basware
Now it all just happens™

Basware Corporation

BASWARE AP AUTOMATION 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 3
INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT 4

SECTION TWO 7
STATEMENT BY THE SERVICE ORGANISATION 8

SECTION THREE 10
DESCRIPTION OF SERVICES PROVIDED BY BASWARE 11
1.1 Overview of the Service Organization and the Services Provided 11
1.2 Principal Service Commitments and System Requirements 11
1.3 Components of the System 11
1.4 Subservice Organizations 14
1.5 System Boundaries 14
1.6 Relevant Aspects of the Control Environment 14
1.7 Risk Assessment Process 15
1.8 Information And Communication 15
1.9 Monitoring Of Controls 15
1.10 Control Objectives 15
DESCRIPTION OF CONTROLS 16
2.1 General Information Technology Controls 16
2.2 AP Automation Application Controls 17
2.2.1 Master Data Management 17
2.2.2 Invoice Processing 18
2.2.3 Automatic Matching Process 18
2.2.4 Processing and Problem Management 19
2.3 Complimentary User Control Considerations 19
2.4 Significant Changes To The System 20

SECTION FOUR 21
OVERVIEW OF CONTROL OBJECTIVES, RELATED CONTROLS, AND TESTS OF OPERATING EFFECTIVENESS 22

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 AP Automation solution (hereinafter also "AP Automation") 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 Amazon Web Services (AWS, subservice organization) to provide cloud infrastructure services for its AP Automation 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 AP Automation 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 AP Automation 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 AP Automation 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 AP Automation 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 Amazon 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 AP Automation 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

iii) 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 AP Automation services ("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

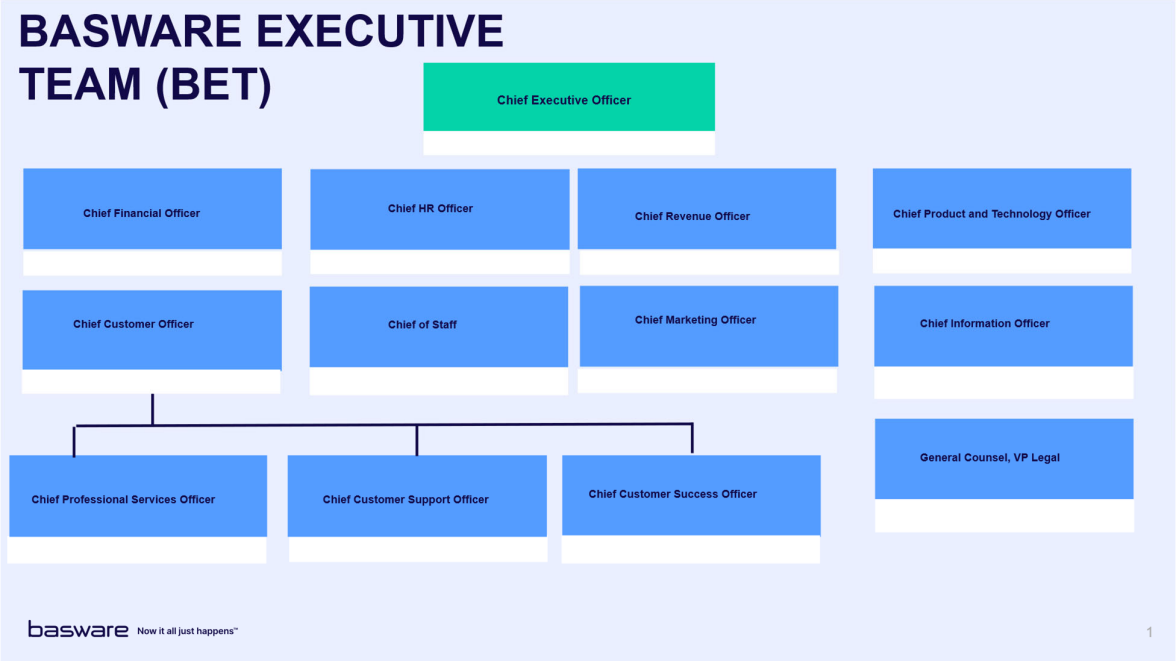
Firewall security deployed to filter traffic to and within the network and block unauthorized traffic is administered via AWS Security groups associated with cloud environment resources as well as Web Application Firewall (WAF) configurations. AWS GuardDuty is enabled to continuously monitor the infrastructure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

Software

Core applications include AP Automation Core, Baselines, and Deployment Baselines. Source code is managed in a Source Code Management (SCM) system with audit trails and version control. Customer portals, admin systems, and monitoring tools are used for job scheduling, incident management, and user provisioning.

People

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



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

Data flows from customer ERP systems into AP Automation via inbound interfaces, with validation and audit trails for all changes.

Types of data processed: invoices, master/basic data (e.g., general ledger codes, cost centers, suppliers, employees), purchase orders, and goods receipts.

1.4 Subservice Organizations

AWS (Amazon Web Services): Provides hosting, physical security, backup/recovery, and network infrastructure.

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

AWS hosting regions currently utilized by Basware for AP Automation system include:

- EU-west-1 (Ireland, EU)
- AP-southeast-2 (Australia, AP)
- US-west-2 (Oregon, US)
- CA-central-1 (Canada, Central)

1.5 System Boundaries

In Scope: AP Automation service, supporting infrastructure, and all processes related to invoice and master data management.

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

Limitations: Customer responsibilities for certain controls (e.g., user access management, invoice validation) are outside Basware's scope.

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:

- Information Security Policy;
- 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;
- Password Policy;
- Clear office 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 AP Automation System are described below. 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. AP Automation Application Controls:
    1. Master Data Management
    2. Invoice Processing
    3. Automatic Matching Process
    4. Processing and Problem Management

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	Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorized as information security incidents.
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 AP Automation Application Controls

2.2.1 Master Data Management

Control Objective 1: *Controls provide reasonable assurance that modification of customer's Master/basic data is authorized and set up completely and accurately.*

Master/Basic data (such as general ledger codes, cost centers, employees, and suppliers) is imported from the customer ERP system into AP Automation via inbound interface provided by Basware's AnyERP system. Import /export job completion is monitored, and incidents tickets are opened for failed or incomplete jobs, according to Basware Incident management process.

There are number of basic data items which requires a unique ID (for example supplier ID) Duplicate ID's are not allowed, and result into failed import or preventing the creation. Upon import or creation in Basware AP Automation a duplicate check will be performed preventing double entries.

Data validations are in place to control the input. Certain fields are set as mandatory, e.g. vendor number, and some fields have an active content validation, e.g. email address.

Ability to set up basic/master data is segregated from the purchasing and accounts payable function. Creation vendor numbers require separate user access to AP Automation Administration. Duties between AP Automation administrator and purchase or accounts payable functional are segregated.

The report of all changes to basic / master data can be generated from the system for auditing purposes. The direct changes have an audit trail to the user initiating the change, and the actual old and new value. Also all changes made in ERP system data, which is transferred to AP Automation are recorded in the history as a change.

2.2.2 Invoice Processing

Control Objective 2: *Controls provide reasonable assurance that invoices are recorded completely and accurately, and invoices are authorized prior to being processed.*

Configuration supports field settings, e.g. mandatory fields. Mandatory fields are required to ensure that invoice data is input completely and accurately. Mandatory fields cannot be empty and data in the fields must be valid against lookup lists (list validation). Data input validation, business rule validation for whole invoice data and additional validations for invoice coding rows. List validation using lookup lists.

All invoices in Basware Invoice are automatically validated against standard rules. If the invoice organization does not match with a valid organization in Basware Invoice organization structure (company, business unit, group), the invoice will be rejected. If the system cannot find a valid process for the invoice, the invoice gets a Ddraft" status and must be updated and re-validated before it can be sent to the process

A full audit trail of all activities from purchase request creation to payment gets built. The information cannot be modified in Basware AP Automation user interface. Only Basware database admins have other than read only access to history information.

The system automatically prevents duplicate invoices. As a default a duplicate invoice identification is based on the company code, supplier number and invoice number. (Also additional identification factors may be configured.)

Standard invoice process requires an invoice approval either through a manual workflow or automatic matching process. Invoices are approved by an appropriate level of management. Approval workflow requires that each invoice must be reviewed and approved by a separate person.

As a default AP Automation application ensures that the invoice is fully coded before the review task can be completed. (Total coding sum = total invoice sum).

Once the final approval has completed the invoice data cannot be modified.

The Invoice and its coding data are transferred to an ERP system for payment after the final approval. If an invoice will be transferred manually separate user rights are required for transfer actions.

2.2.3 Automatic Matching Process

Control Objective 3: *Controls provide reasonable assurance that during the automated matching process all invoices (and other business documents) are recorded completely and approved prior to being processed.*

The system has been configured to perform automatic matching of the invoice, receipt and purchase order. In matching, a purchase order, purchase order line, or a goods receipt is linked to an invoice or invoice line. Any document without this linkage will fail in the import, and therefore not available for automatic matching.

Purchase order import template requires mandatory fields to ensure complete and accurate goods receipts. Goods receipts require a link to organization unit, purchase order, purchase order row and quantity. Goods receipts without this linkage will fail in the import, and therefore not available for automatic matching.

Invoices are sent to automatic matching once the invoice has been successfully validated. If one or more of the validation rules fails, the document must be linked to other documents manually. The failed document is listed in an "error report".

The system generates invoice coding for all invoices that were sent from the association phase to the matching validation phase. Coding is based on the information of purchase order.

The system generates an error report of invoices which have not been successfully matched by automatic matching. The report includes also a system generated description of error occasions.

2.2.4 Processing and Problem Management

Control Objective 4: *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.*

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.

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 Complimentary User Control Considerations

Basware's controls were designed with the assumption that certain internal controls would be implemented by the customer. The application of such internal controls by customer is necessary to achieve the control objectives specified by Basware. There may be additional control objectives and related controls at customer organisations 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, 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.

AP Automation Application Controls:

A. Controls provide reasonable assurance that modification of customer's Master/basic data is authorized and set up completely and accurately.
    - The customer shall agree upon with Basware on the transfer of responsibility for data to be transferred to or from the customer.
    - It was ensured during the audit that Basware has process and reasonable controls in place for detecting technical malfunctions in their systems. However, the Customer is responsible for accounts payable process, and therefore for detecting invoices that have not been transferred correctly.
B. Controls provide reasonable assurance that invoices are recorded completely and accurately and invoices are authorized prior to being processed.

- All application level field settings, including mandatory field checks, the duplicate prevention feature, tolerances and validation rules must be configured, enabled and approved by the customer. Any variances within the data between AP Automation and customer ERP systems must be investigated and resolved by the customer

C. Controls provide reasonable assurance that during the automated matching process all invoices (and other business documents) are recorded completely and approved by prior to being processed.

- To enable the automatic invoice workflow, the customer is responsible for delivering the purchase order data according to the Basware AP Automation system standard. The Customer is responsible for goods receipt entries in their ERP system
- Matching validation and invoice coding rules are maintained and approved by the customer in the AP Automation system
- All invoices in the error report require manual action by the customer. Basware is responsible for incident management procedures if the application operating incorrectly and customer has reported the issue to Basware Helpdesk
- The discount policy and payment terms are typically transferred from the customer ERP system. This information however may be configured and automatically calculated within the AP Automation system also. If the payment term or discount policy is changed in AP Automation system, the customer should implement compensative controls to reconcile the difference between ERP and AP Automation. The AP Automation system is built in a way that the customer may restrict access to payment terms and discount policy modification for authorized users only.

General CUEC's

- Customers must configure and approve application-level field settings, validation rules, and duplicate prevention features.
- Customers are responsible for user access management for their own users, including appropriate segregation of duties.
- Customers must deliver master data according to Basware standards
- 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

AP AUTOMATION GENERAL INFORMATION TECHNOLOGY CONTROLS & 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	***Controls provide reasonable assurance that modification of customer's Master/basic data is authorized and set up completely and accurately.***			
2.1.1	Master/Basic data (such as general ledger codes, cost centers, employees, and suppliers) is imported from the customer ERP system into the AP Automation via inbound interface provided by Basware's AnyERP system. Import /export job completion is monitored, and incidents tickets are opened for failed or incomplete jobs, according to Basware Incident management process.	Auditors inspected the process to import data from the customer's solution to the Basware environment. Auditors also inspected that the import and export jobs were monitored and that the incident tickets were opened when deficiencies were identified during the job processing.	No exceptions noted.	
2.1.2	There are number of basic data items which requires a unique ID (for example supplier ID) Duplicate ID's are not allowed, and result into failed import or preventing the creation. Upon import or creation in Basware AP Automation a duplicate check will be performed preventing double entries.	Auditors inspected that unique IDs were required for basic data items in the application. Auditors also inspected that duplicate ID cannot be created in the application as an automated duplication check was configured to prevent double entries.	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	Data validations are in place to control the input. Certain fields are set as mandatory, e.g. vendor number, and some fields have an active content validation, e.g. email address.	Auditors inquired from the control owner about the design of the control. Auditors observed that automated data validation configurations were implemented. Auditors also observed that mandatory fields were configured to ensure these fields would be filled prior to the import of new data.	No exceptions noted.	
2.1.4	Ability to set up basic/master data is segregated from the purchasing and accounts payable function. Creation vendor numbers require separate user access to AP Automation Administration. Duties between a AP Automation administrator and purchase or accounts payable functional are segregated.	Auditors inspected that segregation of duties was implemented in the application to ensure all administrative functions are limited to authorized personnel granted super user rights in the application.	No exceptions noted.	
2.1.5	The report of all changes to basic / master data can be generated from the system for auditing purposes. The direct changes have an audit trail to the user initiating the change, and the actual old and new value. Also all changes made in ERP system data, which is transferred to AP Automation are recorded in the history as a change.	Auditors inspected that the solution generates history log that can be used as an audit trail for application data changes. Auditors also inspected that logs for all changes to the master / basic data can be reproduced from the system for auditing purposes.	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 invoices are recorded completely and accurately, and invoices are authorized prior to being processed.***			
2.2.1	Configuration supports field settings, e.g. mandatory fields. Mandatory fields are required to ensure that invoice data is input completely and accurately. Mandatory fields cannot be empty and data in the fields must be valid against lookup lists (List validation). Data input validation, business rule validation for whole invoice data and additional validations for invoice coding rows. List validation using lookup lists.	Auditors inspected that certain fields were set as mandatory fields to ensure that invoice data input is complete and accurate. Auditors also inspected that list, data input, and business rule validation configurations, and additional validation for invoice coding rows were implemented.	No exceptions noted.	
2.2.2	All invoices in Basware Invoice are automatically validated against standard rules. If the invoice organization does not match with a valid organization in Basware Invoice organization structure (company, business unit, group), the invoice will be rejected. If the system cannot find a valid process for the invoice, the invoice gets a "Draft" status and must be updated and re-validated before it can be sent to the process.	Auditors inspected that standard rules for invoice automated validation were implemented in the solution to ensure only validated data files can be transferred into the solution.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
2.2.3	A full audit trail of all activities from purchase request creation to payment gets built. The information cannot be modified in Basware AP Automation user interface. Only Basware database admins have other than read only access to history information.	Auditors inspected that the solution's internal log / history can be used as an audit trail for data modifications and other user activities. Auditors also inspected group access right configurations to conclude that only Basware database admins can modify internal log / history data.	No exceptions noted.	
2.2.4	The system automatically prevents duplicate invoices. As a default a duplicate invoice identification is based on the company code, supplier number and invoice number. (Also, additional identification factors may be configured).	Auditors inspected that there is an automated configuration for prevention of duplicate invoices. Auditors also inspected that all invoices were supplement with a unique identification number to ensure no duplicate invoices could be created.	No exceptions noted.	
2.2.5	Standard invoice process requires an invoice approval either through a manual workflow or automatic matching process. Invoices are approved by an appropriate level of management. Approval workflow requires that each invoice must be reviewed and approved by a separate person.	Auditors inspected that standard invoice process requires either manual workflow or automatic matching process for invoice approval. Auditors also inspected that in the solution, separate approval levels can be established for appropriate level of management based on the customer requirements. It was also inspected that approval workflows require an individual review and approval by a separate person for each invoice.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
2.2.7	As a default AP Automation application ensures that the invoice is fully coded before the review task can be completed. (Total coding sum = total invoice sum).	Auditors inspected configurations in the solution to conclude that the invoices require to be fully coded before the review tasks could be completed.	No exceptions noted.	
2.2.8	Once the final approval has completed the invoice data cannot be modified.	Auditors observed that processed invoices were protected, and invoice data cannot be modified without administrative access rights. Auditors also inspected that modifications done by the administrative users were logged in the application history.	No exceptions noted.	
2.2.9	The Invoice and its coding data are transferred to an ERP system for payment after the final approval. If an invoice will be transferred manually separate user rights are required for transfer actions.	Auditors observed that processed invoices were transferred to an ERP system for payment after final approval. Auditors also inspected that separate user rights are required to perform manual transfer of processed invoices.	No exceptions noted.	
Control Objective 3	***Controls provide reasonable assurance that during the automated matching process all invoices (and other business documents) are recorded completely and approved by prior to being processed.***			

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
2.3.1	The system has been configured to perform automatic matching of the invoice, receipt and purchase order. In matching, a purchase order, purchase order line, or a goods receipt is linked to an invoice or invoice line. Any document without this linkage will fail in the import, and therefore not available for automatic matching.	Auditors inspected that standard rules for invoice validation were implemented in the solution to ensure only automatically validated data files can be transferred into the application. Auditors also reviewed that automatic matching rules were established for invoices, receipts and purchase orders prior to the import and automatic matching process.	No exceptions noted.	
2.3.2	Purchase order import template requires mandatory fields to ensure complete and accurate goods receipts. Goods receipts require a link to organization unit, purchase order, purchase order row and quantity. Goods receipts without this linkage will fail in the import, and therefore not available for automatic matching.	Auditors observed that certain fields were set as mandatory fields to ensure that invoice data input is complete and accurate. Auditors also inspected that list, data input, and business rule validation configurations, and additional validation for invoice coding rows were implemented. Additionally, auditors inspected that goods receipts require additional information as mandatory field so that the data related to the receipts could be directed to the right linkages.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
2.3.3	Invoices are sent to automatic matching once the invoice has been successfully validated. If one or more of the validation rule fails, the document must be linked to other documents manually. The failed document is listed in an error report.	Auditors observed that after validation the invoices were sent to automatic matching process with automated configurations. Auditors also inspected that in cases where one or more of the validation rules failed, the invoices were processed only following the manual workflow procedures.	No exceptions noted.	
2.3.4	The system generates invoice coding for all invoices that were sent from the association phase to the matching validation phase. Coding is based on the information of purchase order.	Auditors observed that in the solution invoice coding was generated for all invoices prior to sending them to the matching validation phase.	No exceptions noted.	
2.3.5	The system generates an error report of invoices which have not been successfully matched by automatic matching. The report includes also a system generated description of an error occasions.	Auditors tested with a selection that error reports were generated for the invoices which were not validated with automatic matching. Auditors also inspected that the description of the error was included in the report automatically generated by the application.	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 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.***			
1.5.1	The job scheduling system is used to schedule and complete production processing jobs.	Auditors inspected technical documentation for the job scheduler to determine that the job scheduling system is implemented, and jobs are configured for production processing jobs. Inspected a selection of log records for production processing jobs generated during the attestation period to determine that job scheduler has been operational and completion of jobs is monitored.	No exceptions noted.	

1.5.2	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 job scheduling is in place to schedule and complete production processing jobs and that jobs are monitored to help ensure jobs process completely and timely. Auditors also inspected that incident tickets are opened 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 planned and implemented actions and justification for the delay in resolution. No other exceptions noted.	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 update frequency as higher-priority cases.

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
				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
1.5.3	Access to add, modify, or delete job schedules is restricted to authorized personnel.	Auditors inspected the identity and access management procedures to determine that relevant procedures are established to govern the job scheduler access rights. Inspected access rights to a selection of automated processing job types to determine that access rights to modify or delete scheduled jobs are restricted to authorized personnel.	No exceptions noted.	

1.5.4	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.	Auditors inquired from the control owner and learned that a formal incident management process has been implemented. We 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 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 update frequency as higher-priority cases.

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
				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
Control Objective 5	***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 process, password policy and password guidance document to note that rules to physical and logical access to information and other associated assets is established and implemented based on business and information security requirements. Inspected technical documentation for identity and access management in AP Automation, including segregation of duties for potentially dangerous work combinations. During the walkthrough interview, observed system configurations live to determine that accesses are managed in accordance with the technical documentation description.	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. Inspected that identity management is done on the organizational level with Active Directory SSO, including for AP Automation.	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. Inquired of the control operator and noted that passwords are not configured on AP Automation level, as accesses are managed with Active Directory SSO.	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.	Inspected the access management policy and identity and access process to determine that relevant procedures are established. Inspected work instructions regarding SSO implementation. Inspected a selection of access requests from the ticketing portal managed during the attestation period to determine that in all cases appropriate approvals were obtained prior to granting access. Inspected that access revocation relies on SSO.	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 organization's procedure for access management, including privileged accesses. Inspected that access rights review for AP Automation has been performed in accordance with the procedure during the attestation period and privileged access rights were restricted to the authorized personnel.	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 the access management policy adopted by the organization. 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. Inspected technical documentation for identity and access management in AP Automation, including segregation of duties for potentially dangerous work combinations. During the walkthrough interview, observed system configurations to determine that accesses are managed in accordance with the technical documentation description.	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 technical documentation describing platform operations access management to determine that secure authentication principles, including password requirements, are defined. 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.	

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 changes to systems are properly managed and implemented.***			
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.	Inspected technical documentation for the AP Automation deployment model to determine that relevant security requirements and baseline configurations are defined and documented. Inspected the DevOps team security vulnerability exception process to determine that the process for managing identified vulnerabilities is established and documented. During the walkthrough interview, observed that the team uses a dedicated Kanban board to track and follow-up on activities related to exception and vulnerability management. For a selection of vulnerabilities identified during the testing period, inspected that the vulnerability management process was followed accordingly. In all inspected cases, vulnerabilities were prioritized, assigned a responsible person, analysed and resolution was documented. It was noted that fixes were implemented as relevant.	No exceptions noted.	

Control #	Control description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.25	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.	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 systems are properly monitored and incidents are analyzed and resolved.***			
5.24	The organization shall plan and prepare for managing information security 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.	
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. 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 developed.	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 AP Automation to determine that the disaster recovery plans are developed, maintained up to date and regularly tested. 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
8.6	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Inspected the organization's capacity management policy to determine that relevant procedures for capacity management are defined and documented. Inspected the capacity management process for AP Automation production environment to determine that relevant operational guidelines are defined, documented, and made available for the responsible personnel. Auditors inspected the documentation and capacity predictions and monitoring reports and noted that the use of resources is being monitored and adjusted in line with current and expected capacity requirements. It was noted that AP Automation has monthly meetings. Observed the capacity monitoring tools live during the interview with the control owner to determine that capacity monitoring is implemented as 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 for the AP Automation service. Auditors also inspected a report confirming that a restore test was performed in January 2025 for AP Automation successfully with no data loss encountered.	No exceptions noted.	
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.	