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 3000 REPORT

November 26th, 2025

CONTENTS

SECTION ONE

INDEPENDENT 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 based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, Description Criteria) and the suitability of the design of controls stated in the Description and their operating effectiveness throughout the period from January 1st, 2025 to September 30th, 2025 to provide reasonable assurance that Basware's service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (Trust Services Criteria).

Basware uses Amazon Web Services (AWS, subservice organization) and Microsoft Azure (Azure, subservice organization) to provide cloud infrastructure services for its Basware Network solution. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Basware, to achieve Basware's service commitments and system requirements based on applicable trust services criteria. The Description presents Basware's system, its controls relevant to applicable trust services criteria, and the types of complementary subservice organization controls that the service organization assumes have been implemented, suitably designed, and operating effectively. The Description does not disclose the actual controls at the subservice organization. Our procedures did not extend to the services provided by subservice organizations, and we did not evaluate whether the assumed controls have been implemented at subservice organizations or whether such controls were suitably designed and operating effectively.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Basware, to Basware's service commitments and system requirements based on the applicable trust services criteria. The Description presents Basware's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Basware's controls. Our engagement did not include such complementary user entity controls, and 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 its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that its service commitments and system requirements were achieved. Basware has provided the accompanying statement titled "Statement by the Service Organization" (statement) about the description and the suitability of the design of controls stated therein. Basware is also responsible for preparing the description and statement, including the completeness, accuracy, and method of presentation of the description and statement; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on Basware's description and on the design and operation of controls described therein to meet the applicable trust services criteria, based on our procedures.

We conducted our engagement in accordance with the International Standard on Assurance Engagements 3000, '*Assurance Engagements Other than Audits or Reviews of Historical Financial Information*' issued by the International Auditing and Assurance Board. The standard requires that we plan and perform our engagement to obtain reasonable assurance about whether, in all material respects, the Description is presented in accordance with the Description Criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

A reasonable assurance engagement to report on the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- obtaining an understanding of the system and the service organization's service commitments and system requirements;
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed;
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria if those controls operated effectively;
- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;
- evaluating the overall presentation of the description; and
- performing such other procedures as we considered necessary in the circumstances.

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 behaviour.

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.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that each individual report user may consider important to meet their informational needs.

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

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

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. In our opinion, in all material respects:

(a) The Description fairly presents the Description that was designed and implemented throughout the period from January 1st, 2025 to September 30th, 2025 in accordance with the Description criteria;

(b) The controls stated in the Description were suitably designed throughout the period from January 1st, 2025 to September 30th, 2025 to provide reasonable assurance that Basware's service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively throughout that period, and the subservice organizations and user entities applied the complementary controls assumed in the design of Basware's controls throughout the period from January 1st, 2025 to September 30th, 2025; and;

(c) The controls, stated in the Description operated effectively designed throughout the period from January 1st, 2025 to September 30th, 2025 to provide reasonable assurance that Basware's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls, assumed in the design of Basware's controls, operated effectively throughout the period January 1st, 2025 to September 30th, 2025.

Restricted use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Basware and user entities of Basware's Network solution during some or all of the period January 1st, 2025 to September 30th, 2025, who have sufficient knowledge and understanding of the following:

- the nature of the service provided by the service organization;
- how the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- internal control and its limitations;
- complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements;

- user entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- the applicable trust services criteria; and
- the risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

Helsinki, on November 26th, 2025

KPMG Oy Ab

DocuSigned by:
2477B01D945A425...

Jussi Paski
Partner
Authorized Public Accountant

DocuSigned by:
BB057897E9F64C0...

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 Network solution as designed and implemented throughout the period January 1st, 2025 to September 30th, 2025 in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (description criteria). The description is intended to provide users of the system and their auditors and service providers information that may be useful when assessing the risks arising from interactions with the system throughout the period January 1st, 2025 to September 30th, 2025, particularly information about the system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Basware uses carved-out 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 subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Basware, to achieve Basware's services commitments and system requirements based on applicable trust services criteria. The Description presents Basware's system; its controls relevant to applicable trust services criteria; and the types of complementary subservice organization controls that the service organization assumes have been implemented, suitably designed, and operating effectively. The Description does not disclose the actual controls at the subservice organizations.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Basware, to achieve Basware's service commitments and system requirements based on the applicable trust services criteria. The Description presents Basware's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Basware's controls.

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

a) the Description presents Basware's Network solution that was designed and implemented throughout the period January 1st, 2025 to September 30th, 2025, in accordance with the Description Criteria.

b) The controls stated in the Description were suitably designed throughout the period January 1st, 2025 to September 30th, 2025 to provide reasonable assurance that Basware's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and carved-out subservice organization and user entities applied the complementary controls assumed in the design of Basware's controls throughout the period January 1st, 2025 to September 30th, 2025

c) The controls stated in the Description operated effectively throughout the period January 1st, 2025 to September 30th, 2025 to provide reasonable assurance that Basware's service commitments and system requirements would be achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls, assumed in the design of Basware's controls, operated effectively throughout the period 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. 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.

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.

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.

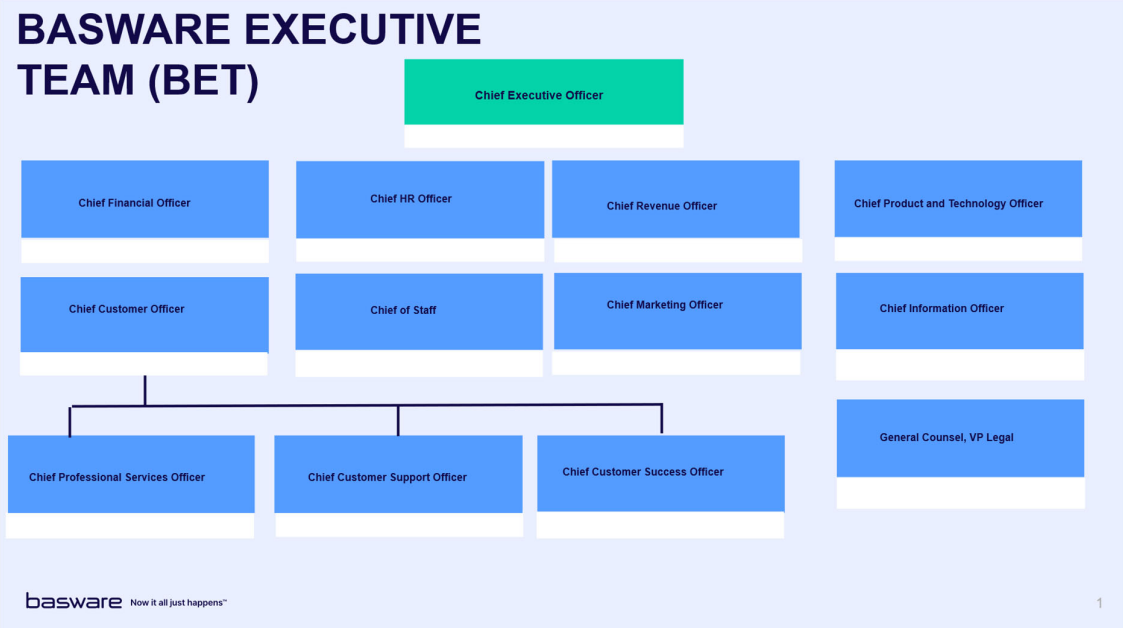
Firewall security deployed to filter traffic to and within the network and block unauthorized traffic is administered via AWS Security groups associated with cloud environment resources as well as Web Application Firewall (WAF) configurations. AWS GuardDuty is enabled to continuously monitors the infrastructure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



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.

4. Sub-Service 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.

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.

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)

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).

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.

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.

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.

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.

10. Complementary User Entity Controls (CUECs)

Customers must manage their own user accounts and passwords.

Customers must comply with the Basware Technical Requirements.

11. 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

2017 TRUST SERVICE CRITERIA (TSC)

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.				
5.36	Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	Auditors observed that there is a systematic Information Security Management System Audit Program that has been documented and managed in Confluence. This ISAE audit acts one example of such audit. As part of control testing for 5.35 auditors noted that Basware has ISO 27001 certification that is audited regularly and processed at different levels of company management.	No exceptions noted.	
6.3	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	Inspected the organization's Learning Management System where onboarding and annual awareness trainings are completed. For a selection of employees, inspected that the annual training was completed. For a selection of new joiners, inspected Navigator Plans (onboarding records from the HR system) to determine that awareness training was completed as part of the onboarding 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
6.4	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Inspected the Employee Relations Policy adopted by the organization to determine that disciplinary process is established and documented and acknowledged by all employees as part of the policy. Inquired and noted that there was 1 case of breach of Code of Conduct during the attestation period. During the walkthrough with the control owner, inspected records and communications to determine that the disciplinary process was followed accordingly.	No exceptions noted.	
6.5	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	Inspected the identity and access management processes for joiners, movers and leavers. It was noted that the changes are triggered automatically from the HR system. Inspected the terms of conditions of employment documented in the employment agreements to determine that information security responsibilities and duties that remain valid after termination or change of employment are defined.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
6.6	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Inspected the organization's employee relations policy, external contractor process and sourcing process to determine that relevant procedures are established. For a selection of new joiners, inspected that employment agreements include confidentiality and non-disclosure obligations. For a selection of new vendors, inspected that contractual agreements include confidentiality and non-disclosure obligations as relevant.	No exceptions noted.	
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.				
5.2	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	Auditors inspected that the Security Team organization has been formally defined. Auditors inspected that security roles are documented in Basware's HR system along with associated responsibilities. Auditors observed that organization's need and current situation for security roles is tracked by KPIs which is monitored by management.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.				
5.3	Conflicting duties and conflicting areas of responsibility shall be segregated.	Auditors inspected Access Management policy and process description and noted that conflicting duties and conflicting areas of responsibilities are segregated. Auditors inspected the process for applying internal access and noted that person who needs access and the authorizer for the request cannot be the same person. It was noted that for Cloudscan there were no changes made to user rights, but access is managed by product manager or product architect. For Cloudscan it was noted that users are assigned to role specific groups instead of direct individual permissions. For other solutions in scope, auditors inspected a selection of tickets for users who were granted access and noted that the authorizer was different from the requestor. It was also noted that responsibilities are segregated, as changes to production need to be reviewed in CAB meetings. Inspected CAB meeting notes as a sample.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.				
6.1	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Inspected the Background Screening Recruitment process adopted by the organization. For a selection of employees who joined the organization during the testing period, inspected the background screening records from the HR system to determine that screening was completed and documented.	No exceptions noted.	
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.				
6.2	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	Inspected that the Basware contract of employment contains clauses on confidentially, the disciplinary process and the acceptable use of IT. For a selection of employees who joined the organization during the testing period, inspected the employment agreements to determine that the agreements include relevant closes and security obligations.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.				
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.	
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.				
8.14	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Auditors inspected SLA, Availability Management, technology strategy documents and relevant processes to note that availability requirements are met by implementing sufficient redundancy. Auditors inspected a selection of system availability reports and noted that availability is monitored.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.				
5.13	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Auditors inspected that Basware uses three labels for all information (public, private and restricted) and that these labels are automatically applied to M365 applications. Auditors learned through inquiry that outside of MS applications users are required to refer to the policy for guidance of how process Basware data and manually apply labels if applications allow.	No exceptions noted.	
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.				
5.35	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	Auditors learned through inquiry that Basware Information Security Management System has been certified against the ISO 27001 standard and that it is Independently reviewed each year by FINAS accredited certification body. Auditors inspected that the report this audit is shared with management at Security Steering Committee and at the Management review meetings. Auditors observed that findings from audits are being logged, monitored and updated in Confluence.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.				
5.4	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Inquired of the control owners and noted that personnel are made aware of the security responsibilities via mandatory training which is completed as part of the onboarding process and annually thereafter. Additionally, clauses on confidentiality and other security obligations are established in the employment contracts. For a selection of Basware employees, inspected records of annual training completion to determine that security responsibilities have been communicated.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.				
5.5	The organization shall establish and maintain contact with relevant authorities.	Auditors observed that in Confluence there is a list of contacts with special interest groups and noted that regulatory authorities and CISA/Traficom are included on the list. Auditors observed that the Data Breach Notifications process has been documented in Confluence, and it details the process for notifying the regulatory bodies. Auditors inquired from management and learned that no such incidents have occurred in 2025 where contacting authorities would be required.	No exceptions noted.	
5.6	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Auditors observed that in Confluence there is a list of contacts with special interest groups. Auditors inspected examples of contact with special interest groups including Traficom, CISA, and Accel-KKR.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.				
5.31	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	Inspected documentation regarding corporate compliance, cybersecurity compliance and data privacy compliance to determine that relevant processes are established. Inquired of the control owner and noted that he continuously monitors changes in the regulatory landscape. Inspected Basware General Terms and Basware SLA to determine that Basware has defined relevant terms and conditions to maintain compliance with regulatory and contractual requirements.	No exceptions noted.	
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.				
5.7	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Auditors observed that Basware actively monitors various intelligence feeds for vulnerabilities and emerging threats. Through inquiry, auditors learned that potential threats are addressed via a documented vulnerability management process. Additionally, auditors inspected examples of inbound threat intelligence.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.				
5.21	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Inspected organization's established processes and procedures related to managing information security risks in the ICT supply chain. For a selection of ICT suppliers, inspected a selection of records to determine that the vendor reviews were performed in accordance with the process and defined schedule.	No exceptions noted.	
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.				
5.14	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	Auditors inspected Cryptography and Key management policy and inquired from the control owner and noted that Information transfer rules, procedures, or agreements are in place. It was noted that emails can be encrypted with company email solution and SSL/TLS encryption is being used for all client-server-traffic.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC4.1 The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.				
5.37	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Auditors inspected process documentations regarding operating procedures and noted that they are documented and made available to personnel who need them. For solutions in scope, auditors inspected a selection of process documentations to note that they were available for employees in Confluence.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC4.2 The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.				
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 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
CC5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.				
5.32	The organization shall implement appropriate procedures to protect intellectual property rights.	Inspected the risk assessment for IP, third party open-source license policy and third-party license compliance policy to determine that the organization has established relevant procedures for IP protection and regulatory compliance.	No exceptions noted.	
5.33	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Auditors observed that there is a formal Record Retention policy that has been published. In the policy, relevant definitions and responsibilities have been documented, and information storage, disposal and destruction have been addressed. Auditors also observed that there are more detailed record retention instructions in Confluence that include e.g. minimum retention times and deletion times for different record types.	No exceptions noted.	
5.34	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Inspected the Privacy policy and Data Privacy Compliance documentation to determine that the organization has established relevant procedures for data privacy protection and regulatory compliance.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives. CC5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.				
5.1	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Auditors observed that information security policy along with several topic-specific policies have been defined. Auditors inspected that the information security policy has been published in the intranet and that it has been reviewed by the CISO in October 2025.	No exceptions noted.	
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.				

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
5.9	An inventory of information and other associated assets, including owners, shall be developed and maintained.	Auditors inspected IT asset management process to note that an inventory of information and other associated assets, including owners, is developed and maintained. It was noted that documentation includes ITAM roles and responsibilities, assets with registry owners, descriptions and related processes. Observed Miradore tool and inspected user endpoint devices as a sample to note they are listed in asset register. For Cloudscan it was noted that assets consist of source code repository and Azure resources. For other solutions in scope auditors inspected asset management documentation and noted it includes assets, owners and it is maintained.	No exceptions noted.	
5.10	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	Auditors inspected that there is an appropriate Acceptable Use Policy. Auditors observed from Basware's intranet that the policy has been published there and that it has been approved in February 2025. Auditors inspected that acceptable use awareness is provided via employee experience platform Viva Engage.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
5.12	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	Auditors learned through inquiry and inspection that there are three classifications levels for information, and for all of them, descriptions, examples and rules have been outlined in the Information Classification and Handling Policy. Auditors observed that the policy has been approved by the CTO in March 2025 and that the policy has been published in Basware's intranet.	No exceptions noted.	
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. For Cloudscan it was noted that user access is not granted directly to Azure resources but managed through role-based user rights. For Cloudscan there was not any access rights were granted during audit period. For other solutions in scope access right tickets were inspected as a sample to note that granting access was based on a business 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
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. For solutions in scope, inspected resigned employees as a sample, to note that identities life cycle was managed fully. Granted access rights were inspected in control 5.17 as a sample.	No exceptions noted.	
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.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
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.	
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.	
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.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.22	Groups of information services, users and information systems shall be segregated in the organization's networks.	Auditors inspected documentation regarding CATO Networks SASE and noted that Basware started using their SASE service gradually in October 2024. Documentation describes project phases and current progress. Inspected documentation and noted that it includes information regarding country, site, rollout schedule, status, priority, region, primary PoP (Point of Presence) and primary PoP WAN IP addresses. Inspected the access design documentation and access management documentation to determine that the guidelines for network segregation and respective segregation of accesses are established. Inspected the list of separate networks within the VPS to determine that network separation is implemented as designed. Observed the dedicated accounts on the cloud hosting platform to determine that separation is configured accordingly.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.24	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Auditors inspected the Cryptography and Key Management policy and best practices documentation and noted that rules for the effective use of cryptography, including cryptographic key management, were defined and implemented. Inspected configurations with control owner as a sample to note they follow Cryptography and Key management policy.	No exceptions noted.	
8.34	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	Auditors learned through inquiry that Basware conducts penetration testing exclusively in non-production environments using only demo data, ensuring confidentiality, integrity and availability, and that the scope of each test is clearly defined, and tests are performed by certified professionals, who are not given access to source code, production systems, or any private or restricted data. Auditors inspected samples of penetration testing reports and noted that testing was done in Basware's QA environment.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.				
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.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.18	The use of utility programs that can be capable of overriding system and applications shall be restricted and tightly led.	Auditors inspected AUP and Client device policies and noted that Endpoint device management process defines how devices are protected, managed and software installations are restricted. Beyondtrust Privilege Endpoint Management on client devices is used for controlling end-user actions on their devices. Inspected Whitelisted applications that can be added to End User Device Software Catalog. For solutions in scope, inspected a list of authorizers, that can grant access rights.	No exceptions noted.	
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives. C1.2 Additional criteria for confidentiality: The entity disposes of confidential information to meet the entity's objectives related to confidentiality.				
6.7	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Auditors inspected the AUP document and noted that it's been approved and reviewed during audit period. Auditors also inspected the When and Where we Work policy. It was noted that security measures are being implemented when personnel are working remotely, to protect information accessed, processed or stored outside the organization's premises.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
7.7	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	Auditors inquired from the control owner and inspected the clear office policy and noted that clear desk rules for papers and removable storage media and clear screen rules are defined and appropriately enforced. It was noted that policy is being reviewed annually, next review in October 2025.	No exceptions noted.	
7.10	Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Auditors inspected AUP documentation, Client device policy and instruction for encrypting removable storage and noted that storage media is managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements. Removal or disposal of equipment was checked in control 7.14 as a sample.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
7.14	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Auditors inquired from the control owner and were informed that any IT equipment can be recycled securely either by using leasing provider's or Fujitsu's Onsite Support provided recycling services. Devices are wiped and a report of Data Erasure is granted. Auditors inspected Data Erasure reports as a sample from audit period and noted that reports include digital signature and hardware details.	No exceptions noted.	
8.1	Information stored on, processed by or accessible via user end point devices shall be protected.	Auditors inspected AUP documentation, Client device policy and endpoint device management process to note that information stored on, processed by or accessible via user endpoint devices is protected. Employee devices were inspected as a sample to note that they are protected with encryption and antivirus software.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.				
5.11	Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Auditors inspected the Exit process adopted by the organization and observed the HR system used to track the offboarding activities. For a selection of employees who have left the organization during the attestation period, inspected the exit checklists to determine that personnel have returned the organization's assets in their possession and the return of assets has been documented in the exit checklists.	No exceptions noted.	
8.10	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	Auditors inspected Privacy, Record Retention and Information Classification policies to note that information is deleted when it's no longer required. For services in scope, auditors inspected cleanup tasks that were run to production environment to remove data based on retention date. Auditors also inspected lifecycle policy for S3 documents. Also inspected data erasure reports in control 7.14 to note that information is removed from devices.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.				
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.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.21	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	Auditors inspected documentation regarding CATO Networks SASE and noted that Basware started using their SASE service gradually in October 2024. 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 the architecture documentation, Azure portal settings and user rights review were inspected to note that security mechanisms and service requirements of network services are identified, implemented and monitored. Cloudscan is serverless application on Azure, many aspects of security and monitoring happen through Microsoft.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.23	Access to external websites shall be managed to reduce exposure to malicious content.	Inquired from the control owner and were informed that firewalls with web filtering feature are enabled. Basware is moving to SASE solution using CATO Networks technology. Observed that all Internet traffic goes through CATO cloud which have web filtering feature enabled.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.				
8.12	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Auditors inspected organization's cryptography guidelines and configurations, including best security practices for cryptography, encryption for data in transit and encryption for data at rest to determine that encryption is implemented to protect data. Inspected organization's information classification and handling policy to determine that the guidelines for acceptable use of data based on category are established. Auditors inspected Information Classification and Handling policy and noted that requirements for information classification and general guidelines for information handling are defined. Classification levels are public, private and restricted. Also inspected Endpoint Device management document.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.				
8.7	Protection against malware shall be implemented and supported by appropriate user awareness.	Auditors inspected Endpoint Device management documentation and noted that Microsoft Defender for Endpoint is used on Windows, MacBook and mobile devices. Antivirus, anti-malware and personal firewall features are centrally managed through Defender management console. It was noted that F-Secure Antivirus tool is used on hosted servers, it is part of hosting providers offering and provider is responsible for its management. Employee endpoint devices were inspected as a sample to note that they are protected against malware.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.19	Procedures and measures shall be implemented to securely manage software installation on operational systems.	Auditors inspected AUP and Client device policies and noted that Endpoint device management process defines how devices are protected, managed and software installations are restricted. It was noted that Beyondtrust Privilege Endpoint Management on client devices is used for controlling end-user actions on their devices. Inspected a user as a sample to note that his devices are within Intune management and Beyondtrust Privileged Endpoint Management solutions. For solutions in scope, inspected a selection of change tickets, to note that procedures and measures are implemented to securely manage software installation on operational systems.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.				
8.9	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	Inspected organization's policies and technical documentation to determine that configurations benchmarks and security requirements are defined, documented and maintained up to date. Changes to configuration follow the standard change management process. Auditors inspected the Change management documentation and work instructions and noted that changes that are about to be implemented are first assessed to check if they meet approval criteria and then they are approved, before they are implemented to production. The CAB process manages that changes are reviewed and approved before implementation. Inspected a selection of CAB memos as a sample to note that changes are reviewed in CAB meetings.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.27	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	Inspected that secure development policy and operational guidelines for change impact analysis are defined and regularly reviewed and updated. Inspected the Enterprise Architecture Review Board structure and process flow diagram to determine that the process for architecture review is established.	No exceptions noted.	
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.				
8.15	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	Auditors inspected the Log and Monitoring policy to note that requirements for logging and monitoring are documented. Log Management document lists different logs, log source, who has access to them, how long and where they are stored. Auditors inspected a Microsoft Defender Alerts as a log sample. Auditors also noted through inspection that for example user logins, SFTP logins, and API calls are logged for Network services.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.16	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Auditors inquired and learned that the internal IT environment is monitored using Microsoft Defender and Sentinel by a 24/7/365 Security Operations Centre (SOC) provided by Fujitsu Finland. Auditors inspected evidence of Defender portal incident dashboard and examples of a SOC issued actions to Basware's IT Support Team. Auditors learned through inquiry that customer products are monitored using GuardDuty which sends alerts to the Splunk SIEM which in turn sends alerts to the 24/7/365 Cloud Operations Team. Auditors inspected evidence about the SIEM monitoring dashboard and inspected Basware's monitoring alerts guidelines.	No exceptions noted.	
8.17	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	Auditors inquired from the control owner and were informed that Active Directory and services are syncing their time from Time Servers on the Internet. Inspected a screenshot from terminal to note clock synchronization as a sample. Observed current clock synchronization configurations for the client domain and AD server to determine that the relevant group policies are configured appropriately to enable clock synchronization.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.				
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.	
5.25	The organization shall assess information security events and decide if they are to be categorized as information security incidents.	Auditors observed that there are formal instructions for Security Incident Validation and Classification. Auditors observed there is a systematic process flow for validating, classifying and declaring security incidents. Auditors tested with a sample that security incidents have been assessed and classified appropriately.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
5.27	Knowledge gained from information security incidents shall be used to strengthen and improve the information security.	Auditors tested with a sample that root cause analysis has been performed for information security incidents and that lessons learned have been identified and documented. Auditors also inspected an example of a vulnerability that was identified during a security incident and then transferred to the vulnerability management process for mitigation.	No exceptions noted.	
5.28	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Auditors tested with a sample that evidence has been collected as part of each step of the security incident management process and that the timeline of events along with supporting evidence has been documented appropriately. Auditors also observed that there are formal process instructions that define the activities needed for security incident related forensic analysis.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.8	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
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.				
6.8	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Auditors observed that standard operating procedures for reporting security incidents are documented in Confluence. Auditors inspected evidence confirming that tools and instructions for reporting suspected security incidents are available on Basware's intranet. Additionally, auditors noted that similar instructions for external users are published on Basware's homepage.	No exceptions noted.	
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.				
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
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 backup management documentation and noted that procedures vary depending on the type of service and where it is hosted. Noted that there were planned tests for Active Directory, Azure hosted servers and Fujitsu hosted servers. Inspected a sample of tests and noted they were documented to Confluence. Also noted next year's plan for future tests exists. 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 #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.				
5.8	Information security shall be integrated into project management.	Inspected the policies and procedures adopted by the organization for project management in development activities and noted that security considerations are embedded in the process. Inspected the Go to Market program management process, product development process, and secure development policy to determine that security considerations are included in the established project management activities in development and regularly reviewed and updated. Inspected the Enterprise Architecture Review Board structure and process flow diagram to determine that the process for architecture review is established.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
5.23	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	Auditors inspected documents regarding vendor assessments, and vendor management and Information Classification and Handling policy to note that processes for acquisition, use, management and exit from cloud services are established in accordance with the information security requirements. It was noted that strategic vendors are reviewed annually and sourcing request assessments when needed, or if there are changes in the contract with the vendor. Inspected a selection of annual and ad-hoc vendor assessments to determine that assessments have been performed accordingly.	No exceptions noted.	
8.4	Read and write access to source code, development tools and software libraries shall be appropriately managed.	Inspected the access request process adopted by the organization and 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. It was also noted 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
8.25	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
8.26	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Auditors inspected Sourcing and Vendor Assessment processes and noted that the goal is to minimize enterprise and operational risks, ensure compliance with their internal and external quality requirements and describe tasks that are required to run the sourcing process successfully. Sourcing process includes exception matrix, where security and data or data privacy matters can be estimated. Security reviewer evaluates the security level of supplier and defines a risk level and then writes a statement according to the evaluations. For solutions in scope, inspected change approval process documentation to note that changes go through the sign off process after the mandatory tests are completed. Selection of normal change tickets were inspected as a sample.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.28	Secure coding principles shall be applied to software development.	Auditors 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
8.30	The organization shall direct, monitor and review the activities related to outsourced system development.	Auditors inspected the Vendor management and Sourcing processes. It was noted that outsourced system development is monitored, and activities are reviewed according to sourcing, vendor management and vendor performance and compliance management process. Inspected annual and ad-hoc vendor assessments as a sample.	No exceptions noted.	
8.31	Development, testing and production environments shall be separated and secured.	Auditors inspected Change Management process and work instructions. According to control owner development, testing and production environment are created and separated when it is needed and feasible. There are situations where separate testing and/or development environments are impossible to have. Inspected the system architecture technical documentation to determine that development, testing, staging and production environments are separated. Observed the accounts from the cloud hosting platform to determine that the accounts are configured accordingly to enable separation of environments and accesses.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
8.32	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.	
8.33	Test information shall be appropriately selected, protected and managed.	Inspected the production database extraction procedures and operational guidelines on how to mask data in the database schema. Inquired regarding the requests for production data testing during the attestation period and noted that there were no such occurrences.	No exceptions noted. Auditors did not perform the test of operating effectiveness, as there were no occurrences of control operation 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
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.				
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 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
CC9.2 The entity assesses and manages risks associated with vendors and business partners.				
5.19	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Inspected the Vendor Assessment, Review, and Management processes to determine that the processes are established, documented and maintained up to date. For a selection of suppliers, inspected the assessments performed to determine that the process was followed accordingly.	No exceptions noted.	
5.20	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	Inspected the Vendor Assessment, Review, and Management processes to determine that the processes are established, documented and maintained up to date. For a selection of suppliers, inspected the assessments performed to determine that the process was followed accordingly.	No exceptions noted.	

Control #	Control Description	Planned nature and extent of audit procedures to evaluate the control's operating effectiveness	Testing results	Management response
5.22	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Auditors inspected the Vendor Assessment process and noted Vendor Portfolio. It was noted that the organization regularly monitors, reviews, evaluates and manages changes regarding supplier information security practices and service delivery. Strategic vendors are reviewed annually and sourcing requests assessments through TrustArc solution when needed, or if there are changes in the contract with the vendor. Selection of assessments were inspected as a sample in control 5.23.	No exceptions noted.	