Kriptone

Ekran System
User activity videorecording system

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 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. Internal organization.	To establish a management framework to initiate and control the implementation and operation of information security within the organization.	Partially. Based on the advanced technology of screenshot processing, Ekran System creates the complete video records of everything that takes place on the screens in the network – so you can control the implementation and daily operation of your information security strategy.
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.
A.9.2. User access management.	To ensure authorized user access and to prevent unauthorized access to systems and services.	Partially. As Ekran System records all sessions with the user name/host name information, you are able to figure out whether suspicious user sessions appeared on you hosts or not, all user accounts are legally registered or not.
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.9.2.6. Removal or adjustment of access rights.	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Ekran System records all user sessions, including the privileged ones. With it, you are able to control that all access rights/accounts were removed and timely detect some illegal user sessions to appear.
A.9.4. System and application access control.	To prevent unauthorized access to systems and applications.	Partially, with Ekran System you can control the access to the key systems and applications and detect if some non-authorized accounts access your assets.
A.9.4.1. Information access restriction.	Access to information and application system functions shall be restricted in accordance with the access control policy.	There is a role-based permission model in Ekran System, and integration with Active Directory is also provided. As for the corporate application systems you can track any activity regardless of application type.
A.12.1. Cryptographic 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's screen recording system is universal, because every user action performed is displayed on the screen, and thus will be recorded. As Ekran System records privileged user activity, all the changes to the system made by them will be tracked.
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 screens of the computers in the network. 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 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 the privileged ones, so activities of administrators are under control. All recorded data is stored at the server in the compressed format and can be easily analyzed.
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.13.1. Network security management.	To ensure the protection of information in networks and its supporting information processing facilities.	Partially. We provide you universal monitoring coverage for any Windows-based infrastructure; Ekran System works for any network protocol.
A.13.1.1. Network controls.	Networks shall be managed and controlled to protect information in systems and applications.	While many network monitoring systems can be evaded, or don't cover all the scopes and types of user activity, the Ekran System's screen recording system is universal, because every user action performed is displayed on the screen, and thus will be recorded. Ekran System can also monitor the terminal connections used to access networking devices for any network protocol.
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 of information, which can serve as evidence.	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 prevent manipulation or misuse. Any record can be exported to the external video-format to provide it to the third-party experts.

Using Ekran System for ISO 27011 compliance

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

Its 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 essential tool to control all user actions in the network. Security department can create a policy around Ekran System: users and physical machines to be monitored, a set of norms for regular or incident-based replay of recorded sessions. Analyzing records, you can also monitor implementation of information security 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.

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.
10.2 Third party service delivery management.	To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.	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.
10.10 Monitoring.	To detect unauthorized information processing activities.	Ekran System records all user sessions, including the privileged ones. As we are tracking all the sessions, we are able to figure out whether unauthorized user sessions appeared or not as well as quickly detect in there were some illegal information processing activities – using keyword-based 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.
Clause 13. Information security incident management.	Reporting information security events, management of information security incidents and improvements Business continuity management.	Ekran System records are perfect tool to log any events, and even more – integrally log any event sequence. They can be considered as analysis materials, improvement logs or evidencesInstant reporting is possible with alerts - the events that notify you of specific activity (potentially malicious/prohibited actions), and allow you to respond to them quickly without performing the search.
13.2 Management of information	To ensure a consistent and effective approach is applied	In order to manage security incidents Ekran System provides a possibility to

security incidents and improvements.	to the management of information security incidents.	review recorded activity, search for episodes by keywords, and set alerts to respond to them quickly. Besides, Ekran System provides you with an option to monitor screens of the computers in the network in real-time mode. After connecting to the "live" session you can see what is going on at this computer/session at the moment. 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 2.2.1.	Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, webservers, database servers, and DNS should be	Ekran System can be installed on any terminal server for controlling particular type of functions, and being integrated with Active Directory, supports the existent security permissions.

	implemented on separate servers.) Where virtualization technologies are in use, implement only one primary function per virtual system component.	
Requirement 2.3.	Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	While controlling your servers and end-points including all administrative sessions on them, Ekran System uses agent-server encryption to protect monitored data travelling in the network.
Requirement 10.1.	Implement audit trails to link all access to system components to each individual user.	Ekran System carefully records any session of access to the system components catching user name. Association of usernames with anonymous “administrator” login will be included to Ekran System 3.1
Requirement 10.2.	Implement automated audit trails for all system components to reconstruct the following events.	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.
Requirement 10.2.2.	All actions taken by any individual with root or administrative privilege.	Ekran System helps to control and audit the remote access of administrators to the protected servers. The recorded audit trails can be replayed like a movie to review the events exactly as they occurred. Every action of the administrators is visible in the audit trail.
Requirement 10.2.3.	Access to all audit trails.	All recorded data is stored at the server in the compressed format. Administrators can access these data only in accordance with their permissions.
Requirement 10.2.6.	Initialization, stopping, or pausing of the audit logs.	Ekran System is a transparent system, independent from the clients and the audited servers. The users of the remote servers do not need to have accounts on Ekran System, only users with explicit access to Ekran System can control the auditing.

Requirement 10.2.7.	Creation and deletion of system-level objects.	Commonly only privileged users can perform such operations, and their activity is audited.
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 ■ 10.3.6 Identity or name of affected data, system component, or resource.	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.
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. One example of time synchronization technology is Network Time Protocol (NTP).	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 to the AVI’format 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,	Ekran System records user screens when working in terminal sessions, local, and remote sessions. This solution creates the complete searchable video records of everything that takes place on

	parsing, and alerting tools maybe used to meet this Requirement.	the screens of the computers in the network. Thus, all of user activities can be easily reviewed anytime. Ekran System also provides searching events by keywords. Real-time monitoring and alerting feature allows you to save time on searching a suspicious episode and check it out as soon as it occurs.
Requirement 10.6.1.	Review the following at least daily: ■ 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.).	Ekran System is built around keyword-indexed video that is the most powerful and clear way to represent findings, and is very easy to analyze. Using search options, you can promptly get logs for a selected system component or activity.
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.
Requirement 12.5.5.	Monitor and control all access to data.	Ekran System provides a way to control and audit access to data throughout remote servers and local end-points, any network protocols, architectures, and applications. As we are tracking all the sessions, we are also able to figure out whether unknown or illegal user sessions appeared or not.

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.	In order to protect information Ekran System provides possibility to control all the 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 of the computers in the network accompanied with the synchronized metadata and keylogs. Thus, we give you a powerful tool not only for session recording, but also for performing keyword search.

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.
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 a universal tool to work on servers and end-points, any network protocol, application, even for all types of architecture (AD or non-AD users). With Ekran System, you can control any session of work with personal data. Keyword-based search gives you an effective tool to perform retrospective user action analysis and incident investigation. At the same time, due to its flexible licensing scheme and beneficial pricing, Ekran System can save your security budget.

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 the complete video records of everything that takes place on the screens of the computers in the network during local, remote, and terminal sessions under any network protocol. The solution records also metadata - such as active window title, application name, etc. - and logs all keystrokes i.e. records all text typed by user at keyboard including chat/web messages, emails, documents, passwords and other. Due to this, administrator can search for the episodes by keywords and replay all sessions of work with sensible data. Real-time monitoring and alerting feature allows you to save time on searching a suspicious episode and check it out as soon as it occurs.