EKRAN®

NUTZEN SIE EKRAN SYSTEM ZUR SICHERSTELLUNG DER ISO/IEC 27001-COMPLIANCE

Nutzen Sie Ekran System zur Sicherstellung der ISO/IEC 27001-Compliance

Die Normenfamilie der International Organization for Standardization (ISO) 27000 hilft Organisationen dabei, Informationsressourcen sicher zu halten. Die in diesen Standards enthaltenen Empfehlungen helfen Ihnen, die Sicherheit von Finanzinformationen, geistigem Eigentum, personenbezogenen Daten von Mitarbeitern und Informationen, die Ihnen von Dritten anvertraut wurden, zu verbessern.

ISO 27001 ist der bekannteste Standard in der Familie und bietet Anforderungen an Informationssicherheits-Managementsysteme (ISMS).

Ekran System ist eine vollumfängliche Plattform für das Management von Insider-Bedrohungen, die Insider-Bedrohungen effektiv erkennt, verhindert und stört. Es handelt sich um eine All-in-One-Plattform zum Schutz vor Insider-Bedrohungen, mit der Sie Sicherheitsbedrohungen erkennen und darauf reagieren können. Die Funktionen von Ekran System decken viele ISO 27001-Kontrollen sowie andere Anforderungen zur Einhaltung der Cybersicherheit ab. Verfolgen Sie, welche ISO 27001-Anforderungen Sie durch die Bereitstellung von Ekran System erfüllen können:

Anforderung	Beschreibung	Wie Ekran System bei der Einhaltung hilft
A.6.1.2. Aufgabentrennung	Widersprüchliche Aufgaben und Verantwortungsbereiche sind zu trennen, um die Möglichkeit einer nicht autorisierten oder unbeabsichtigten Änderung oder eines Missbrauchs der Vermögenswerte der Organisation zu verringern.	Mit Ekran System können Sie die Aktivitäten aller Benutzer steuern und überwachen, einschließlich privilegierter Benutzer und Serveradministratoren. Dies hilft beim Auffinden menschlicher Fehler erheblich und verringert die Möglichkeit des Missbrauchs von Privilegien. Ekran System kann in Active Directory integriert werden, sodass es problemlos mit Ihrem vorhandenen Berechtigungsmodell verwendet werden kann. Mit Ekran System können Sie auch benutzerdefinierte Warnungen festlegen, um jeden Versuch, auf eine bestimmte Anwendung zuzugreifen, zu erkennen und

		so die Aufgabentrennung zu steuern.
A.6.2.2. Telearbeit	Eine Richtlinie und unterstützende Sicherheitsmaßnahmen sind umzusetzen, um Informationen zu schützen, auf die an Telearbeitsplätzen zugegriffen, diese verarbeitet oder gespeichert werden.	Ekran System überwacht den Remotezugriff der Mitarbeiter und sogar die Telearbeitsplätze, um zu steuern, wie auf Daten zugegriffen und wie diese verwendet werden.
A.8.3.1. Verwaltung von Wechselmedien	Die Verfahren für die Verwaltung von Wechselmedien sind gemäß dem von der Organisation festgelegten Klassifizierungsschema durchzuführen.	Ekran System kann USB-Geräte und deren Typen sowohl auf Kernel- als auch auf Benutzerebene erkennen und Benachrichtigungen an Sicherheitsbeauftragte senden, wenn ein USB-Gerät angeschlossen ist. Sie können eine weiße Liste der zulässigen USB-Geräte erstellen, und Ekran System blockiert automatisch alle Geräte, die nicht in dieser Liste enthalten sind.
A.9.1.2. Zugang zu Netzwerken und Netzwerkdiensten	Benutzer erhalten nur Zugriff auf das Netzwerk und die Netzwerkdienste, für deren Nutzung sie ausdrücklich autorisiert wurden.	Ekran System stellt eine detaillierte Zugriffsverwaltung sicher, indem Zugriffsrechte für jeden Benutzer definiert werden. Es ist auch möglich, Benutzerrollen für Gruppen von Mitarbeitern mit ähnlichen Berechtigungen zu erstellen, den Zugriff manuell zu gewähren und Zeitbeschränkungen durchzusetzen.
A.9.2.3. Verwaltung privilegierter Zugriffsrechte	Die Zuweisung und Nutzung von privilegierten Zugriffsrechten erfolgen eingeschränkt und kontrolliert.	Ekran System bietet die Möglichkeit, einem Benutzer privilegierte Zugriffsrechte zu gewähren, Berechtigungen jederzeit zu ändern und die Aktivitäten privilegierter Benutzer zu überwachen, zu auditieren und zu überprüfen. Es ist auch möglich, temporäre Anmeldeinformationen für privilegierte Benutzer zu erstellen und die Endpunkte und Ressourcen zu definieren, auf die sie zugreifen können.

A.9.2.4. Verwaltung geheimer Authentifizierungsinformationen von Benutzern	Die Zuweisung geheimer Authentifizierungsinformationen ist durch einen formellen Verwaltungsprozess zu kontrollieren.	Ekran System verwendet einen integrierten Passwort-Manager, um die für die Benutzerauthentifizierung erforderlichen Geheimnisse und Anmeldeinformationen zu verarbeiten. Dieser Passwort-Manager gewährleistet die sichere Erstellung, Zustellung, Speicherung, Rotation und Beendigung von Geheimnissen. Um die Daten in seinem Passwort-Manager zu sichern, verwendet Ekran System FIPS 140-2-kompatible Verschlüsselungsalgorithmen.
A.9.2.5. Überprüfung der Benutzerzugriffsrechte	Die Eigentümer von Vermögenswerten überprüfen in regelmäßigen Abständen die Zugriffsrechte der Benutzer.	Ekran System sammelt kontextreiche Aufzeichnungen in Form von Bildschirmaktivitätsprotokollen, die mit Metadaten zu Benutzeraktionen indiziert sind (abgerufene Dateien, Ordner, URLs, ausgeführte Befehle, verbundene Geräte usw.). Es ist einfach, diese Protokolle in einem integrierten YouTube-ähnlichen Videoplayer zu überprüfen, und Sie können anhand verschiedener Parameter nach Ereignissen suchen.
A.9.2.6. Entfernung oder Anpassung von Zugriffsrechten	Die Zugriffsrechte aller Mitarbeiter und externen Benutzer auf Informationen und Informationsverarbeitungseinrichtungen sind nach Beendigung ihres Arbeitsverhältnisses, Abkommens oder Vertrags zu entfernen oder bei Änderung anzupassen.	Das Gewähren, Überprüfen und Beenden von Benutzerzugriffsrechten in Ekran System erfordert nur wenige Klicks. Sie können Benutzern auch temporäre Zugriffsrechte zuweisen.
A.9.4. System- und Anwendungs zugriffskontrolle	Der unbefugte Zugriff auf Systeme und Anwendungen ist zu verhindern.	Mit Ekran System können Sie den Zugriff auf alle Systeme und Anwendungen steuern. Wenn ein unbefugtes Konto versucht, auf Ihre Assets zuzugreifen, erhalten Sie eine Benachrichtigung. Dann können Sie dieses Konto ohne Verzögerungen remote blockieren, oder Ekran System kann dies von selbst tun.

A.9.4.1. Einschränkung des Informations zugriffs	Der Zugang zu Informationen und Funktionen des Anwendungssystems ist gemäß der Zugriffssteuerungsrichtlinie einzuschränken.	Mit Ekran System können Sie Benutzerrollen definieren und angeben, auf welche Ressourcen Benutzer mit diesen Rollen zugreifen können. Außerdem können Sie personalisierte Zugriffsrechte für jeden Benutzer manuell konfigurieren.
A.9.4.2. Sichere Anmeldeverfahren	Sofern die Zugriffssteuerungsrichtlinie dies erfordert, muss der Zugriff auf Systeme und Anwendungen durch ein sicheres Anmeldeverfahren kontrolliert werden.	Die Überwachungsfunktion von Ekran System protokolliert jede Benutzeraktion, einschließlich der Versuche, auf Systeme und Anwendungen zuzugreifen. Diese Protokolle werden verschlüsselt und auf Ekran System Server gespeichert und können in einem geschützten Format exportiert werden.
A.9.4.3. Passwortverwaltungssystem	Passwortverwaltungssysteme müssen interaktiv sein und qualitativ hochwertige Passwörter sicherstellen.	Der Passwort-Manager von Ekran System verwaltet Benutzeranmeldeinformationen in allen Phasen, von der Erstellung bis zur Beendigung, sicher.
A.12.1.2. Änderungsmanagement	Änderungen an Organisation, Geschäftsprozessen, Informationsverarbeitungseinrichtungen und Systemen, die sich auf die Informationssicherheit auswirken, sind zu kontrollieren.	Ekran System bietet universelle Bildschirmaufzeichnungsfunktionen, die jede Benutzeraktion protokollieren. Durch Aufzeichnen der Aktivitäten privilegierter Benutzer können Sie mit Ekran System alle an Ihrem Informationsverarbeitungssystem vorgenommenen Änderungen verfolgen und steuern.
A.12.4.1. Ereignisprotokollierung	Ereignisprotokolle, in denen Benutzeraktivitäten, Ausnahmen, Fehler und Informationssicherheitsereignisse aufgezeichnet sind, müssen erstellt, aufbewahrt und regelmäßig überprüft werden.	Ekran System zeichnet Benutzerbildschirme und Audioeingabe/-ausgabe in Terminal-, lokalen und Remote-Sitzungen auf. Basierend auf der fortschrittlichen Screenshot-Verarbeitungstechnologie werden vollständige durchsuchbare Videoaufzeichnungen von allem erstellt, was auf dem Bildschirm eines überwachten Computers stattfindet. Somit können alle Benutzeraktivitäten leicht überprüft werden.

A.12.4.2. Schutz der Protokollinformationen	Protokollierungseinrichtungen und Protokollinformationen müssen vor Manipulationen und unbefugtem Zugriff geschützt sein.	Alle aufgezeichneten Daten werden verschlüsselt und auf dem Ekran System Server gespeichert. Nur Administratoren mit relevanten Berechtigungen können über das Online-Verwaltungstool auf diese Daten zugreifen.
A.12.4.3. Administrator- und Bedienerprotokolle	Systemadministrator- und Systembetreiberaktivitäten müssen protokolliert und die Protokolle geschützt und regelmäßig überprüft werden.	Ekran System zeichnet alle Benutzersitzungen auf, einschließlich Sitzungen privilegierter Benutzer, und protokolliert alle Aktionen von Systemadministratoren. Diese Protokolle enthalten Administratoraktivitäten im Ekran System Client und im Management Tool. Alle aufgezeichneten Daten werden in einem geschützten Format auf dem Ekran System Server gespeichert und können zur forensischen Analyse exportiert werden.
A.15.2.1. Überwachung und Überprüfung der Lieferantendienste	Die Organisationen überwachen, überprüfen und auditieren regelmäßig die Erbringung von Lieferantenservices.	Mit Ekran System können Sie Dritte überwachen und deren Aktivitäten in Ihrer Infrastruktur aufzeichnen und überprüfen.
A.16.1.2. Melden von Informationssicherheitsereignissen	Informationssicherheitsereignisse sind so schnell wie möglich über geeignete Verwaltungskanäle zu melden.	Mit Ekran System können Sie regelmäßige oder Ad-hoc-Berichte zu Benutzeraktivität, Produktivität, aufgerufenen URLs, Befehlen, Tastenanschlägen, Warnungen und vielem mehr erstellen. Berichte können in mehreren Formaten erstellt und mit Ihren Unternehmensanmeldeinformationen angepasst werden.
A.16.1.4. Bewertung und Entscheidungsfindung zu Informationssicherheitsereignissen	Ereignisse der Informationssicherheit sind zu bewerten und es ist zu entscheiden, ob sie als Vorfälle der Informationssicherheit eingestuft werden sollen.	Ekran System sammelt Aktivitätsprotokolle und bietet einen integrierten Player, um diese zu überprüfen und mithilfe vieler Protokollparameter nach bestimmten Vorfällen zu suchen. Mit diesen Tools können Sie jede Aktion analysieren, ihren Kontext festlegen und die Bedrohungsstufe bestimmen.

A.16.1.5. Reaktion auf Informationssicherheitsvorfälle	Auf Vorfälle der Informationssicherheit ist es gemäß den dokumentierten Verfahren zu reagieren.	Ekran System verwendet vordefinierte und vom Benutzer generierte Warnungen, um Sicherheitsverletzungen zu erkennen. Wenn eine Warnung ausgelöst wird, benachrichtigt die Software die Sicherheitsbeauftragten über dieses Ereignis und stellt einen Link zur Sitzung bereit. Über diesen Link können Beauftragten die Bedrohung bewerten und die Sitzung oder den Benutzer bei Bedarf blockieren. Außerdem kann Ekran System automatisch auf kritische Vorfälle reagieren, indem Benutzer und Prozesse automatisch blockiert werden.
A.16.1.7. Sammlung von Beweisen	Die Organisation muss Verfahren zur Identifizierung, Sammlung, Erwerbung und Aufbewahrung von Informationen, die als Beweismittel dienen können, definieren und anwenden.	Ekran System sammelt Informationen von überwachten Endpunkten und speichert sie auf seinen Servern. Alle aufgezeichneten Daten werden in einem verschlüsselten Format auf dem Server gespeichert, um Manipulationen oder Missbrauch zu verhindern. Daten können zur weiteren Analyse in einem forensischen Format exportiert werden.

About BAKOTECH Group

BAKOTECH is an international group of companies, a flagship in focused Value Added IT Distribution that represents solutions of leading IT vendors. Positioning itself as a True Value Added IT distributor BAKOTECH provides professional pre-sales, post-sales, marketing and technical support for partners and end-customers. Geographically the Group operates in 26 countries covering Central and Eastern Europe, the Balkans, the Baltic States, the Caucasus, Central Asia with offices in Prague, Krakow, Riga, Vienna, Minsk, Kyiv, Baku and Nur-Sultan.

BAKOTECH is an official distributor of Ekran System solutions in Ukraine, the Republic of Belarus, Azerbaijan, Georgia, Armenia, Germany, Austria and Switzerland.

For more information about Ekran System solutions contact us at
+4366475315225, **www.bakotech.at**, **Ekran_System@bakotech.at**