Using Ekran System for ISO/IEC 27001 compliance

The ISO 27000 family of standards helps organizations keep information assets secure.

Using this family of standards will help your organization to manage the security of assets such as financial information, intellectual property, employee details, or information entrusted to you by third parties.

ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).

Requirement	Description	How Ekran System helps you
A.6.1.2. Segregation of duties.	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Ekran System allows to control and audit activity of all users, including privileged users and server administrators. This greatly helps to find human errors and decreases the possibilities of internal misuse. Ekran System is integrated with Active Directory, so the solution will simply carry on with the existing permission model. Ekran System also has custom alerts feature that can track and notify when user accesses certain applications, helping to control segregation of duties.
A.6.2.2. Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Ekran System can monitor remote employee access or even teleworking workstations themselves to provide control over how data is accessed and used.
A.8.3.1. Management of removable media.	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Ekran System can detect USB devices and their type both on kernel and on user level and can send notifications when such device is connected. Option exists to automatically block any USB device.
A.9.2. User access management.	To ensure authorized user access and to prevent unauthorized access to systems and services.	Ekran System provides secondary user authentication before the start of the session, making sure that shared account users are clearly identified. Access to

		monitored workstation is constantly monitored.
A.9.2.3. Management of privileged access rights.	The allocation and use of privileged access rights shall be restricted and controlled.	Ekran System tracks all the activities of privileged users and it's practically impossible to avoid. You will be aware of any activity on the server, including user permission and account changes.
A.9.4. System and application access control.	To prevent unauthorized access to systems and applications.	With Ekran System you can control the access to the key systems and applications and detect if some non-authorized accounts access your assets. You can then immediately remotely block the user account.
A.10Cryptographic controls.	To ensure correct and secure operations of information processing facilities.	Partially, owing to recording all the types of privileged user sessions.
A.12.1.2. Change management.	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Ekran System provides a universal screen recording feature allowing every user action displayed on the screen to be recorded. By recording privileged user activity Ekran System allows to track and control all the changes made to the system.
A.12.4. Logging and monitoring.	To record events and generate evidence.	Ekran System is a universal logging tool for local, terminal, and remote sessions.
A.12.4.1. Event logging.	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Ekran System records user screens when working in terminal sessions, local and remote sessions. Based on the advanced technology of screenshot processing, this solution creates the complete searchable video records of everything that takes place on the screen of a computer. Thus, all of user activities can be easily reviewed anytime.
A.12.4.2. Protection of log information.	Logging facilities and log information shall be protected against tampering and unauthorized access.	All recorded data is stored at the server in the compressed format. Administrators can access these data via online Management Tool only in accordance with their permissions.
A.12.4.3. Administrator and operator logs.	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Ekran System records all user sessions, including privileged ones, allowing to control system administrator activity. All recorded data is stored at the server in the compressed format and can be easily analyzed. Ekran System also features an internal user log, recording

		actions of Management Tool user, allowing to review them later if necessary.
A.12.4.4. Clock synchronization.	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.	Ekran System automatically synchronizes all the time in the network with server time. Thus, the audit trails will be synchronized.
A.12.7.1 Information system audit controls.	Control - Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.	Ekran System does not require any changes to the network configuration or workflow to conduct user action recording. Recording process is non-intrusive with minimal impact on business processes.
A.13.2.1. Information transfer policies and procedures.	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Ekran System can record all user activity allowing to control data transfer procedures. It can also automatically optionally detect and block USB storage devices, preventing unauthorized data transfer via them,
A.15.2. Supplier service delivery management.	To maintain an agreed level of information security and service delivery in line with supplier agreements.	Partially, owing to tracking the actions of all privileged accounts, including the third party service providers.
A.15.2.1. Monitoring and review of supplier services.	Organizations shall regularly monitor, review and audit supplier service delivery.	Ekran System is a great solution to monitor, review and audit supplier service delivery. It provides full and detailed, replayable and searchable audit trails and reports to review the actions of the third party service provider accounts.
A.16.1. Management of information security incidents and improvements.	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	Partially. Ekran System creates the complete searchable video records of all user actions – that is clear and easy-to-analyze evidence for any incident.
A.16.1.7. Collection of evidence.	The organization shall define and apply procedures for the identification, collection, acquisition and preservation	Ekran System collects information independently from the clients and the servers, therefore it cannot be manipulated. All recorded data is stored at the server in the compressed format to

	of information, which can serve as evidence.	prevent manipulation or misuse. Data can be exported in a forensic format to guarantee that it was not altered in any way.

Using Ekran System for ISO 27011 compliance

The telecommunications sector standard, ISO 27011, based upon ISO 27002, provides guidelines and principles for initiating, implementing, maintaining, and improving information security management (ISM) within telecommunications organizations.

Standards objectives are to offer practical guidance especially suited for telecommunications organizations.

Requirement	Description	How Ekran System helps you
Clause 6. Organization of information security.	Establish a management framework to initiate and control the implementation of information security within the organization.	Ekran System is an insider threat detection and control tool. Video recordings produced by Ekran Systems can be used to analyze and control the implementation of security policy within the organization.
Clause 10. Communications and operations management.	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Ekran System permission system is integrated with Active Directory. You won't have to create and manage a separate user database for the Ekran System – the solution will simply carry on with the existing hierarchy. Ekran System also has custom alerts feature that can track and notify when user accesses certain applications, helping to control segregation of duties.
10.1 Operational procedures and responsibilities.	To ensure authorized user access and to prevent unauthorized access to systems and services.	Ekran System records server administrator sessions, so you will be aware of any activity on the server, including infrastructure setting changes, new accounts creation, etc. All server sessions are recorded – so if there are any unauthorized access session, it will be also logged. Ekran System also provides a secondary authentication option allowing to distinguish between users of a shared account and know exactly who had access to the system.
10.2 Third party service delivery management.	To implement and maintain the appropriate level of information security and	Ekran System is a great solution to monitor, review and audit supplier service delivery. It provides full and

	service delivery in line with third party service delivery agreements.	detailed, replayable and searchable audit trails and reports to review the actions of the third party service provider accounts.
10.10 Monitoring.	To detect unauthorized information processing activities.	Ekran System records all user sessions, including the privileged ones. By tracking all sessions, we are able to figure out whether unauthorized user sessions appeared or not as well as quickly detect unauthorized information processing activities using advanced search and instant alerts.
Clause 11. Access control.	Business requirement for access control, user access management, user responsibilities, network access control, operating system access control and information access control.	Ekran System records all the local, terminal and remote sessions. Thus you can track all user activities including system and permission management. In addition Ekran System provides integration with Active Directory. You won't have to create and manage a separate user database – the solution will simply carry on with the existing hierarchy. Ekran System also has custom alerts feature that can track and notify when user accesses certain applications, helping to control segregation of duties.
Clause 13. Information security incident management.	Reporting information security events, management of information security incidents and improvements Business continuity management.	Ekran System video records are a perfect tool to log any events, and even more – integrally log any event sequences. They can be used for analysis, as improvement logs, or as an evidence. Instant reporting is possible with alerts that can be customized to notify you upon certain specific events, allowing you to detect malicious activity and quickly respond to any potential issues.
13.2 Management of information security incidents and improvements.	To ensure a consistent and effective approach is applied to the management of information security incidents.	In order to manage security incidents Ekran System provides ability to review recorded activity, search episodes by various parameters, and set alerts to respond to them quickly. Besides, Ekran System provides you with an option to monitor all on-screen activity in real-time mode. After connecting to the "live" session you can see what is

		going on at this computer/session at the moment. Ekran System also allows you to immediately block malicious user sessions if needed. These features are a valuable addition to the incident management policies, which can be built around Ekran System.

Using Ekran System for Payment Card Industry Data Security Standard (PCI DSS) compliance

The PCI DSS is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.

Defined by the Payment Card Industry Security Standards Council, the standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure.

Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) that creates a Report on Compliance (ROC) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.

Requirement	Description	How Ekran System helps you
Requirement 8.1.1.	Assign all users a unique ID before allowing them to access system components or cardholder data.	Ekran System provides a secondary authentication feature allowing to assign a unique ID to every user.
Requirement 8.5.	Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: ■ Generic user IDs are disabled or removed. ■ Shared user IDs do not exist for system administration and other critical functions. ■ Shared and generic user IDs are not used to administer any system components	Ekran System employs a secondary authentication system that provides users with unique credentials that can be used to identify users attempting to log in via shared accounts.
Requirement 10.1.	Implement audit trails to link all access to system components to each individual user.	Ekran System carefully records all access to system components and clearly identifies it with a specific user name. Users of shared accounts can be identified by using the secondary authentication system.

Requirement 10.2.	Implement automated audit trails for all system components to reconstruct the following events: ■ 10.2.1. All individual user accesses to cardholder data ■ 10.2.2. All actions taken by any individual with root or administrative privilege. ■ 10.2.3. Access to all audit trails. ■ 10.2 5. Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges ■ 10.2.6. Initialization, stopping, or pausing of the audit logs ■ 10.2.7. Creation and deletion of system level objects	Ekran System records all activity during user session regardless of the application used. ■ Ekran System video recording can be used to monitor and control access to sensitive user data including cardholder data. ■ Ekran System records actions of privileged users including system administrators. Privileged user will not be able to pause or stop the recording. ■ All recorded data is stored at the server in the compressed format. Administrators can access these data only in accordance with their permissions. Every instance of such access is recorded in an internal user log. ■ By monitoring actions of privileged users Ekran System can be used to track any system changes including creation or removal of accounts and elevation of privileges. ■ Only users with explicit access to the Ekran System control panel can control the recording process. User, whose actions are being recorded cannot stop or pause the recording regardless of the level of privilege they possess. ■ By monitoring actions of privileged users Ekran System can be used to track and control creation and deletion of any system level objects.
Requirement 10.3.	Record at least the following audit trail entries for all system components for each event: ■ 10.3.1. User identification ■ 10.3.2. Type of event ■ 10.3.3. Date and time ■ 10.3.4. Success or failure indication ■ 10.3.5. Origination of event	Ekran System records all these data and other metadata. Besides being representative itself, each screenshot is supplemented with text metadata: active window title (full application name, document name, web site name, etc.), application name, user name, host name, session type, date and time.

	■ 10.3.6. Identity or name of affected data, system component, or resource.	
Requirement 10.4.	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time: ■ 10.4.1. Critical systems have the correct and consistent time. ■ 10.4.2. Time data is protected. ■ 10.4.3. Time settings are received from industry-accepted time sources.	Ekran System automatically synchronizes all the time in the network with server time. Thus the audit trails will be synchronized.
Requirement 10.5.1.	Limit viewing of audit trails to those with a job-related need.	Administrators can access recorded data only in accordance with their permissions.
Requirement 10.5.2.	Protect audit trail files from unauthorized modifications.	Partially. All recorded data is stored at the server in the compressed internal format and no tools for modifying it is provided. Administrators can access these data only in accordance with their permissions.
Requirement 10.5.3.	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	All recorded data is stored at the server in the compressed internal format and no tools for modifying it is provided. Any record can be exported and saved to the selected protected location.
Requirement 10.6.	Review logs and security events for all system components to identify anomalies or suspicious activity. Log harvesting, parsing, and alerting tools maybe used to meet this Requirement.	Ekran System records user screens when working in terminal sessions, local, and remote sessions. This solution creates the complete searchable video records that can be easily reviewed anytime. Ekran System also allows to perform search by various parameters. Real-time monitoring and alerting feature allows you to save time on searching a suspicious episode and perform a check as soon as suspicious actions are occurred.
Requirement 10.6.1.	Review the following at least daily:	Ekran System has a customizable alert feature that can be configured to send

	■ All security events ■ Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD ■ Logs of all critical system components Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	notifications upon certain events, allowing you to immediately react to potential security events as they happen. A number of customizable reports can also be generated for a quick daily review.
Requirement 10.7.	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	There is no time limits for Ekran System to store audit trails. Smart database management allows to manage used storage.

Using Ekran System for Australian Privacy Principle (APP) compliance

The Australian Privacy Principles (APPs) regulate the handling of personal information by Australian government agencies and some private sector organizations.

The 13 APPs are contained in schedule 1 of the Privacy Act 1988 (the Privacy Act).

The APPs cover the collection, use, disclosure and storage of personal information. They allow individuals to access their personal information and have it corrected if it is incorrect.

Requirement	Description	How Ekran System helps you
11.1.	If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss; and from unauthorized access, modification or disclosure.	Ekran System is an effective tool to control user activities. We provide you universal coverage for any Windows-based infrastructure. Based on the advanced technology of screenshot processing, this solution creates the complete searchable video records of everything that takes place on the screens along with the synchronized metadata and keylogs. Thus, Ekran System is a powerful tool for protecting from insider threats and sensitive data misuse.

Using Ekran System for EU Data Protection Directive 95/46/EC compliance

The Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) is a European Union directive adopted in 1995 which regulates the processing of personal data within the European Union. It is an important component of EU privacy and human rights law.

Requirement	Description	How Ekran System helps you
16. Confidentiality of processing.	Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data, must not process them except on instructions from the controller, unless he is required to do so by law.	Ekran System is a great solution to monitor, review and audit user activities. It provides detailed, replayable, and searchable audit trails and reports to review the user activities in the system. Thus, Ekran System can be used to make sure that no personal data is accessed or processed without authorization.
17.1. Security of processing.	Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.	Ekran System is internal threat detection and prevention tool that can work on servers and end-points with any network protocol, application, and even for all types of architecture (AD or non-AD users). With Ekran System, you can control any access and actions to and performed with personal data. Advanced search feature gives you an effective tool to perform retrospective user action analysis and incident investigation. Alerts feature can notify your security personal about malicious actions as they happen and user can then be immediately blocked if needed.

Using Ekran System for Data Protection Principles (DPP) of the Personal Data (Privacy) Ordinance compliance

The Ordinance came into force on 20 December 1996. It applies to any person who collects, holds, processes and uses personal data within the private and public sectors as well as government departments. Generally speaking, the Ordinance governs the ways of collecting and using personal data, and prevents any abuse of data that is considered as intruding on an individual's privacy.

Under current statutory and common law in the Hong Kong SAR, only personal data is protected under the Ordinance.

Requirement	Description	How Ekran System helps you
DPP4.	All practicable steps shall be taken to ensure that personal data are protected against unauthorized or accidental access, processing or erasure.	Based on the advanced technology of screenshot processing, Ekran System creates a complete video records of everything that takes place on the screens during local, remote, and terminal sessions. Relevant metadata, such as active window title, application name, pressed keystrokes, visited URLs, etc., are also recorded. Security personal can easily analyze these recordings and search them by various parameters. Real-time monitoring and alerting feature allows you to detect an incident while it happens and issue an immediate response.

Using Ekran System to comply with HIPAA (Health Insurance Portability and Accountability Act)

The Health Insurance Portability and Accountability Act, also known as the Kennedy-Kassebaum Act or Kassebaum-Kennedy Act, was enacted by the United States Congress and signed by the president in 1996.

Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

Requirement	Description	How Ekran System helps you
160.308	Compliance reviews	Compliance auditors can easily access and analyze monitoring results in several ways: ■ Replay searchable video records of all user actions and perform advanced search, as audit trails are supplemented with appropriate text metadata like active application name, currently opened window title, URL address, keystrokes, etc. ■ Analyze reports that contain information on user activity (including alert events and visited URLs) in different formats: grid reports, summary reports, and chart reports. They can be generated on a daily, weekly, or monthly basis and sent via email at the specified time, or they can be generated manually at any time for any time period.
164.306	Security standards	Ekran System provides complete monitoring of all user activity, allowing to track all operations with protected information and detect suspicious behavior. Customizable alert feature allows to detect suspicious incident in real time with an ability to watch the

		session live and block the user access remotely if needed. Ekran System can also optionally detect and block USB devices, allowing to prevent data leaks via USB mass storages. Ekran System is reliable security solution for controlling, detecting and preventing insider threats.
164.308	Administrative Safeguards	Ekran System provides a secondary authentication feature allowing to assign additional credentials to all users. This allows to clearly identify users of shared accounts and thoroughly and precisely control information access.
164.312	Technical Safeguards	Based on the advanced technology of screenshot processing, Ekran System creates a complete video records of everything that takes place on the screens during local, remote, and terminal sessions. Relevant metadata, such as active window title, application name, pressed keystrokes, visited URLs, etc., are also recorded. Security personal can easily analyze these recordings and search them by various parameters. Real-time monitoring and alerting feature allows you to detect an incident while it happens and issue an immediate response.