EKRAN®

USING EKRAN SYSTEM TO ENSURE ISO/IEC 27001 COMPLIANCE

Using Ekran System for ISO/IEC 27001 compliance

The International Organization for Standardization (ISO) 27000 family of standards helps organizations keep information assets secure. Recommendations provided in these standards help you improve the security of financial information, intellectual property, employees' personal data, and information entrusted to you by third parties.

ISO 27001 is the best-known standard in the family, providing requirements for information security management systems (ISMS).

Ekran System is a full-cycle insider threat management platform that effectively deters, detects, and disrupts insider threats. It's an all-in-one insider threat protection platform that allows you to detect and respond to security threats. Ekran System functionality covers many ISO 27001 controls as well as other cybersecurity compliance requirements.

Let's see which ISO 27001 requirements you can meet by deploying Ekran System:

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 you to control and audit the activity of all users, including privileged users and server administrators. This greatly helps in finding human errors and decreases the possibility of privilege misuse. Ekran System can be integrated with Active Directory, so it can easily work with your existing permission model. Ekran System also allows you to set custom alerts for detecting every attempt to access a certain application, thus helping to control the 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 monitors remote employee access and even teleworking workstations 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 types at both the kernel and user levels and send notifications to security officers when a USB device is connected. You can create a white list of allowed USB devices and Ekran System will automatically block any device not on that list.
A.9.1.2. Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Ekran System ensures granular access management by defining access rights for each user. It's also possible to create user roles for groups of employees with similar permissions, grant access manually, and enforce time restrictions.
A.9.2.3. Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	Ekran System provides the possibility to grant privileged access rights to a user, change permissions at any time, and monitor, audit, and review the activity of privileged users. It's also possible to create temporary credentials for privileged users and define the endpoints and resources they can access.
A.9.2.4. Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	Ekran System uses a built-in password manager to handle secrets and credentials required for user authentication. This password manager ensures secure creation, delivery, storage, rotation, and termination of secrets. To secure the data in its password manager, Ekran System uses FIPS 140-2 compliant encryption algorithms
A.9.2.5. Review of user access rights	Asset owners shall review users' access rights at regular intervals.	Ekran System collects context-rich recordings in the form of screen activity logs indexed with metadata on user actions (accessed files, folders, URLs, executed commands, connected devices, etc.). It's easy to review these logs in a built-in YouTube-like video player, and you can search for events by various parameters.

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.	Granting, reviewing, and terminating user access rights in Ekran System takes just a couple of clicks. You can also assign users with temporary access rights.
A.9.4. System and application access control	Prevent unauthorized access to systems and applications.	With Ekran System, you can control access to any systems and applications. If an unauthorized account tries to access your assets, you'll get a notification. Then you can remotely block this account without delays, or Ekran System can do so on its own.
A.9.4.1. Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	Ekran System allows you to define user roles, specifying which resources users with these roles can access. It also allows you to manually configure personalized access rights for each user.
A.9.4.2. Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	The monitoring functionality of Ekran System logs each user action, including attempts to access systems and applications. These logs are encrypted and stored on Ekran System Server and can be exported in a protected format.
A.9.4.3. Password management system	Password management systems shall be interactive and shall ensure quality passwords.	Ekran System's own password manager securely handles user credentials at all stages, from creation to termination.
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 universal screen recording functionality that logs each user action. By recording the activity of privileged users, Ekran System allows you to track and control all changes made to your information processing system.
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 and audio input/output in terminal, local, and remote sessions. Based on advanced screenshot processing technology, it

		creates complete searchable video records of everything that takes place on the screen of a monitored computer. Thus, all user activities can easily be reviewed.
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 encrypted and stored on Ekran System Server. Only administrators with relevant permissions can access this data via the online Management Tool.
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 sessions of privileged users, logging all actions of system administrators. These logs include administrator activity in Ekran System Client and the Management Tool. All recorded data is stored on the Ekran System Server in a protected format and can be exported for forensic analysis.
A.15.2.1. Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	Ekran System allows you to monitor third parties, recording and reviewing their activity within your infrastructure.
A.16.1.2. Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	With Ekran System, you can generate periodic or ad hoc reports on user activity, productivity, accessed URLs, commands, keystrokes, alerts, and much more. Reports can be generated in multiple formats and customized with your company credentials.
A.16.1.4. Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Ekran System collects activity logs and provides a built-in player to review them and to search for specific incidents using lots of log parameters. With these tools, you can analyze each action, establish its context, and determine the threat level.
A.16.1.5. Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Ekran System relies on predefined and user-generated alerts to detect security violations. When an alert is triggered, the

		software notifies security officers about this event and provides a link to the session. Following this link, officers can evaluate the threat and block the session or the user if needed. Also, Ekran System can automatically respond to critical incidents by blocking users and processes automatically.
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 from monitored endpoints and stores it on its servers. All recorded data is stored on the server in an encrypted format to prevent any manipulations or misuse. Data can be exported in a forensic format for further analysis.

GET MORE DETAILS

Contact us

General inquiries: info@ekransystem.com
Partner program: partner@ekransystem.com

www.ekransystem.com

Ekran System®