ivanti

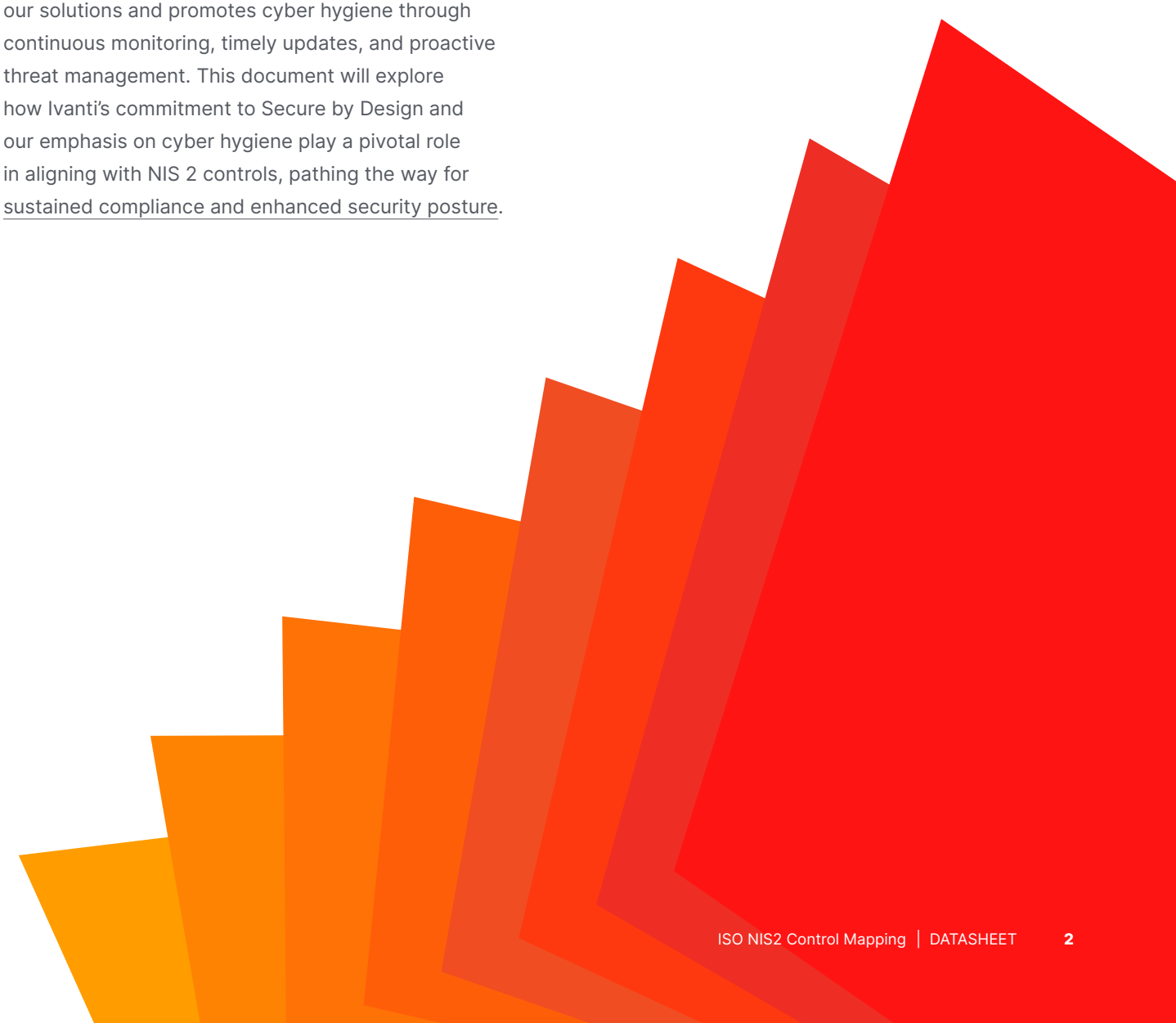

# ISO NIS2 Control Mapping

## Ivanti Helps Prepare for NIS 2 Compliance

In an era where digital threats are evolving with increasing sophistication, the implementation of robust cybersecurity measures is more crucial than ever. The NIS 2 Directive, an EU-wide legislation aimed at bolstering network and information system security across member states, establishes a framework for achieving higher levels of security. For organizations striving to comply with these regulations, understanding how cybersecurity controls map to NIS 2 is essential. This document aims to demonstrate how Ivanti's processes as a software vendor and supplier align with these requirements, ensuring that they not only meet but exceed the regulatory standards.

Ivanti is committed to supporting our customers in their cybersecurity endeavors, which is why we are proud to be ISO 27001 certified. This certification is a testament to our dedication to maintaining high security standards and delivering quality assurance in all our products and services. By choosing Ivanti as a supplier, our customers can trust that they are partnering with a provider that adheres to internationally recognized best practices and standards in information security management. Our alignment with ISO standards reinforces our capability to assist customers in navigating the landscape of NIS 2 compliance effectively.

Furthermore, Ivanti embraces the Secure by Design pledge, which ensures that every product is built from the ground up with security as a foundational element. This approach enhances the protection of our solutions and promotes cyber hygiene through continuous monitoring, timely updates, and proactive threat management. This document will explore how Ivanti's commitment to Secure by Design and our emphasis on cyber hygiene play a pivotal role in aligning with NIS 2 controls, pathing the way for sustained compliance and enhanced security posture.



| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| **A.** Policies on risk analysis and information system security. | 5.2, A.5.1 | Ivanti adheres to its Information Security Policy, which undergoes annual review. These policies are accessible to all employees through the Ivanti Intranet (Ivanti Everywhere) page.<br><br>Additionally, Ivanti maintains and adheres to its Risk Management Policy and Risk Treatment Plan. | Ivanti Enterprise Security Policies are developed by the Enterprise Security team and approved by the Security Council.<br><br>The Information Security policies are incorporated as part of the Information Security training decks. It is communicated to all employees through ISMS training sessions and awareness programs.<br><br>**ISMS policy statement**<br>To ensure all stakeholders (external, internal and interested parties) are appropriately informed regarding Information Security policies and procedures, and to keep to the commitment for continuous improvement in accordance with business requirements and relevant legal, statutory and regulatory requirement, Ivanti adheres to its Information Security Policy, which is reviewed annually. |
| | 6.1.2, 8.2 | | As part of Ivanti's risk management activities, Ivanti conducts an annual Information Security Risk Assessment. The assessment is an interview-based process that focuses on identification of key risks within the organization.<br><br>The result of the risk assessment interviews is the creation of an annual Risk Assessment Report and Risk Matrix. These documents are then used to drive internal risk management activities for the forthcoming year.<br><br>**Ivanti's approach to risk management involves the following activities:**<br>**Risk identification and assessment:** Includes identification and evaluation of risks and potential impact to existing environment, determining existing controls in place and recommendation of risk-reduction measures.<br>**Risk migitaion:** Involves prioritizing, implementing and maintaining appropriate risk-reduction measures recommended from the risk assessment process.<br>**Report:** Develop a risk report inclusive of risk evaluation data, progress and mitigation procedures for submission to Ivanti administration and management.<br>**Continual evaluation:** The continuous process of monitoring and evaluating the treated risks and associated residual risks. This phase further determines the control improvements required to mitigate similar risks. |
| | 6.1.3, 8.3 | | A risk treatment plan is developed based on risk assessment result. The risk manager will identify the risk owner, what additional controls shall be implemented, who is responsible for them and the target date of closure. The purpose of additional controls selection and implementation is to reduce risk to an acceptable level. Determination of control objectives and controls is based on the results and conclusions of the risk assessment and risk treatment processes, legal or regulatory requirements, contractual obligations and the organization's business requirements for information security. Appropriate control objectives and controls have been determined from Annex A of ISO/IEC 27001:2022 and implemented to meet the requirements identified by risk assessment and risk treatment processes to reduce risks to an acceptable level. |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| **B.** Incident handling. | A.5.24 | Ivanti has a well-defined Information Security Incident Management policy to establish the requirement that all departments develop and maintain an Incident Response Plan.<br><br>Ivanti maintains Acceptable Use Policy and Incident Response Policy. Management responsibilities and procedures are established to ensure a quick, effective and orderly response to information security incidents. | The Security Incident Management team analyzes and classifies the incident as per the Incident Management Plan. The criticality of the affected resource (Ivanti and/or customer information assets, personnel and infrastructure) and the severity of impact of the event / incident will be prioritized based on incident classification.<br><br>This classification is helpful in prioritizing the response to events/incidents. Prioritization is determined by considering both the urgency of the incident (how quickly the business needs a resolution) and the level of impact. An indication of impact is often (but not always) the number of users affected. In some cases, the loss of service to a single user can have a major business impact.<br><br>Based on the severity of impact, immediate steps shall be taken to minimize the impact of the event/incident, including implementation of commensurate compensating controls. |
| | A.5.25, A.6.8 | | **Employees shall report:**<br><br>• Cloud information security incidents to DL-CloudComplianceSecurity@ivanti.com<br>• Physical security events/incidents to facilities administration, service desk or building reception/security officer.<br>• Password compromise events/incidents related to Ivanti Network to security@ivanti.com.<br>• Password compromise events/incidents related to Ivanti Cloud Network to DL-CloudComplianceSecurity@ivanti.com. |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| | A.5.26 | Networks and network devices are secured, managed and controlled to protect information in systems and applications. Networks, systems and applications are monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents.<br><br>Groups of information services, users and information systems should be segregated in the organization's networks. | Ivanti has a well-defined and documented Information Security Incident Response Plan that addresses incident reporting, incident analysis and classification, notification to relevant stakeholders and incident resolution. Incident analysis shall be performed by the CSC Team, as applicable, to determine the actions to be taken by Ivanti and sufficient controls to be implemented to prevent similar events. . |
| | A.5.27 | | Incidents shall be analyzed and appropriate actions taken to prevent recurrence of these incidents. Actions shall also be taken to prevent future Information security incidents.. |
| | A.5.28 | | Incident Management Team members shall collect evidence from the site of incident.<br><br>Evidence collected shall be admissible (presentable in a court of law), complete and of good quality (have evidential integrity). Copies of the evidence shall be used for internal root cause analysis and as forensic evidence where follow-up involves legal action (either civil or criminal) against a person or an organization. The original evidence shall be kept secure and untouched.<br><br>For computer media or soft-copy Information, mirror images or copies should be used for investigative purposes. Logs of all actions during the copying process shall be kept. |
| | A.8.16 | | **System performance monitoring**<br>Ivanti Cloud Operations utilizes automated monitoring systems (New Relic) that provide a high level of service performance and availability. Monitoring activities are intended to identify and remediate areas of risk including strategic risk, financial risk, operational risk and legal/regulatory risk.<br><br>**Network perimeter monitoring**<br>Ivanti monitoring tools are implemented to monitor servers and application performance, application traffic threshold and anomaly detection. These monitoring tools are configured with threshold alarms notifications to Ivanti Cloud Operations.<br><br>**Event-logging monitoring activities**<br>For added granularity, Ivanti utilizes a centralized non-editable log collection tool for centralized monitoring of server and application logs. An SOC monitors events including, but not limited to, Windows security, application and system logs indicating use of privileged accounts, software installation, and changes to user permissions or privileges. Audit logs and security events shall be archived to assist in future investigations. |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| **C.** Business continuity, such as backup management and disaster recovery, and crisis management. | A.5.29 | Ivanti maintains an ISMS Manual, which explains how equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.<br><br>Backup copies of information, software and system images are taken and tested regularly in accordance with ISM Backup Policy and schedule. | Ivanti has a well-defined disaster recovery plan in the event of failure of Ivanti Cloud infrastructure components, based on the risk assessment and the security objective.Theinformation processing facilities have sufficient redundancy to meet the availability requirements of Ivanti Cloud and customers. The redundant information systems are tested annually to ensure the failover from one component to another component.<br><br>Disaster recovery process will be tested periodically as per guidelines or customer requirements. Test plan will be defined and validated by relevant stakeholders. The results of the tests and action taken to improve the plans will be recorded.<br><br>The Disaster Recovery Procedures/Business Continuity Plans will be updated based on the lessons learned or key issues identified during planned recovery testing. |
| | A.5.30 | | Regarding the approach to disaster recovery and business continuity that an organization is taking, two major elements that need to be identified and analyzed are those events that can cause interruptions to the business process, and the impacts such interruptions can have on the organization. |
| | A.8.13, A.8.14 | | Ivanti information owners will ensure that all the essential business Information is backed up at agreed-upon frequency and can be restored in case of an outage.<br>Customer data is backed up utilizing the cloud provider's services. In the event of an exception, operations personnel will work with the cloud provider to re-establish services.<br>Backup infrastructure resides on private networks logically secured from other networks.<br><br>**Azure:** Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.<br>Customer data is automatically replicated within Azure to minimize isolated faults. Azure services are configured to automatically restore customer services upon detection of hardware and system failures.<br>**AWS**: Critical AWS system components are replicated across multiple availability zones and backups are maintained. Backups of critical AWS system components are monitored for successful replication across multiple availability Zones. |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| | A.8.15 | | Audit logging configurations are in place for infrastructure components to capture the following events.<br><br>• Account logon events.<br>• Account management.<br>• Directory Service Access.<br>• Logon events.<br>• Object access.<br>• Policy changes.<br>• Privilege use.<br>• Process tracking.<br>• System events.<br><br>Ivanti utilizes a centralized non-editable log collection tool for centralized monitoring of server and application logs. An SOC monitors events including, but not limited to, Windows security, application and system logs indicating use of privileged accounts, software installation, and changes to user permissions or privileges. Audit logs and security events shall be archived to assist in future investigations. |
| | A.8.16 | | **System performance monitoring**<br>Ivanti Cloud Operations utilizes automated monitoring systems (New Relic), which provide a high level of service performance and availability. Monitoring activities are intended to identify and remediate areas of risk including strategic risk, financial risk, operational risk and legal/regulatory risk.<br><br>**Network perimeter monitoring**<br>The Ivanti monitoring tools are implemented to monitor servers and application performance, application traffic threshold and anomaly detection. These monitoring tools are configured with threshold alarms notifications to Ivanti Cloud Operations.<br><br>**Event-logging monitoring activities**<br>For added granularity, Ivanti utilizes a centralized non-editable log collection tool for centralized monitoring of server and application logs. An SOC monitors events including, but not limited to, Windows security, application and system logs indicating use of privileged accounts, software installation, and changes to user permissions or privileges. Audit logs and security events shall be archived to assist in future investigations. |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| **D.** Supply chain security, including security-related aspects concerning the relationships among each entity and its direct suppliers or service providers | A.5.19 | All relevant information security requirements are established and agreed upon with each supplier that may access, process, store, communicate or provide IT infrastructure components for the organization's information.<br><br>Information security requirements for mitigating the risks associated with suppliers' access to the organization's assets are agreed upon with the supplier and documented. | Ivanti has a Partner and Vendor Risk Management Policy for third-party connections. The objective of this policy is to protect Ivanti Cloud assets that are accessed by suppliers by identifying the risk to employees with the supplier's access to Ivanti Information Assets.<br><br>Information security requirements are addressed in supplier contracts. A list of suppliers/vendors is maintained in the Vendor Risk Management system. |
| | A.5.20 | | Information security requirements are addressed as part of the vendor agreement, and necessary controls are implemented based on the risk category of vendor.<br><br>• Legal function will be involved in developing an agreement/contract with any third party to ensure that Ivanti interests are safeguarded.<br>• Identified security requirements shall be incorporated in the third-party agreements.<br>• The agreements shall clearly spell out the obligations and the responsibilities of the parties without ambiguity to ensure that there is no misunderstanding between the parties.<br>• Depending on the sensitivity and criticality of the information or services provided, relevant stakeholders shall consider commissioning or requesting an independent review of the service provider's internal control structure.<br>• An NDA should be established between Ivanti and any vendor who has access to confidential data. |
| | A.5.21 | | Ivanti's Enterprise Security and Compliance team will ensure that security requirements are included in the agreement with suppliers who provide Information and communications technology services and IT products. The services provided by these suppliers are reviewed/monitored to validate that the delivered Information and communication technology services are in line with the stated security requirements.<br>The respective stakeholders ensure that the delivered Information and communication technology products are functioning as expected without unexpected or unwanted features. |
| | A.5.22 | | The respective functions will monitor and review the records and reports provided by third-party services to ensure that the Information security terms and conditions of the agreements are being adhered to.<br><br>The following shall be monitored and reviewed (including but not limited to):<br>• Service performance levels to check adherence to the agreements.<br>• Service reports produced by the supplier.<br>• For high-risk Vendors, conduct audits.<br>• Supplier's capability to maintain service continuity.<br><br>The suppliers/vendors are evaluated, reviewed and documented in the Vendor Risk Management system |
| | A.5.23 | | Processes for acquisition, use, management and exit from cloud services are established in accordance with the organization's information security requirements. |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| **E.** Security in Network and Information System acquisition, development and maintenance, including vulnerability handling and disclosure. | A.5.20 | Information security requirements are addressed as part of the vendor agreement, and necessary controls are implemented based on the risk category of vendor. | Information security requirements are addressed as part of the vendor agreement, and necessary controls are implemented based on the risk category of vendor.<br>• Legal department will be involved in developing an agreement/contract with any third party to ensure that Ivanti interests are safeguarded.<br>• Identified security requirements shall be incorporated in the third-party agreements.<br>• The agreements shall clearly spell out the obligations and the responsibilities of the parties to ensure there is no misunderstanding between the parties.<br>• Depending on the sensitivity and criticality of the information or services provided, relevant stakeholders shall consider commissioning or requesting an independent review of the service provider's internal control structure.<br>• An NDA should be established between Ivanti and any vendor who has access to confidential data |
| | A.5.24 | | The Security Incidents Management team analyzes and classifies the incident as per the Incident Management Plan. The criticality of the affected resource (Ivanti and/or Customer Information Assets, personnel and infrastructure) and the severity of impact of the event/incident will be prioritized based on incident classification.<br><br>This classification is helpful in prioritizing the response to events/incidents. Prioritization is determined by considering both the urgency of the incident (how quickly the business needs a resolution) and the level of impact. An indication of impact is often (but not always) the number of users affected. In some cases, the loss of service to a single user can have a major business impact. |
| | A.5.37 | | Ivanti's IT team documents and maintains operating procedures on system activities associated with handling Ivanti Cloud assets. These documents follow formal document control procedure, and changes to these documents shall be approved before release.<br>The Ivanti Cloud Operations team documents and maintains operating procedures for system activities associated with Information processing. |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| | A.6.8 | | As soon as an employee encounters an information security event or incident, he/she shall report it to the Enterprise Security and Compliance team and/or the CSC Team.<br><br>**Employees shall report:**<br>• Cloud information security incidents to DL-CloudComplianceSecurity@ivanti.com.<br>• Physical security events/incidents to facilities administration, service desk or building reception/security officer.<br>• Password compromise events/incidents related to Ivanti Network to security@ivanti.com.<br>• Password compromise events/incidents related to Ivanti Cloud Network to DL-CloudComplianceSecurity@ivanti.com. |
| | A.8.8 | | Ivanti has a dedicated vulnerability management team that performs scans on a weekly basis; remedial actions are taken where necessary. In addition, a third party performs a penetration test annually to identify and exploit vulnerabilities identified within the environment. |
| | A.8.9 | | Ivanti has defined configuration standards to ensure compliance. |
| | A.8.20 | | Ivanti's Cloud Operations team maintains well-documented procedures on hardware and software configurations of networks and all critical parameter settings, scripts and configuration files used. The team ensures networks are adequately managed and protected from threats and security is maintained for systems and applications (including information in transit).<br><br>• An IDS is utilized to analyze network events and report possible or actual network security breaches.<br>• A firewall is in place to filter unauthorized inbound network traffic from the internet.<br>• The firewall system is configured to deny any type of network connection not explicitly authorized by a firewall system rule.<br>•The security groups are configured to filter traffic (inbound and outbound) and block unauthorized access to organizational Information, information assets and information processing facilities by adhering to a least-privilege model. Unnecessary ports shall not be allowed on the inbound access list. |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| | A.8.21 | | The Ivanti Cloud Operations team shall identify the security features, service levels and management requirements for all network services and include them as part of any network services agreement. Network services will be enabled based on a business “need-to-have” basis. CSC Team assesses the security risks associated with a network service before enabling it. Any unused or unwanted network service shall be removed or disabled. CSC Team shall assess the risks for cloud network services used and shall implement adequate controls to mitigate the identified risks. |
| **F.** Policy and procedure to assess the effectiveness of cybersecurity risk-management measures | 9.1 | Ivanti performs internal audit according to the ISO 27001:2022 standards. The management review is performed during the Security Council meetings. | To ensure that the identified security objectives are met, Ivanti evaluate the information security performance through well-defined metrics. The metrics are established to assess the effectiveness of the implemented Information Security Management System (ISMS).<br><br>To ensure the continuing suitability, adequacy and effectiveness of the compliance process, independent reviews are carried out. Multiple reviewsbeing performed in Ivanti are:<br><br>• Self-review by functions.<br>• Review by the compliance team reporting to the compliance manager.<br>• ISO27001, SOC2 audit by external auditors. |
| | 9.2 | | Ivanti’s Enterprise Security and Compliance team is responsible for conducting an independent internal verification and validation process to ensure the organization conforms to the specified Information security policies and procedures and relevant external requirements (customer, legal and regulatory requirements). |
| | 9.3 | | Enterprise compliance team will annually review ISMS implementation for its operational efficiency, continuing suitability, adequacy and effectiveness. results, then discuss/present to management/streeting committee annually or as needed. |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| **G.**PBasic cyber hygiene practices and cybersecurity training. | 7.3 | All employees of the organization receive appropriate awareness education, training and regular updates in organizational policies and procedures as relevant for their job function. Advantage Learning Dashboard displays the completed learning courses for each employee.<br><br>Rules to control physical and logical access to information are established and implemented based on business and information security requirements. The use of utility programs that can override system and application controls is restricted and tightly controlled.<br><br>Configurations, including security configurations, of hardware, software, services and networks are established, documented, implemented, monitored and reviewed. | Ivanti employees must take security awareness training upon hire and annually. ISMS training covers the importance of information security, the appropriate use of information and information processing facilities, expectations from employees and information security incident<br>reporting to minimize possible security risks. The training content is periodically reviewed and updated to ensure consistency with information security policies and procedures commensurate to employee roles and responsibilities. |
| | 7.4 | | Security and Compliance determines the need for internal and external communication with respect to information security. Depending on the situation, customer requirements or need, the communication objectives are identified, and the required communication content is developed. |
| | A.5.15 | | Ivanti uses role-based access control (RBAC) to ensure employees receive the least level of access privileges required to perform their jobs. Access is granted via security groups and elevated accounts in Active Directory. All system and user accounts are requested by an employee's manager or the Human Resources department and authorized and established through the IT department. Additional approvals may be required for contractors and consultants and for specific levels of access to some applications.<br><br>For new employees, a new access request is automatically generated when HR enters the employee in Workday. The request includes access required by the employee for the job role entered into the HRIS. Active directory accounts, permissions based on GPO and several other system accesses are automatically provisioned using automation scripts. The scripts ensure that all user accounts are unique, and employees are not allowed to share accounts. User IDs are based on the user's first and last name. A new employee checklist is used for action items that are not already automated. Any additional access must be requested by submitting a ticket in the ISM platform. |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| | A.5.16 | Backup copies of information, software and system images are taken and tested regularly in accordance with an agreed-upon backup policy.<br><br>Groups of information services, users and information systems are segregated on networks. | Ivanti uses role-based access control (RBAC) to ensure employees receive the least level of access privileges required to perform their jobs. Access is granted via security groups and elevated accounts in Active Directory. All system and user accounts are requested by an employee's manager or the Human Resources department and authorized and established through the IT department. Additional approvals may be required for contractors and consultants and for specific levels of access to some applications.<br><br>The organization uses Microsoft Active Directory as its logical access control system, and group policy objects (GPOs) are applied to users and computer groups. Multi-factor authentication (MFA) is used where available and required at a minimum for all external-facing service and for customer environments.<br><br>Active Directory Password Policy is enforced on all internal user accounts. Ivanti's password policy is developed in line with NIST 800-63B. Standard user accounts are required to have a password with a minimum of 15 characters, while administrator accounts are required to have 20 characters with complexity requirements enabled. |
| | A.5.18 | | Relevant stakeholders (information owners/information custodians) will review access rights for every employee in Ivanti Cloud Operations teams. The access rights of all employees shall be removed within 24 hours of an employee's termination. Access rights to cloud assets and Information shall be reviewed regularly in quarterly compliance reviews and updated as required. |
| | A.5.24 | | The Security Incidents Management team analyzes and classifies the incident as per the Incident Management Plan. The criticality of the affected resource (Ivanti and/or customer information assets, personnel and infrastructure) and the severity of impact of the event/incident will be prioritized based on incident classification.<br><br>This classification is helpful in prioritizing the response to events/incidents. Prioritization is determined by considering both the urgency of the Incident (how quickly the business needs a resolution) and the level of impact. An indication of impact is often (but not always) the number of users affected. In some cases, the loss of service to a single user can have a major business impact.<br><br>Based on the severity of impact, immediate steps shall be taken to minimize the impact of the event/incident, including implementation of commensurate compensating controls. |
| | A.6.3 | | Ivanti employees must take security awareness training upon hire and annually.<br><br>ISMS training covers the importance of Information security, the appropriate use of Information and Information processing facilities, expectations from employees and Information security incident reporting to minimize possible security risks. The training content is periodically reviewed and updated to ensure consistency with information security policies and procedures commensurate to employee roles and responsibilities. |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| | A.6.5 | | The HR team will notify relevant stakeholders (like IT, facilities administration, etc.) of transfer or separation of employees, trainees, vendors and contractors. The goal of the termination process is to ensure a professional, smooth transition for both the employee and the company. For the protection of both the company and the employee, it may be necessary to restrict access to files, email, etc., and to reclaim certain company property immediately upon termination. |
| | A.6.8 | | As soon as an employee encounters an information security event or incident, he/she shall report it to the Enterprise Security and Compliance team and/or the CSC Team. |
| | A.8.2 | | Ivanti uses role-based access control (RBAC) to ensure employees receive the least level of access privileges required to perform their jobs. Access is granted via security groups and elevated accounts in Active Directory. All system and user accounts are requested by an employee's manager or the Human Resources department and authorized and established through the IT department. Additional approvals may be required for contractors and consultants, and for specific levels of access to some applications. |
| | A.8.3 | | Ivanti uses role-based access control (RBAC) to ensure employees receive the least level of access privileges required to perform their jobs. Access is granted via security groups and elevated accounts in Active Directory. All system and user accounts are requested by an employee's manager or the Human Resources department and authorized and established through the IT department. Additional approvals may be required for contractors and consultants, and for specific levels of access to some applications.<br><br>The organization uses Microsoft Active Directory as its logical access control system, and group policy objects (GPOs) are applied to users and computer groups. Multi-factor authentication (MFA) is used where available and required at a minimum for all external-facing service and for customer environments. |
| | A.8.5 | | The organization uses Microsoft Active Directory as its logical access control system, and group policy objects (GPOs) are applied to users and computer groups. Multi-factor authentication (MFA) is used where available and required at a minimum for all external-facing service and for customer environments. Active Directory Password Policy is enforced on all internal user accounts. Ivanti's password policy is developed in line with NIST 800-63B. Standard user accounts are required to have a password with a minimum of 15 characters, while administrator accounts are required to have 20 characters with complexity requirements enabled. |
| | A.8.7 | | Ivanti has centralized antivirus software installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures, and it is configured to scan workstations continuously. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| | A.8.9 | | Ivanti maintains the secure information system and IS hardening standard documents, which the operations team follows via the change management process to ensure assets are configured in accordance with the documents. |
| | A.8.13 | | Ivanti information owners will ensure that all the essential business information is backed up at agreed-upon frequency and can be restored in case of an outage. Customer data is backed up utilizing the cloud provider's services. In the event of an exception, operations personnel will work with the cloud provider to re-establish services. Backup infrastructure resides on private networks logically secured from other networks.<br><br>**Azure:** Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.<br>Customer data is automatically replicated within Azure to minimize isolated faults. Azure services are configured to automatically restore<br>customer services upon detection of hardware and system failures.<br>**AWS:** Critical AWS system components are replicated across multiple availability zones, and backups are maintained. Backups of critical AWS system components are monitored for successful replication across multiple availability zones. |
| | A.8.15 | | Ivanti utilizes a centralized non-editable log collection tool (Splunk) for centralized monitoring of server and application logs. An SOC monitors events including, but not limited to, Windows security, application and system logs indicating use of privileged accounts, software installation, and changes to user permissions or privileges. Audit logs and security events shall be archived to assist in future investigations. |
| | A.8.19 | | Ivanti's Acceptable Use Policy prohibits employees from using pirated software or downloading pirated media on Ivanti technology. Penalties for non-compliance include termination. Only Ivanti-licensed software and media may be placed on Ivanti information resources, and Ivanti resources must never utilize company technology to engage in activity leading to copyright infringement of media or software. Software changes to the hosted Neurons Platform components must go through a strict change management process, and measures are in place to detect unauthorized software installation or changes on production systems. |
| | A.8.22 | | The internal and external network domains are segregated by defined security group rules using features available in cloud hosting platform.<br><br>The security groups are configured to filter traffic (inbound and outbound) and block unauthorized access to organizational Information, information assets and information processing facilities by adhering to least-privilege model. Unnecessary ports shall not be allowed on the inbound access list.<br><br>Networks are segregated based on the classification and value of information, access requirements and contractual requirements. |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| **H.** Policies and procedures regarding the use of cryptography and, where appropriate, encryption. | A.8.24 | Rules for the effective use of cryptography, including cryptographic key management, are defined and implemented.<br>Assets associated with information and information processing facilities are identified.<br><br>Background verification checks on all candidates for employment are carried out in accordance with relevant laws, regulations and ethics. It will be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.<br><br>All employees and external-party users will return all organizational assets in their possession upon termination of their employment, contract or agreement.<br><br>The contractual agreements with employees and contractors will state Ivanti's responsibilities for information security. | Passwords and production data are stored in an encrypted format using Advanced Encryption Standard (AES) encryption and configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority. |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| **I.** Human resources security, access control policies and asset management. | A.5.9 | Assets associated with information and information processing facilities are identified. | Information owners or information custodians will identify all information assets and maintain an inventory. The inventory shall be reviewed yearly and updated accordingly.<br><br>The inventory of cloud assets is maintained on the cloud service provider's console. |
| | A.5.10 | Background verification checks on all candidates for employment are carried out in accordance with relevant laws, regulations and ethics. It will be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.<br><br>All employees and external-party users will return all organizational assets in their possession upon termination of their employment, contract or agreement.<br><br>The contractual agreements with employees and contractors will state Ivanti's responsibilities for information security. | Ivanti has a well-defined Acceptable Use Policy. The objective of this policy is to ensure that Information and Information assets of Ivanti are used in an acceptable manner.<br><br>Employees will be made aware of the Acceptable Use Policy through Enterprise Security and Compliance training sessions and awareness campaigns.<br><br>The Acceptable Use Policy will be signed by employees upon hire and on an annual basis. Annual acknowledgment of Acceptable Use Policy shall be completed on talent advance learning portal by all employees. |
| | A.5.11 | | All Ivanti employees will return all information assets issued to them, such as laptops, keys, ID cards, access cards, software, data, documentation and manuals, on their last working day of separation from Ivanti. |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| | A.5.15 | | Ivanti uses role-based access control (RBAC) to ensure employees receive the least level of access privileges required to perform their jobs. Access is granted via security groups and elevated accounts in Active Directory. All system and user accounts are requested by an employee's manager or the Human Resources department and authorized and established through the IT department. Additional approvals may be required for contractors and consultants, and for specific levels of access to some applications. |
| | A.5.16 | | Ivanti uses role-based access control (RBAC) to ensure employees receive the least level of access privileges required to perform their jobs. Access is granted via security groups and elevated accounts in Active Directory. All system and user accounts are requested by an employee's manager or the Human Resources department and authorized and established through the IT department. Additional approvals may be required for contractors and consultants, and for specific levels of access to some applications.<br><br>The organization uses Microsoft Active Directory as its logical access control system, and group policy objects (GPOs) are applied to users and computer groups. Multi-factor authentication (MFA) is used where available and required at a minimum for all external-facing service and for customer environments.<br><br>Active Directory Password Policy is enforced on all internal user accounts. Ivanti's password policy is developed in line with NIST 800-63B. Standard user accounts are required to have a password with a minimum of 15 characters , while administrator accounts are required to have 20 characters with complexity requirements enabled. |
| | A.5.17 | | Ivanti has a well-defined password policy that defines good security practices in the selection and use of passwords. Employees are made aware of this policy through information security training sessions. Employees are not to disclose passwords to anyone. Employees are not to keep records (e.g., paper, electronic, etc.) of passwords. Passwords are considered confidential data and treated with the same discretion as any of the organization's proprietary Information. |
| | A.5.18 | | Relevant stakeholders (information owners/information custodians) will review access rights for every employee in Ivanti Cloud Operations teams. The access rights of all employees shall be removed within 24 hours of employee termination. Access rights to cloud assets and Information shall be reviewed regularly in quarterly compliance reviews and updated as required. |
| | A.6.1 | | Human Resources team performs background screening (BGC based on Ivanti) for associates through authorized/approved BGC vendors during the hiring process. During the hiring process flow, the BGC is initiated after the candidate accepts the offer. Candidate is onboarded after the BGC clears/completes. |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| | A.6.2 | | HR will ensure that all employees understand and sign the Non-Disclosure Agreement of Ivanti. The Ivanti Employee Policy Guide contains a code of conduct that must be acknowledged by newly hired Ivanti employees. Employees are made aware of the disciplinary action process as defined in The Ivanti Employee Policy Guide for any violation of organizational policies and procedures; any violation of the security responsibilities will lead to disciplinary actions. |
| | A.6.4 | | Ivanti has a formal disciplinary process in place that is documented as part of The Ivanti Employee Policy Guide. Ivanti will take appropriate action against any employee, agent or contractor whose actions are found to violate policy. Disciplinary actions may include, at the company's sole discretion: oral or written reprimand, suspension, immediate termination of employment or business relationship, or any other disciplinary action or combination of disciplinary actions as deemed appropriate to the circumstances. A record of the disciplinary action will be retained in the employee's file. |
| | A.6.5 | | The HR team will notify relevant stakeholders (IT, facilities administration, etc.) of transfer or separation of employees, trainees, vendors and contractors. The goal of the termination process is to ensure a professional, smooth transition for both the employee and the company. For the protection of both the company and the employee, it may be necessary to restrict access to files, email, etc., and to reclaim certain company property immediately upon termination. |
| | A.6.6 | | Non-Disclosure Agreements shall address the requirement to protect "Confidential" and "Private and Confidential" Information using legally enforceable terms. Ivanti NDAs are perpetual in nature and shall continue to apply beyond an employee's tenure with Ivanti.<br>All employees sign NDAs at time of hire as a part of The Ivanti Employee Policy Guide prior to accessing Ivanti information, information assets or information-processing facilities.<br><br>An NDA must be established between Ivanti and external parties before transmission of Ivanti confidential Information. |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| **J.** The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate. | A.5.14 | Ivanti has formal transfer policies, procedures and controls in place to protect the transfer of information through the use of all types of communication facilities. The ISMS Manual provides a detailed explanation.<br><br>Allocation and management of authentication information is controlled by a management process, including advising personnel on the appropriate handling of authentication information. Secure authentication technologies and procedures are implemented based on information access restrictions and the topic-specific policy on access control. | Exchange agreements will be established for the exchange of Information and software between the organization and external parties. The agreements will be in the form of MSA or NDA. All exchanges of information and software will be guided as per the contractual requirements.<br><br>When using company resources to access and use the internet, employees must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that “the opinions expressed are my own and not necessarily those of Ivanti.” |

| NIS 2 Control Article 21-Cyber Security Risk Management Measure | ISO 27001 Control | Response | Details per ISO Control |
|---|---|---|---|
| | A.5.16 | | Ivanti uses role-based access control (RBAC) to ensure employees receive the least level of access privileges required to perform their jobs. Access is granted via security groups and elevated accounts in Active Directory. All system and user accounts are requested by an employee's manager or the Human Resources department and authorized and established through the IT department. Additional approvals may be required for contractors and consultants, and for specific levels of access to some applications.<br><br>The organization uses Microsoft Active Directory as its logical access control system, and group policy objects (GPOs) are applied to users and computer groups. Multi-factor authentication (MFA) is used where available and required at a minimum for all external-facing service and for customer environments.<br><br>Active Directory Password Policy is enforced on all internal user accounts. Ivanti's password policy is developed in line with NIST 800-63B. Standard user accounts are required to have a password with a minimum of 15 characters, while administrator accounts are required to have 20 characters with complexity requirements enabled. |
| | A.5.17 | | Ivanti has a well-defined password policy that defines good security practices in the selection and use of passwords. Employees are made aware of this policy through Information security training sessions. Employees are not to disclose passwords to anyone. Employees are not to keep records (e.g., paper, electronic, etc.) of passwords. Passwords are considered confidential data and treated with the same discretion as any of the organization's proprietary Information. Employees shall adhere to the password policy, and noncompliance shall incur appropriate disciplinary actions. |

## About Ivanti

Ivanti elevates and secures Everywhere Work so that people and organizations can thrive. We make technology work for people, not the other way around. Today's employees use a wide range of corporate and personal devices to access IT applications and data over multiple networks to stay productive, wherever and however they work. Ivanti is the only technology company that finds, manages and protects every IT asset and endpoint in an organization. Over 40,000 customers, including 88 of the Fortune 100, have chosen Ivanti to help them deliver an excellent digital employee experience and improve IT and security team productivity and efficiency. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit ivanti.com



ivanti

For more information, or to contact Ivanti, please visit ivanti.com.