bluezone | integrated compliance fabric

SECURITY TECHNIQUES

ISO/IEC 27000 COMPLIANCE

REGULATORY ALIGNMENT BRIEF

Solve the complex challenges of sensitive data protection in compliance with ISO Information Security Management Systems standards.

/// BLUEZONE

MEET AND DEMONSTRATE ISO/IEC 27000 COMPLIANCE

ISO/IEC 27000 Background

Structured model of international standards for information security management.

ISO/IEC 27000 family of standards was prepared by a Joint Technical Committee (JTC) 1 of International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) governing a specialized system for worldwide standardization.

The committee developed a family of international standards for information security implementation and oversight, also known as Information Security Management Systems (ISMS). Through the use of the ISMS family of standards, organizations can design, implement and maintain a framework for managing the security of their information assets and prepare for an independent assessment of their technology environment applied to the protection of information, such as financial records, intellectual property, employee details or information entrusted to them by customers or third parties.

The ISMS standards define high-level requirements for cyber security management delivery and audit, provide direct support and interpretation for plan-do-check-act (PDCA) processes, address sector-specific guidelines and cover methods to validate ISMS conformance of the security framework.

The ISMS family of standards is intended to assist organizations of all types and sizes to develop a skill set in proven security techniques, and establish a discipline of following security best practices. Enabling accurate and complete information to be available in a timely manner to those with an authorized need is a catalyst for business efficiency. In addition, protecting information assets through information security management is essential to enable an organization to achieve its objectives, and maintain its legal compliance and image.

Specification Overview

Security techniques for improving the protection of information assets and managing risks.

ISO/IEC 27000 model incorporates features on which experts have reached a consensus as being the state of the art in information security. The model is continually updated to incorporate new guidelines based on the industry trends and innovation in the area of electronic information protection.

The ISMS family of standards is issued under a general title of *Information Technology – Security Techniques* and consists of the following specifications:

Standard	Description
ISO/IEC 27001	ISMS Requirements
ISO/IEC 27002	Code of Practice for Information Security Management
ISO/IEC 27003	ISMS Implementation Guidance
ISO/IEC 27004	ISMS Measurement
ISO/IEC 27005	Information Security Risk Management
ISO/IEC 27006	Requirements for Bodies Providing Audit and Certification of ISMS
ISO/IEC 27007	Requirements for ISMS Auditing
ISO/IEC 27008	Guidelines for Auditors on Information Security Controls
ISO/IEC 27011	Information Security Management Guidelines for Telecommunications
ISO/IEC 27017	Code of Practice for Information Security Controls for Cloud Computing
ISO/IEC 27018	Code of Practice for PII Protection in Public Cloud Acting as PII Processors
ISO/IEC 27799	Health Informatics – Information Security Management in Health

Analyzing the requirements for information security management, and applying appropriate controls to ensure the protection of critical assets, contributes to the successful implementation of a complete and resilient information security framework. The following fundamental principles also contribute to the successful implementation of an ISMS:

- Awareness of the need for information security
- Assignment of roles and responsibilities
- Incorporating management commitment and the interests of stakeholders
- Enhancing societal values
- Risk assessments determining appropriate controls to reach acceptable levels of risk
- Security incorporated as an essential element of information networks and systems
- Active prevention and detection of information security incidents
- Ensuring a comprehensive approach to information security management
- Continual reassessment of information security and making of modifications as appropriate

ISO/IEC deems information being an asset essential to an organization's business and, consequently, such that needs to be suitably protected. Information and communication technology is a key element in any organization, and assists in facilitating the creation, processing, storage, transmission and destruction of information. Where the extent of the interconnected global business environment expands, so does the requirement to protect information, as it is exposed to a wider variety of threats and vulnerabilities

Information security is achieved by implementing an applicable set of controls selected through the chosen risk management process and managed via an ISMS, including policies, processes, procedures, organizational structures, software and hardware to protect the identified information assets.

An effective ISMS uses a framework of resources to achieve an organization's objectives. In terms of information security, such framework allows to:

- Satisfy the security and privacy requirements of customers and other business stakeholders
- Improve an organization's plans and activities
- Meet the organization's information protection levels and improve critical data availability
- Comply with government regulations, legislation and industry mandates
- Manage information assets in an organized way that facilitates continual improvement and adjustment to the current business goals

Industry leading organizations design an information security program to implement ISMS requirements internally within their IT infrastructure, followed by a formal audit conducted by an Accredited Registrar (AR) to certify their ISMS compliance.

Regulatory Alignment

Protecting critical data with bluezone ensures simplified ISO/IEC 27000 compliance certification.

An industry-leading bluezone solution tremendously reduces the footprint of your critical private information, therefore minimizing compliance delivery costs and expediting the overall ISO/IEC 27000 certification process. The exposure of your sensitive digital assets is limited to the on-premise or hosted bluezone environment, eliminating your own information systems and applications from the scope of ISMS assessment.

The value of bluezone is tremendous in helping organizations implement effective ISMS requirements while meeting their ISO/IEC 27001 compliance, and is realized through the following built-in capabilities:

ISMS Requirement	Capabilities and Benefits
4.2 Establishing and Managing the ISMS	
4.2.1 Plan – Establish the ISMS	
a) Define the scope and boundaries of the ISMS in terms of characteristics of the business, the organization, its location, assets and technology.	♦ Substantially reduces the scope of unprotected information flow by encrypting, tokenizing and masking confidential electronic assets ♦ Diverts the threat of security attack away from de-identified data sources ♦ Provides justification for removing business applications from ISMS scope
c) Define the risk assessment approach of the organization.	♦ Promotes a data-centric security approach of devaluing sensitive data and making the overall risk assessment process manageable and efficient
d) Identify risks.	♦ Assists in identifying critical assets, threats and the impact of data loss ♦ Avoids the inherent risks of processing, transmitting or storing private data
e) Analyze and evaluate risks.	♦ Streamlines the process of risk level and impact evaluation ♦ Simplifies the definition of risk assessment criteria
f) Analyze and evaluate options for the treatment of risks.	♦ Applies risk mitigation controls via secure zone implementation ♦ Helps avoid risk and transfer responsibility outside of IT infrastructure
4.2.2 Do – Implement and Operate the ISMS	
c) Implement controls for the treatment of risks.	♦ Ensures secure access and safe communications when dealing with critical information, also reducing the effort to assess ISO/IEC 27001 compliance
f) Manage the ISMS operation.	♦ Reduces security operations to a small, controlled bluezone environment ♦ Provides options for internal and outsourced cloud service management
g) Manage the ISMS resources.	♦ Offers qualified security architecture, delivery and operations personnel ♦ Provides resources to ensure continuous improvement of ISMS effectiveness
h) Implement procedures and other control capable of enabling prompt detection of security events and response to security incidents.	♦ Provides audit trails unique to each bluezone environment component ♦ Provides alerting mechanisms for critical confidential data access events ♦ Integrates with external logging and monitoring management systems
4.2.3 Check – Monitor and Review the ISMS	
a) Execute monitoring and reviewing procedures and other controls to promptly detect errors, breaches and incidents.	♦ Automates detection of critical events and prevention of security incidents
b) Undertake regular reviews of the effectiveness of the ISMS taking into account results of security audits and incidents.	♦ Reduces the cost of recurring ISMS effectiveness reviews ♦ Groups, correlates and presents security events on a web-based dashboard
e) Conduct internal ISMS audits at planned intervals.	♦ Minimizes the scope of recurring internal ISMS audits and reviews ♦ Lowers the effort of audit management with third-party service providers

ISMS Requirement	Capabilities and Benefits
4.2.4 Act – Maintain and Improve the ISMS	
a) Implement the identified improvements in the ISMS.	♦ Supports gradual transition to de-identified data and continuous improvement of IT security and risk management levels
4.3 Documentation Requirements	
4.3.2 Control of Documents	
f) Ensure the documents are only available to those who need them, and are transferred, stored and ultimately disposed in accordance with procedures applicable to their classification.	♦ Ensures user and system access to sensitive documents is readily available, controlled and recorded for auditing and incident resolution activities ♦ Provides cost-effective, long-term document archiving capability
h) Ensure that the distribution of documents is controlled.	♦ Securely delivers sensitive electronic documents to authorized requestors without violating data owners' privacy rights
4.3.3 Control of Records	
Ensure protected and controlled maintenance of records, such as access logs and audit reports, in accordance with any relevant legal or regulatory requirements.	♦ Maintains information access logs for sustainable compliance ♦ De-identifies sensitive elements of audit reports and records for reviews ♦ Maintains records readily identifiable and retrievable for legal, regulatory, forensic investigation, customer service and other business purposes
5.2 Resource Management	
5.2.1 Provision of Resources	
a) Provide resources needed to implement, operate, monitor, review, maintain and improve the ISMS.	♦ Offers qualified personnel and supporting technology infrastructure for continuous bluezone operation, including hosted and on premise options
c) Identify and address legal and regulatory requirements and contractual security obligations.	♦ Simplifies partner and supplier contract management on the basis of automated security and privacy controls that prevent data exposure
d) Maintain adequate security by correct application of all implemented controls.	♦ Data protection measures are enforced by the bluezone implementation, where sensitive records are not circulated without de-identification
e) Carry out reviews when necessary and react appropriately to the results of these reviews.	♦ Minimize the scope and lower the effort of the ISMS effectiveness review
6 Internal ISMS Audits	
a) Conduct internal ISMS audits at planned intervals, to conform to the ISMS requirements and other legislation or regulations.	♦ Provides a solid foundation for the data-centric security implementation, inherently reducing the scope, frequency and effort of ISMS audits ♦ Delivers multiple regulatory compliance readiness at once, including PCI DSS, OSFI Cyber Security, FedRAMP, PII / PIPEDA and Common Criteria
b) As part of an internal ISMS audit, validate whether the control objectives, controls, processes and procedures conform to the identified information security requirements.	♦ Maintains security controls and operational procedures in compliance with the regulatory, industry and adopted corporate security requirements ♦ Small-footprint secure zone allows
c) As part of an internal ISMS audit, validate that the control objectives, controls, processes and procedures are effectively implemented and maintained.	♦ Small-footprint secure zone allows conducting organization-wide ISMS audits with high accuracy and minimal effort ♦ Provides runtime logs and archived records for effective audit reviews ♦ Supplies audit trail data to assist in running compliance reviews addressing IT systems and business applications outside of bluezone environment
8.1 Continual Improvement	

ISMS Requirement	Capabilities and Benefits
Continually improve the effectiveness of the ISMS through the use of the information security policy, information security objectives, audit results and analysis of monitored events.	♦ Re-purposes IT security effort towards constant service quality improvement ♦ Elevates ISMS effectiveness with a transition to the data-centric security, where information protection controls attached to the data itself ♦ Endorses a "zero trust" network with the risk-free data exchange between customers, partners, suppliers and controlling regulatory bodies
8.2 Corrective Action	
Take action to eliminate the cause of non-conformance with the ISMS requirements in order to prevent incident recurrence.	♦ Accelerates detection and analysis of non-conformance cases ♦ Reduces the extent and time of remediation measure delivery and testing
8.3 Preventive Action	
Determine action to eliminate the cause of potential non-conformance with the ISMS requirements in order to prevent initial occurrence of incidents.	♦ Prevents data theft via tokenization and de-identification of critical assets ♦ Creates a secure "bubble" around IT systems and communication channels ♦ Simplifies security event monitoring and incident management

In addition, the bluezone solution assists with achieving normative ISMS objectives and implementing the controls in accordance with the code of practice outlined in the ISO/IEC 27002 standard. The alignment with its guidelines and general principles is maintained through the following built-in capabilities:

ISMS Objective / Control	Capabilities and Benefits
4 Risk Assessment and Treatment	
4.1 Assessing Security Risks	
Define the scope and boundaries of the ISMS in terms of characteristics of the business, the organization, its location, assets and technology	♦ Assists in translating complex business processes and the associated interconnected systems to a simple and resilient security framework ♦ Significantly reduces the scope of security risk assessment down to a primary secure zone, where such process is practical, realistic and helpful
4.2 Treating Security Risks	
Implement controls for the treatment of risks	♦ Converts an organization's IT infrastructure to a safe digital space, where the risks can be knowingly and objectively accepted as per the security policy
5 Security Policy	
5.1 Information Security Policy	
5.1.1 Information security policy document	♦ Each hosted bluezone instance maintains a security policy which covers a complete set of ISMS objectives addressing physical and electronic access
5.1.2 Review of the information security policy	♦ Simplifies security policy reviews with a reduced span of private information capture, transmission, processing, storage and subsequent exposure
6 Organization of Information Security	
6.1 Internal Organization	
6.1.4 Authorization process for information processing facilities	♦ Centrally authorizes users and systems for access to confidential data ♦ Enforces role based access control (RBAC) for granting data related privileges
6.1.6 Contact with authorities	♦ Automates integration with law enforcement and supervisory authorities
6.1.8 Independent review of information security	♦ Reduces the scope and simplifies the procedures for independent internal and external reviews of ISMS implementation adequacy and effectiveness
6.2 External Parties	
6.2.1 Identification of risks related to external parties	♦ Provides secure channels of B2B integration and the related risk management ♦ Governs how sensitive information access is granted, verified and reported on

ISMS Objective / Control	Capabilities and Benefits
6.2.2 Assessing security when dealing with customers	♦ Simplifies processes for protecting organizational confidential assets and customer personal information retention according to privacy laws
7 Asset Management	
7.1 Responsibility for Assets	
7.1.1 Inventory of assets	♦ Assists in creating an inventory of important electronic assets
7.1.2 Ownership of assets	♦ Stimulates designated ownership, classification and protection of assets
7.1.3 Acceptable use of assets	♦ Helps enforce acceptable use of assets via access bluezone control
7.2 Information Classification	
7.2.1 Classification guidelines	♦ Assists in classifying information by sensitivity and criticality
7.2.2 Information labeling and handling	♦ Facilitates secure processing, transmission and storage of critical assets, combined with chain of custody and security event logging
9 Physical and Environmental Security	
9.1 Secure Areas	
9.1.1 Physical security perimeter	♦ Hosted bluezone instances are deployed in solid construction data centers ♦ Secure information processing is further encapsulated in bluegrid cabinets ♦ Data center facilities are equipped with motion sensors and video surveillance ♦ Security guards are available 24 x 7 to authorize access to monitor the site
9.1.2 Physical entry controls	♦ Entrance and departure of facility visitors is recorded by manned personnel ♦ All site visitors are required to pass through a man trap next to the reception ♦ Facility zones and cages are equipped with HID card readers and biometrics ♦ Site visitors are required to enter a PIN number in addition to the hand scan
9.1.3 Securing offices, rooms, and facilities	♦ Data center facilities give minimum indication of their purpose ♦ All hosted bluezone sites meet Tier 3 rating in accordance with TIA standards
9.1.4 Protecting against external and environmental threats	♦ Data center facilities provide minimum N+1 power and cooling redundancy ♦ HVAC equipment meets ASHRAE standards of safety and disaster recovery ♦ All data center sites are equipped with multiple diesel engine generators ♦ Appropriate fire fighting equipment is provided and suitably placed
9.1.5 Working in secure areas	♦ All working areas are monitored with CCTV cameras with video recorders ♦ Vacant secure areas and rooms are periodically inspected for authorized use
9.1.6 Public access, delivery, and loading areas	♦ Access to delivery areas and loading docks is controlled by security guards ♦ All incoming material is inspected for potential threats and registered
9.2 Equipment Security	
9.2.1 Equipment siting and protection	♦ Hosted bluegrid units are placed in smaller cages for further isolation ♦ Site temperature and humidity are automatically monitored and remediated
9.2.2 Supporting utilities	♦ HVAC, electricity and water supply provide redundancy and diversity
9.2.3 Cabling security	♦ Overhead cable tray systems provide security and interception protection
9.2.4 Equipment maintenance	♦ Only authorized personnel is allowed to carry out equipment maintenance
9.2.5 Security of equipment off-premises	♦ Hosted bluezone instances deliver superior, fully managed security service ♦ Any previously used devices are transported off-premise under supervision
9.2.6 Secure disposal or re-use of equipment	♦ Any sensitive data is removed from permanent storage prior to disposal ♦ Persistent data is rendered non-retrievable prior to physical media disposal
9.2.7 Removal of property	♦ Devices are not allowed to be taken off-site unless explicitly authorized
10 Communications and Operations Management	
10.1 Operational Procedures and Responsibilities	
10.1.1 Documented operating procedures	♦ Data center operation policies and procedures are available upon request ♦ Maintenance, recovery and incident handling procedures are documented

ISMS Objective / Control	Capabilities and Benefits
10.1.2 Change management	♦ Provides strict control over any changes to operational environment
10.1.3 Segregation of duties	♦ Fully supports segregation of duties to prevent critical asset misuse
10.1.4 Separation of development, test and operational facilities	♦ Provides full isolation of integration and production bluezone environments, including separate hardware infrastructure and operational procedures ♦ The rules for software provisioning to production systems are clearly defined
10.2 Third-party Service Delivery Management	
10.2.1 Service delivery	♦ Provides direct secure integration with partner networks and systems
10.2.2 Monitoring and review of third-party services	♦ Reduces the effort of third-party providers' security and compliance reviews ♦ Maintains bluezone components in compliance with the ISMS requirements
10.2.3 Managing changes of third-party services	♦ Minimizes the impact of partner service changes on IT systems via a service mediation gateway, which provides a level of indirection to partner interfaces
10.3 System Planning and Acceptance	
10.3.1 Capacity management	♦ Provides usage monitoring for key system resources, to ensure availability
10.3.2 System acceptance	♦ Purpose-built equipment simplifies acceptance and accreditation processes
10.5 Backup	
10.5.1 Information backup	♦ Includes shared storage tier with instant, off-node data backup capability
10.6 Network Security Management	
10.6.1 Network controls	♦ Maintains confidentiality and integrity of private data in transit
10.6.2 Security of network services	♦ Includes DMZ, NAT, firewall tier, VPN overlay and explicit traffic routing ♦ Provides private, cross-site VPLS connectivity between bluezone instances
10.7 Media Handling	
10.7.3 Information handling procedures	♦ Ensures secure means of data storage and transfer across any network ♦ Facilitates the distribution of data strictly on a need-to-know basis
10.7.4 Security of system documentation	♦ Provides de-identification and tokenization of sensitive document parts ♦ Offers archiving and controlled access to documents in secure storage
10.8 Exchange of Information	
10.8.4 Electronic messaging	♦ Provides masking and encryption of personal and system messaging
10.8.5 Business information systems	♦ Enables secure sharing of private data internally and with partners ♦ Prevents from vulnerability exploits of system communication channels
10.9 Electronic commerce services	
10.9.1 Electronic commerce	♦ Applies public key cryptography and digital signatures to e-commerce data
10.9.2 Online transactions	♦ Provides secure data routing, transmission and access authorization ♦ Ensures critical elements of online transactions are tokenized and encrypted
10.9.3 Publicly available information	♦ Prevents direct privileged access to publicly accessible service endpoints ♦ Includes web application firewall to protect public-facing web systems
10.10 Monitoring	
10.10.1 Audit logging	♦ Includes centralized logging facility to record critical security events
10.10.2 Monitoring system use	♦ Includes event management system to monitor and alert on security issues
10.10.3 Protection of log information	♦ Provides log file protection from tampering and unauthorized access
10.10.4 Administrator and operator logs	♦ Maintains audit trail of on-demand administrative access to secure zone ♦ Provides automated log monitoring for privileged access violations
10.10.5 Fault logging	♦ Exceptions are logged with time, context and root cause details

ISMS Objective / Control	Capabilities and Benefits
10.10.6 Clock synchronization	♦ Includes centralized NTP service to ensure bluegrid clock synchronization
11 Access control	
11.2 User Access Management	
11.2.2 Privilege management	♦ Enforces allocation of privileges on the need-to-know basis
11.2.3 User password management	♦ Passwords are stored encrypted in a centralized LDAP service facility ♦ Includes password policy management, such as locking, matching and aging
11.4 Network Access Control	
11.4.2 User authentication for external connections	♦ Uses passwords and certificates for secure outbound access to partner networks; similar access controls are applied to inbound requests
11.4.4 Remote diagnostic and configuration port protection	♦ Requires TLS transport for diagnostic and management access ♦ Supports configurable custom ports for enhanced operational security
11.4.5 Segregation in networks	♦ Operates segregated platform clusters in a private IP address space
11.4.6 Network connection control	♦ Network access is limited to trusted service consumer endpoints which present X.509 digital certificates to assert their identity
11.4.7 Network routing control	♦ Provides explicit secure routing at Layer 3 and traffic management at Layer 7
11.5 Operating System Access Control	
11.5.1 Secure logon procedures	♦ Requires password and certificate based logon to services and consoles
11.5.2 User identification and authentication	♦ Uniquely identifies users and systems accessing bluezone with the bundled identity management based on a centralized LDAP directory service
11.5.3 Password management system	♦ Passwords are checked for strength and kept in a centralized security store ♦ Temporary end-user passwords require reset at the initial use
11.5.4 Use of system utilities	♦ Excludes utilities that can override system and application control
11.5.5 Session time-out	♦ Administrative sessions automatically time out after a period of inactivity
11.5.6 Limitation of connection time	♦ Business service tokens are time-limited and require renewal upon expiration ♦ Administrative sessions require re-authentication after a maintenance period
11.6 Application and Information Access Control	
11.6.1 Information access restriction	♦ Requires access authorization to bluezone business and system services ♦ Access permissions are stored in a centralized LDAP directory service
11.6.2 Sensitive system isolation	♦ Provides completely isolated on-premise or hosted bluezone environment ♦ Supports system isolation within bluegrid via routing and containerization
12 Information Systems Acquisition, Development and Maintenance	
12.1 Security Requirements of Information Systems	
12.1.1 Security requirements analysis and specification	♦ Provides out-of-the-box security controls in support of ISMS requirements ♦ Delivers engineered systems that passed rigorous security evaluation
12.2 Correct Processing in Applications	
12.2.1 Input data validation	♦ Provides online or batch service request validation against schema
12.2.2 Control of internal processing	♦ Performs private data validation prior to tokenization or masking ♦ Alleviates the risk data entry corruption or unauthorized data modification
12.2.3 Message integrity	♦ Supports message encryption, hashing and digital signatures
12.2.4 Output data validation	♦ Provides online or batch service response validation against schema
12.3 Cryptographic Controls	
12.3.2 Key management	♦ Each trusted configured endpoint requires a set of unique keys ♦ Encryption keys are kept in a protected software key store (SKS) or an HSM

ISMS Objective / Control	Capabilities and Benefits
12.4 Security of System Files	
12.4.1 Control of operational software	♦ Embeds hardened and tested secure OS images on all bluegrid nodes ♦ Employs containerization to protect the underlying host-level infrastructure
12.4.2 Protection of system test data	♦ Uses only production-like test data, such as card numbers or IDs ♦ Copying and use of operational data for test purposes is not permitted
12.5 Security in Development and Support Processes	
12.5.1 Change control procedures	♦ Upgrades and patches to bluezone environment are subject to change control ♦ Reduces the impact of internal and partner system changes on IT operations
12.5.2 Technical review of applications after OS changes	♦ System-level patches and upgrades are subject to an end-to-end test cycle ♦ Only hardened and tested appliance images are provisioned to production
12.5.3 Restrictions on changes to software packages	♦ Provides signature verification of product packages for authenticity
12.5.4 Information leakage	♦ A locked-down bluezone environment provides de-identification and explicitly authorized re-identification of data to prevent information leakage
13 Information Security Incident Management	
13.1 Reporting information security events and weaknesses	
13.1.1 Reporting information security events	♦ Provides alerting for critical events, including security control violations ♦ Offers 24 × 7 secure zone support and rapid-fire incident response
14 Business Continuity Management	
14.1 Information Security Aspects of Business Continuity Management	
14.1.1 Including information security in the business continuity management process	♦ Delivers high availability and fault tolerance via bluegrid node redundancy ♦ Offers a multi-site deployment with an active-active service delivery
14.1.2 Business continuity and risk assessment	♦ Reduces probability and impact of business process interruption ♦ Facilitates expedient and controlled risk assessment process
14 Compliance	
15.1 Compliance with Legal Requirements	
15.1.3 Protection of organizational records	♦ Provides encryption, tokenization and masking of business critical records ♦ Offers record archiving for legal, regulatory and customer service purposes
15.1.4 Data protection and privacy of personal information	♦ Provides employee, customer and partner information privacy guards ♦ Conforms to PII, PIPEDA and other legislative or industry privacy rules
15.1.6 Regulation of cryptographic controls	♦ Uses military-grade cryptographic algorithms and processes approved by the government and industry supervision bodies
15.2 Compliance with Security Policies and Standards, and Technical Compliance	
15.2.1 Compliance with security policies and standards	♦ Expedites compliance delivery and audit of adherence to ISMS policies and information security standards
15.2.2 Technical compliance checking	♦ Minimizes the scope of recurring IT system assessments against the criteria of ISMS policies and information security standards
15.3 Information Systems Audit Considerations	
15.3.1 Information systems audit controls	♦ Minimizes the interference of ISMS audits with technology operations ♦ Provides built-in audit trail, alerting and access controls to support audits
15.3.2 Protection of information systems audit tools	♦ Provides read-only access to system logs for auditing purposes ♦ Offers cost-effective, long-term archiving of log records

ISO/IEC 27000 Solution Summary

Limit the exposure of sensitive data within or outside your organization IT infrastructure.

A unique, innovative bluezone solution reduces the footprint of business-critical private data, leaving only benign, non-sensitive information behind. A self-contained, engineered environment becomes your lightweight secure inter-connect, with privacy controls applied to sensitive data elements.

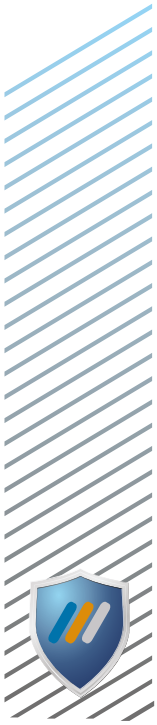
The solution allows you to centrally and uniformly manage any type of private data transfer, whether it is exchanged internally within your organization, or with your partners and customers involved in the automated business process flow. In a secure, integrated bluezone environment you can quickly and safely manage your cyber assets with minimal administration and maintenance effort. As a result, the cost and timeline to prepare for your ISO/IEC 27000 certification are significantly reduced.

Such substantial benefits have become possible due to a concept of capturing sensitive data at the network perimeter, preventing it from ever entering and "contaminating" the computing systems and network devices in your IT environment.

The encrypted and tokenized digital assets are no longer in the scope of ISMS compliance audit, or at risk of being lost or compromised. The complex business processes and inter-connected information systems no longer require redesign.

In the era of cloud computing having evolved as a model for enabling ubiquitous and convenient access to a pool of digital resources, the bluezone solution managed to combine both elasticity of the cloud and security of sensitive data. A "zero trust" approach, where the so called "trusted network" no longer exists, was laid in the foundation of a small-footprint data protection environment with access to components strictly on a need-to-know basis.

In a nutshell, your applications and infrastructure have been eliminated from the exposure to cyber-threat. The systems and processes that appeared on the ISMS conformance plan have been reduced to carefully engineered and validated zone, safely accessed regardless of who initiates the network communication and where it originates.



Reliable, simple, affordable. Certified.

An instance of the zone is powered by bluegrid, the industry's first integrated security system engineered to address the complexity and cost of ISO/IEC 27000, among other standards.

The compact, portable cloud service is based on a high-density component architecture covering network, servers, storage and applications which support large transaction volumes and carrier-grade communication throughput.

Every component of bluezone provides built-in redundancy to meet continuous service availability, fault tolerance and scalability. ISO/IEC 27000 conformance is now simple and sustainable.

Contact

Phone 1.888.414.5739
E-mail info@bluezonex.com
Web www.bluezonex.com

bluezone

10 Four Seasons Place, Fl. 10
Toronto, Ontario M9B 6H7