level backups and continuous monitoring of system performance and security including IDS/IPS.

AWS CloudFormation, AWS SAM and AWS CDK are used to deploy secure resources within the AWS environment. Production servers supporting the System utilize Linux Operating systems. The following key technologies are used:

- Data management - Amazon S3, AWS Glue Data Catalog, Amazon EMR Serverless, AWS Glue Jobs.
- Data analytics - Amazon Quicksight
- RDBS databases - Amazon RDS with either Oracle, MySQL, PostgreSQL or MSSQL engines
- NoSQL databases - Amazon DynamoDb and Amazon DocumentDb with MongoDB

Azure compatible IaC solutions are used to deploy secure resources within the Azure environment. Production servers supporting the System utilize Linux Operating systems and are supported by MySQL.

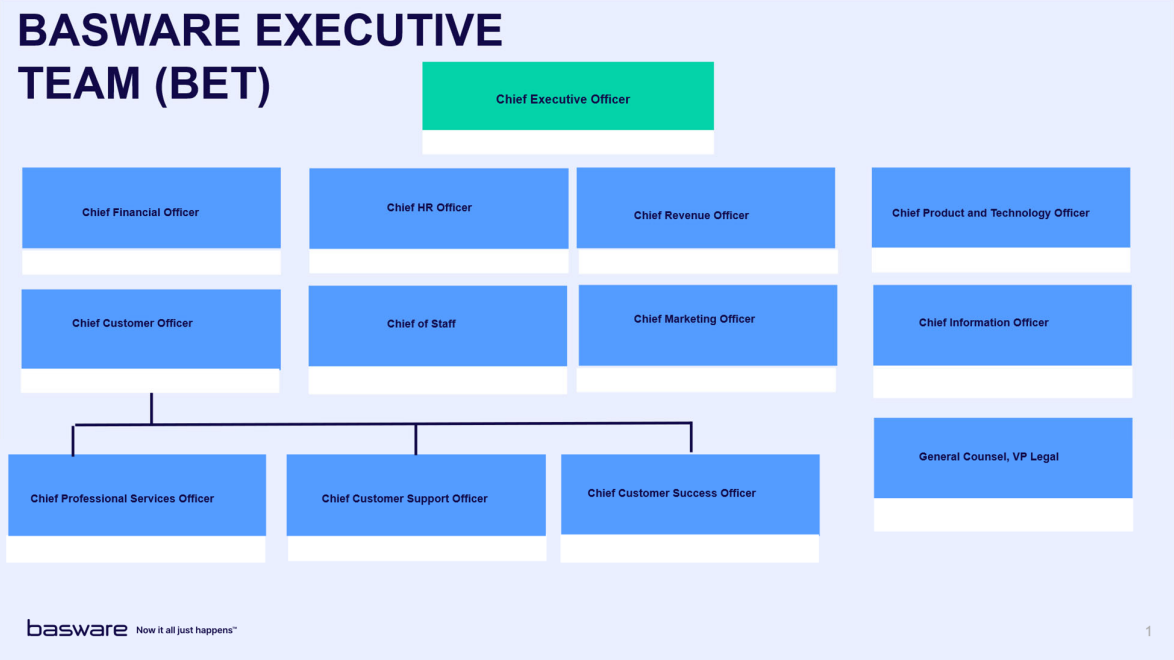
Firewall security deployed to filter traffic to and within the network and block unauthorized traffic is administered via AWS Security groups associated with cloud environment resources as well as Web Application Firewall (WAF) configurations. AWS GuardDuty is enabled to continuously monitors the infrastructure for malicious activity and alerting operations personnel.

Software

The software consists of the System and other software that supports the system such as customer portals, admin systems, and monitoring tools that are used for job scheduling, incident management, and user provisioning. Source code is managed in a Source Code Management (SCM) system with audit trails and version control.

People

The organizational structure of Basware provides the overall framework for planning, directing, controlling operations and achieving business objectives.



basware
Now it all just happens™

Key Information Security Management Roles and Responsibilities

Roles	Key Responsibilities
Basware Executive Team	1. Establish ISMS policies and integrate controls into processes. 2. Allocate resources and communicate security importance.
Security Steering Committee	1. Review and improve ISMS policies aligned with ISO/IEC 27001. 2. Monitor changes and legal obligations impacting security.
CISO	1. Define roles, responsibilities, and corporate security policies. 2. Oversee risk assessments and incident management.
DPO	1. Advise and monitor privacy obligations. 2. Ensure compliance with data protection regulations.
Legal	1. Define and monitor legal obligations for security and privacy. 2. Manage procurement of cyber insurance.
Technical Product Owner	1. Integrate security measures and risk assessments into projects. 2. Validate and monitor security throughout project lifecycle.
All employees	1. Following policies, processes, and instructions provided by Basware on information security

Other Roles include Product Managers, DevOps, QA, Operations, Security Team, and Database Administrators. Segregation of duties is enforced for production access.

Change Advisory Board (CAB) oversees major changes and emergency deployments.

Procedures

Basware has implemented Quality and Information Security Management Systems and has documented all key procedures including but not limited to:

- Quality Steering
- Product Life Cycle Management
- Nonconformity Management
- Internal Audit
- Vendor Management
- Change Management

- Security Steering
- Security Incident Management
- Vulnerability Management
- Data Backup and Disaster Recovery

Data

Basware Network receives data from multiple inbound interfaces, primarily using HTTPS and SFTP protocols. All incoming data undergoes validation, and a comprehensive audit trail is automatically recorded to ensure full traceability throughout the entire business document lifecycle.

Document types processed include invoices and procurement documents, typically in XML and PDF formats.

1.4 Subservice Organizations

AWS (Amazon Web Services): Data center operations, long-term data storage, backup/recovery, network infrastructure.

Microsoft Azure: Data center operations, long-term data storage, backup/recovery, network infrastructure.

AWS hosting regions currently utilized for Basware Network include:

- EU-west-1 (Ireland, EU)

Azure hosting regions currently utilized for Basware Network include:

- Azure North Europe (Ireland, EU)

This report utilizes the carve-out approach to controls at AWS and Azure, so those controls or their testing are not included in this report, but they are reviewed by Basware via AWS/Azure SOC 1 and SOC 2 assurance reports.

1.5 System Boundaries

In Scope: Basware Network service, supporting infrastructure, and all processes related to business document and financial data management.

Out of Scope: Controls managed solely by AWS and Azure (physical access, network hardware).

1.6 Relevant Aspects of the Control Environment

Basware maintains a documented organizational structure with defined roles and responsibilities and has implemented an ISMS with supporting policies and process to ensure controls are effectively implemented. Basware maintains the following policies:

- Acceptable Use Policy;
- Information Classification and Handling Policy;
- Access Management Policy;
- Secure Development Policy;
- Vulnerability Management Policy;

- Cryptography and Key Management Policy;
- Supplier Adoption and Relationship Policy;
- Logging and Monitoring Policy; and
- Backup Policy.

Governance includes Security Steering Committee, CAB oversight for changes, and regular review of controls via internal and external audits.

Risk management practices include segregation of duties, least privilege access, data backup and disaster recovery, vulnerability management, security incident management and system monitoring.

1.7 Risk Assessment Process

Management is responsible for identifying information security risks that threaten achievement of the control activities and could affect the organization's ability to provide secure and reliable service to its users. The risk assessment occurs annually, or as business needs change, and covers identification, evaluation, treatment and monitoring.

1.8 Information and Communication

Documented processes and policies are available for all staff to access. Basware also completes onboarding and annual compliance training coverings subjects such as our code of conduct, privacy and information security awareness. Key operational meetings such as Security Steering Committee are documented and retained.

Changes are communicated via JIRA tickets, Confluence documentation, and formal sign-off procedures via various Change Advisory Boards.

Relevant information is communicated to customers through various channels, such as ServiceNow.

1.9 Monitoring of Controls

Basware monitors information security controls through a combination of technical, operational, and governance measures. This includes access controls and authentication via IAM logs and MFA enforcement, monitoring network and infrastructure through firewalls, IDS/IPS, and vulnerability scans, and ensuring application security with code scanning and API monitoring.

Data protection is maintained through encryption checks, DLP tools, and backup integrity validation, while endpoint security relies on EDR and patch compliance.

Threat detection and incident response are supported by SIEM systems, threat intelligence, and response metrics. Compliance is monitored through audits, incident management and vendor risk assessments.

1.10 Control Objectives

The control objectives and activities that assist in producing Basware's Network solution are described thoroughly in section 3, "Description of General Information Technology Controls and Application Controls". Controls are divided and presented in the following groups:

1. General Information Technology Controls:

- Access Management
- Change Management
- IT Operations
- Logical Security
- Software Development Lifecycle

2. Network Application Controls:
   - Processing of Business Documents
   - Monitoring & Incident / Problem Management of Transactions

DESCRIPTION OF CONTROLS

2.1 General Information Technology Controls

ITGC	Control	Control Objectives
Access Management	Access Control	Rules to physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.
Access Management	Identity management	The full life cycle of identities shall be managed.
Access Management	Authentication information	Allocation and management of authentication information shall be led by a management process, including advising personnel on appropriate handling of authentication information.
Access Management	Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access .
Access Management	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.
Access Management	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access .
Access Management	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access
Change Management	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.
IT Operations	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.

IT Operations	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.
IT Operations	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.
IT Operations	ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.
IT Operations	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.
IT Operations	Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.
Logical Security	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.
Logical Security	Networks security	Networks and network devices shall be secured, managed and led to protect information in systems and applications.
Software Development Lifecycle	Secure development life cycle	Rules for the secure development of software and systems shall be established and applied
Software Development Lifecycle	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.

2.2 Network Application Controls

SLA Reports

Control Objective 1: *Control provides reasonable assurance that SLA reports are available to contracted customers when required.*

Service level SLA reports can be requested by customers when required through ServiceNow.

DATA BACKUP

Control Objective 2: *Controls provide reasonable assurance that application, operating systems, files, and data are backed up on a scheduled basis and replicated to another location.*

ICT readiness is planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.

Business Continuity Strategies and recovery plans have been developed and assessed annually.

Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.

PROCESSING OF BUSINESS DOCUMENTS

Control Objective 3: *Controls provide reasonable assurance that Business Documents on the Basware Commerce Network are authorized, secured and recorded.*

Only known users / entities (user / organization / interop) provided documents can be routed in the Network. Non-authenticated senders or otherwise non-defined document flows will not be routed.

Access to Business Documents is secured by authentication mechanism to verify that the accessing user identity matches the user account. Customer users can only access Business Documents they are allowed to access (secured by an authorization mechanism).

Customer users can only access Business Documents they are allowed to access (secured by an authorization mechanism).

Every Business Document on the Basware Commerce Network is tracked and can be followed by the means of a unique identifier.

At any time, the status and history of the Business Document used for processing and error follow-up can be consulted.

At any time, the change history of a Business Document can be consulted.

Business Documents are stored for a predefined retention period at least.

MONITORING & INCIDENT / PROBLEM MANAGEMENT OF TRANSACTIONS

Control Objective 4: *Controls provide reasonable assurance that message processing is monitored and related customer incidents are resolved in a timely manner*

Actions that relate to the resolution of customer incident tickets are registered in the ticketing system. All incident tickets are tracked and followed-up until closure. All messages are monitored on error states and customers are appropriately notified. All manual status adjustments to a message are performed by authorized personnel only.

PROCESSING AND PROBLEM MANAGEMENT

Control Objective 5*: Controls provide reasonable assurance that processing is appropriately authorized and scheduled, that deviations from scheduled processing are identified and resolved, and that problems and errors are recorded, analyzed, and resolved.*

A service level agreement (SLA) exists between service organization and its users. Company reports performance against the SLA.

The job scheduling system is used to schedule and complete production processing jobs. Job schedules are defined for processing cycles. Jobs are monitored to help ensure jobs process

completely and timely. Incident tickets are issued as needed to track resolution. Incident controllers approve the closure of incidents.

Access to add, modify, or delete job schedules is restricted to authorized personnel.

Computer operations management monitors operator activity through automatic threshold alerts.

The production environment is monitored by operations for incidents and failures. Operations personnel open a production environment incident ticket for any incident or failure. Incident tickets are assigned and prioritized. Assigned personnel analyze, resolve, and document the resolution of the problem within the ticket.

2.3 Complementary User Entity Controls

Basware's controls were designed with the assumption that certain internal controls would be implemented by the user entity. The application of such internal controls by the user entity is necessary to achieve the control objectives specified by Basware. There may be additional control objectives and related controls at the user entity that would be appropriate for the relevant processes that are not identified in this report. There may also be other controls, possibly conflicting with controls identified in this report, that have been agreed upon between Basware and the customer (user entity), that are excluded from this report.

This section describes certain controls that the customer should consider for the achievement of control objectives identified in this report. Customer auditors should consider whether the following internal controls are implemented and operating effectively. The customer control considerations presented below should not be regarded as a comprehensive list of all controls that should be employed by customer organisations.

Network Application Controls

A. Controls provide reasonable assurance that logical access to critical systems and applications is restricted to authorized personnel.

- Customers are responsible for establishing appropriate controls over the appropriate use and management of their user's accounts and passwords.

B. Controls provide reasonable assurance that Business Documents on the Basware Commerce Network are authorized, secured and recorded.

- Customers are responsible for establishing appropriate controls to ensure that data inputted to Basware Network solution is complete and accurate in terms of content. Basware does not inspect the quality and accurateness of the data inputted by customers.
- All application level field settings, including mandatory field checks, the duplicate prevention feature, tolerances and validation rules must be configured / enabled / approved by the customer. Any variances within the data between Basware Network solutions and customer ERP systems must be investigated and resolved by the customer.
- The customer shall agree upon with Basware on the transfer of responsibility for data to be transferred to or from the customer.
- In Basware Portal customers can set the retention period for their own documents. If not configured, the baseline for retention is 90 days.

General CUEC's

- Customers must manage their own user accounts and passwords
- Customers must comply with the Basware Technical Requirements

2.4 Significant Changes to the System

There were no significant changes during the reporting period that would likely affect users' understanding of the system's operational effectiveness or service delivery.

SECTION FOUR

OVERVIEW OF CONTROL OBJECTIVES, RELATED CONTROLS, AND TESTS OF OPERATING EFFECTIVENESS

Our tests of the effectiveness of controls have included such tests that are considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, are sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the defined period. Our tests of the operational effectiveness of the controls were designed to cover a representative number of events throughout the defined test period, for controls listed in Section Three, which are designed to achieve the specified control objectives. In selecting particular tests of operational effectiveness of controls, we have considered:

- the nature of the items to be tested
- available evidential material
- the nature of the objectives to be achieved
- the assessed level of control risk

NETWORK GENERAL INFORMATION TECHNOLOGY CONTROLS & NETWORK APPLICATION CONTROLS

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
Control Objective 1	***Control provides reasonable assurance that SLA reports are available to contracted customers when required.***			
2.2.3	Service level SLA reports are requested by customers when required through ServiceNow.	Auditors inquired from management about SLA reports. Auditors inspected SLA reporting statistics from ServiceNow and Basware's internal guidance regarding how SLA reports can be generated and how SLA requests are handled. Auditors inspected examples of ServiceNow tickets where a customer requested an SLA report and Basware provided to the customer in a timely manner.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
Control Objective 2	***Controls provide reasonable assurance that application, operating systems, files, and data are backed up on a scheduled basis and replicated to another location.***			
1.4.9	Business Continuity Strategies and recovery plans have been developed and assessed annually.	Auditors observed that there is a page for Disaster Recovery 2025 plans in Confluence. Auditors noted that it has been planned and defined which systems are in scope. Auditors learned through inquiry and inspection that Basware annually evaluates which systems will undergo a disaster recovery exercise based on factors such as recent architectural changes, risk profile, and business impact. Auditors also inspected a report confirming that a restore test was performed in September 2025 for Basware Network service module Gateway (GW). It was noted from the report that the system restoration to operational status was completed successfully and well within the RPO and RTO targets.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
5.30	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Auditors inspected that Basware has a corporate level Business Continuity Plan that has been published in the intranet. Auditors observed that Business Continuity Management guidelines and information is documented in Confluence. More detailed business continuity planning and testing of customer facing services is being carried out at business unit level. Inspected the disaster recovery project plan and IT disaster recovery management documentation for Network to determine that the disaster recovery plans are developed, maintained up to date and regularly tested. Inspected that the disaster recovery testing results report to determine that regular disaster recovery testing is performed and the results are analysed to further develop the DRPs. It was noted that based on the annual cycle, the latest testing was performed in Q4 2024, and the plans for testing in Q5 2025 have been designed.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.13	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Auditors inspected Jira tickets and noted that in 2025 Basware has performed backup management specification reviews, backup configuration audits, and backup alert audits also for the Basware Network service. Auditors also inspected a report confirming that a restore test was performed in September 2025 for Basware Network service module Gateway (GW). It was noted from the report that the system restoration to operational status was completed successfully and well within the RPO and RTO targets.	No exceptions noted.	
Control Objective 3	***Controls provide reasonable assurance that Business Documents on the Basware Commerce Network are authorized, secured and recorded.***			
2.1.1	Only known users/entities (user/ organization/interop) provided / defined documents can be routed in the Network. Non-authenticated senders or otherwise non-defined document flows will not be routed.	Auditors inspected Basware system architecture documentation, technical documentation for API and privilege model and flow to determine that there are procedures in place to restrict routing in the Network to allow only authenticated users and entities and defined document flows.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
2.1.2	Access to Business Documents is secured by authentication mechanism to verify that the accessing user identity matches the user account.	Auditors inspected technical documentation describing the architecture and authentication mechanisms to determine that the technological controls are implemented to verify the identity of accessing users. Auditors inspected configurations and log records from the attestation period to determine that technological controls have been operating as expected to verify that the user identity matches the user account.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
2.1.3	Customer users can only access Business Documents they are allowed to access (secured by an authorization mechanism).	Auditors inspected technical documentation describing the privilege model and flow in place to determine that the mechanisms are implemented to restrict user access according to their authorizations. Auditors re-performed negative testing with the control owner to determine that document access is restricted for unauthorized users.	No exceptions noted.	
2.1.4	Every Business Document on the BCN is tracked and can be followed by the means of a unique identifier.	Auditors inspected the technical documentation for Basware Unique Message ID (BUM-ID) to determine that mechanisms are in place to track business documents by assigning a unique identifier to each logical instance of a Business Document. Inspected a selection of business document instances to determine that unique identifiers were in place and documents on the Basware Network can be followed with the unique identifier.	No exceptions noted.	
2.1.5	At any time, the status and history of the Business Document used for processing and error follow-up can be consulted.	Auditors inspected technical documentation for the BT message history, including state diagram, and a selection of logs generated during the attestation period to determine that functionality is implemented to trace the status and history of business documents, including error state.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
2.1.6	At any time, the change history of a Business Document can be consulted.	Auditors observed that a functionality is in place through which the change history of a Business Document can be consulted. Inspected technical documentation for the message history and data retention, removal and archiving to determine that functionality is implemented to record and retain the change history of business documents. Inspected a selection of system logs generated during the attestation period to determine that change history of the business documents has been recorded.	No exceptions noted.	
2.1.7	Business Documents are stored for a predefined retention period at least.	Auditors inspected that retention periods for business documents are defined, and the documents are retained for the predefined retention period at least. Auditors observed lifecycle rules in the cloud hosting environment to determine that configurations are implemented to store Business Documents for the predefined retention period.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
Control Objective 4	**Controls provide reasonable assurance that message processing is monitored and related customer incidents are resolved in a timely manner**			
2.2.1	Actions that relate to the resolution of incident tickets are registered in the ticketing system.	Auditors tested with a selection that actions related to incident resolutions are registered in the ticketing system. For the selection, auditors also inspected that corrective actions and resolution methods have been documented in the corresponding incident tickets.	No exceptions noted.	
2.2.2	All incident tickets are tracked and followed-up until closure.	Auditors inspected that a process is established for tracking and following up on the incident tickets. Auditors also tested with a selection that incident tickets are tracked and followed up until closure in accordance with the process.	No exceptions noted.	
2.2.4	All messages are monitored on error states and customers are appropriately notified.	Auditors inspected technical documentation describing message history and states implementation to determine that a functionality is implemented to continuously monitor message statuses. Auditors inspected a selection of logs and investigation records to determine that processing statuses are monitored and error states are investigated in accordance with the established process.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
2.2.6	All manual status adjustments to a message are performed by authorized personnel only.	Auditors learned through inquiry and observation that relevant user roles and their features have been documented and that there is a list of current and expired users. Auditors observed from the system that strong access rights are required to manually adjust message statuses.	No exceptions noted.	
Control Objective 5	***Controls provide reasonable assurance that processing is appropriately authorized and scheduled, that deviations from scheduled processing are identified and resolved, and that problems and errors are recorded, analysed, and resolved.***			
1.5.1	The job scheduling system is used to schedule and complete production processing jobs. Job schedules are defined for processing cycles. Jobs are monitored to help ensure jobs process completely and timely. Incident tickets are issued as needed to track resolution. Incident controllers approve the closure of incidents.	Auditors inspected that jobs are monitored to help ensure jobs process completely and timely. Auditors also inspected that incident tickets are created for failed or incomplete jobs. Auditors inspected that the incidents and related activities are documented and tracked in the ticketing system. Auditors tested with a selection that incidents have been handled according to priority and in a timely manner.	For some of the inspected tickets, it was noted that incident resolution time was not in accordance with the SLA / OLA, and in two cases significantly deviated from the set resolution goal. The tickets did not sufficiently document the details, such as updates on	We acknowledge the auditor's observation that certain incident tickets within our system were not resolved within expected timelines and, in some cases, lacked regular updates. The primary reason for this is that our prioritization framework places critical focus on customer-facing issues, including widespread service disruptions and degradations, as well as urgent customer-impacting cases.

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
			planned and implemented actions and justification for the delay in resolution.	In contrast, the types of incidents noted in the finding – such as cases involving incomplete or missing notification addresses – are classified as lower priority, as they do not pose an immediate or material impact to customer operations. As a result, these tickets may remain open for longer periods and may not receive the same level of update frequency as higher-priority cases. That said, we recognize the importance of improving consistency and timeliness in managing these customer-specific internal incidents. Basware's Customer Experience Leadership Team is actively working on a plan, to enhance processes and resource allocation in order to strengthen control over such tickets. This initiative

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
				will take time to implement fully, but it reflects our commitment to continuous improvement and maintaining strong operational practices. We can confirm all outstanding tickets have now been closed.
1.5.2	Access to add, modify, or delete job schedules is restricted to authorized personnel.	Inspected access management procedures and system access processes for key systems, including BT, Gateway, ONP and Cloudscan to determine that relevant procedures are established to govern the job scheduler access rights. Inspected technical documentation and access matrices for key systems and observed access configurations from production environments and Active Directory user groups to determine that access rights to add, modify or delete scheduled jobs are restricted to authorized personnel.	No exceptions noted.	

1.5.3	The production environment is monitored by operations for incidents and failures. Operations personnel open a production environment incident ticket for any incident or failure. Incident tickets are assigned and prioritized. Assigned personnel analyse, resolve, and document the resolution of the problem within the ticket.	Audits inspected that there are formal monitoring process description and related instructions and observed that there are specific tools and systems being used for monitoring the production environment. Auditors inquired from the control owner and learned that a formal incident management process has been implemented. Auditors observed that the incident management process has been defined and documented. Auditors inspected that the incidents and related activities are documented and tracked in the ticketing system. Auditors tested with a selection that incidents have been handled according to priority and resolved in a timely manner.	For some of the inspected tickets, it was noted that incident resolution time was not in accordance with the SLA / OLA, and in two cases significantly deviated from the set resolution goal. The tickets did not sufficiently document the details, such as updates on planned and implemented actions and justification for the delay in resolution.	We acknowledge the auditor's observation that certain incident tickets within our system were not resolved within expected timelines and, in some cases, lacked regular updates. The primary reason for this is that our prioritization framework places critical focus on customer-facing issues, including widespread service disruptions and degradations, as well as urgent customer-impacting cases. In contrast, the types of incidents noted in the finding – such as cases involving incomplete or missing notification addresses – are classified as lower priority, as they do not pose an immediate or material impact to customer operations. As a result, these tickets may remain open for longer periods and may not receive the same level of

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
				update frequency as higher-priority cases. That said, we recognize the importance of improving consistency and timeliness in managing these customer-specific internal incidents. Basware's Customer Experience Leadership Team is actively working on a plan, to enhance processes and resource allocation in order to strengthen control over such tickets. This initiative will take time to implement fully, but it reflects our commitment to continuous improvement and maintaining strong operational practices. We can confirm all outstanding tickets have now been closed.

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
1.5.4	Computer operations management monitors operator activity through automatic threshold alerts.	Auditors observed from Dynatrace that there are several automatic thresholds configured that will raise an alert in case exceeded. Auditors also inspected example dashboards and alerts from Splunk that prove that there are automatic thresholds which when exceeded cause alerts that are raised to the monitoring team.	No exceptions noted.	
1.5.5	A service level agreement (SLA) exists between (service organization) and its users. Performance is measured against the SLA.	Auditors inspected a selection of service level agreements between Basware and its users. Auditors also inspected that performance of Network solution is measured against the SLA by the responsible personnel using defined KPIs.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
Control objective 6	***Controls provide reasonable assurance that access to systems and data are properly limited and managed.***			
5.15	Rules to physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	Auditors inspected Access Management policy and process description and noted that rules to physical and logical access to information and other associated assets is established and implemented based on business and information security requirements. Auditors also inspected Access Revoking process. Inspected a selection of access right tickets regarding solutions in scope to note that granting access was based on a business role.	No exceptions noted.	
5.16	The full life cycle of identities shall be managed.	Auditors inspected Access management documentation and processes for account creation, account termination and mover processes to note that the full life cycle of identities are managed. Granted access rights were inspected in control 5.17 as a sample. Inspected a selection of resigned employees to note that identities life cycle is fully managed.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
5.17	Allocation and management of authentication information shall be led by a management process, including advising personnel on appropriate handling of authentication information.	Auditors inspected Access Management documentation and processes for account creation and termination to note that allocation and management of authentication information is led by a management process, including advising personnel on appropriate handling of authentication information. It was noted that a policy regarding passwords was approved during audit period. Inspected a selection of access right tickets regarding solutions in scope to note that they follow the process.	No exceptions noted.	
5.18	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access.	Auditors inspected the access management and password policies to note rules for access. Also inspected that user access right review was done during audit period for each solution in scope, to note that access rights are provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.2	The allocation and use of privileged access rights shall be restricted and managed.	Auditors inspected that the allocation and use of privileged access rights are restricted and managed according to access management policy. Inspected a selection of users with privileged access rights for solutions in scope to note that privileged access rights are restricted and managed. It was noted that Cloudscan team members have privileged access rights into Azure, which are required to maintain the production environment. For other solutions in scope a selection of authorizers, who can grant access when needed, were inspected as a sample.	No exceptions noted.	
8.3	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access.	Auditors inspected access profiles, which defined roles that are assigned to users based on their job function (role-based security) and noted that these are implemented to restrict access to information and other associated assets. For solutions in scope, inspected a selection of access right tickets to note that access was granted based on job role.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.5	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access.	Auditors inspected the access management policy and process description to note that secure authentication technologies and procedures are implemented. Inspected a selection of employees to note that MFA was active for users.	No exceptions noted.	
8.8	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	Auditors observed from Confluence that the process for vulnerability management is formally defined and appropriately documented. Through inquiry and inspection, auditors learned that tools such as Snyk and Tenable are utilized for scanning and identifying various vulnerabilities. Auditors noted that Jira is used for documenting and managing vulnerabilities. Auditors tested with a sample that vulnerabilities have been documented and resolved appropriately. Additionally, auditors found that Key Performance Indicators (KPIs) for vulnerabilities are in place. Auditors observed that these security KPIs are reported to the CIO and the Board of Directors.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.20	Networks and network devices shall be secured, managed and led to protect information in systems and applications.	Auditors inspected technical documentation for key system components, including Gateway, BT and ONP architecture to determine that relevant security requirements and baseline configurations are defined and documented. Observed security groups policies implemented for key system components, including Gateway, BT and ONP to determine that network security configurations are implemented as designed and operated accordingly during the attestation period. For Cloudscan, auditors inspected the Cloudscan architecture documentation, Azure portal settings and disaster and recovery documentation to note that networks and network devices are secured, managed and led to protect information in systems and applications. It was noted that Cloudscan environment is secured with BW SSO authentication and user rights are granted by product manager or product architect.	No exceptions noted.	We acknowledge the auditor's observation that the penetration testing procedure was not up to date. This was because the procedure was being updated and there was a delay in publishing the final version as it was still being reviewed ahead of final approval. It has now been finalized, approved, and published.

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
Control Objective 7	***Controls provide reasonable assurance that changes to systems are properly managed and implemented***			
8.25	Rules for the secure development of software and systems shall be established and applied.	Inspected the approach to secure software development, vulnerability management process and external pentesting process adopted by the organization. For a selection of vulnerabilities identified during the testing period, inspected that vulnerability identification, analysis and resolution followed the established process, and identified vulnerabilities were resolved in a timely manner.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.29	Security testing processes shall be defined and implemented in the development life cycle.	Auditors inspected organization's vulnerability management process to determine that procedures are established for security testing and vulnerability management. Auditors inspected external penetration testing process and reports to determine that procedures are established for independent security testing and penetration testing has been performed regularly. It was noted that the penetration testing process description was not up to date. Auditors inspected that Basware subsequently updated the process during the attestation period. For a selection of vulnerabilities identified during the attestation period, auditors inspected that the vulnerability management process was followed accordingly, and fixes were implemented as required.	It was noted that the penetration testing process description was not up to date during the attestation period.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.32	Changes to information processing facilities and information systems shall be subject to change management procedures.	Inspected the organization's life cycle management process, development process, product release process and production change authorization process. For a selection of releases published within the attestation period, inspected release documentation, including CAB meeting notes and all tasks in each selected release, to determine that change management followed the standard release and approval procedures.	No exceptions noted.	
Control Objective 8	***Controls provide reasonable assurance that systems are properly monitored and incidents are analyzed and resolved***			
5.24	The organization shall plan and prepare for managing information secu-rity incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Auditors observed that Basware has a defined information security incident management process, which includes relevant activities, roles and responsibilities, communication instruction and key contacts. Auditors observed that bi-weekly calls are organized to review open incidents and to communicate any process or responsibility changes.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
5.26	Information security incidents shall be responded to in accordance with the documented procedures.	Auditors inquired from management about security incidents that have occurred in 2025 and about the organization's response to these incidents. Auditors observed that there is a dedicated Confluence page for all reported information security incidents. Auditors tested with a sample that information security incidents have been responded to in accordance with the documented procedures.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
5.29	The organization shall plan how to maintain information security at an appropriate level during disruption.	Auditors inspected that Basware has a corporate-level Business Continuity Plan which includes reference to Information Security and the involvement of the Security Team in any disruptive event. Auditors also observed that the Security Incident Management process has been defined and documented in Confluence with reference to business continuity. Auditors inspected the disaster recovery project plan and IT disaster recovery management documentation for Network to determine that the disaster recovery plans are developed, maintained up to date and regularly tested. Inspected that the disaster recovery testing results report to determine that regular disaster recovery testing is performed and the results are analysed to further develop the DRPs. It was noted that based on the annual cycle, the latest testing was performed in Q4 2024, and the plans for testing in Q4 2025 have been designed.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.6	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Inspected the documentation and capacity predictions and noted that the use of resources is being monitored and adjusted in line with current and expected capacity requirements. According to the control owner volumes are predicted for future year, and they are estimated by financial department annually. Inspected capacity predictions for the next year from annual report to note that capacity is predicted.	No exceptions noted.	