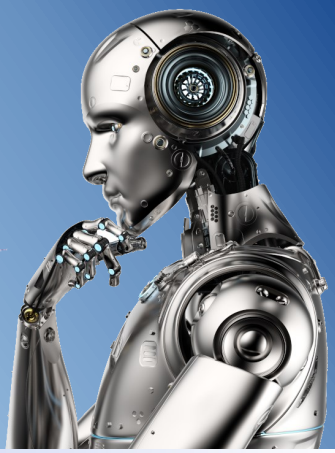
DSP More IT-Value



Informationssicherheit

Rechtliche Anforderungen

KRITIS

- Gemäß dem **IT-Sicherheitsgesetz** sind seit 2015 Qualitätsanforderungen und Meldepflichten zu erfüllen, die von den Betreibern kritischer Infrastrukturen gegenüber dem BSI und der BNetzA verlangt werden
- Gesetzliche Vorgabe für Organisationen mit Versorgungsauftrag der Bevölkerung kritischer Größe ab 01.01.2018
- **9 Branchen** (Energie, Ernährung, Finanz– und Versicherungswesen, Gesundheit, Informationstechnik und Telekommunikation, Siedlungsabfallentsorgung, Transport und Verkehr, Wasser, Unternehmen von besonderem öffentlichem Interesse [UBI] Staat und Verwaltung)
- In der KRITIS-Verordnung sind für jeden Anlagentyp spezifische **Schwellenwerte** festgelegt. Überschreitet eine Anlage den ihr zugeordneten Schwellenwert, gilt sie als Kritische Infrastruktur. Unternehmen, die solche Anlagen betreiben, sind KRITIS-Betreiber und verpflichtet, entsprechende Cyber-Security-Maßnahmen umzusetzen und dies durch ein unabhängiges KRITIS-Audit nachzuweisen. [Quelle: usd AG]
- Die Schwellwerte sind so angelegt, dass eine Anlage, die mindestens 500.000 Menschen mit der kritischen Dienstleistung versorgt, als kritische Infrastruktur angesehen wird. Dazu wird für jede Anlagenart der geschätzte, mittlere Jahresbedarf pro Kopf berechnet und anschließend mit dem Faktor 500.000 multipliziert. [Quelle: usd AG]
- Verpflichtung zur Implementierung eines unternehmensweiten **Information Security Management Systems („ISMS“)**
- **Empfehlung:** Verwendung von **ISO 27001** oder eines vergleichbaren Branchenstandards (z.B. **ISO 27799 oder B3S oder TISAX**) in Verbindung mit **BSI Grundschutz**
- Einreichung eines **ISMS Zertifikats** beim BSI

Weitere Vorgaben für die Implementierung eines ISMS

- Weitere Gesetze (z.B. **75c SGB**) und Branchenvorgaben (z.B. **TISAX**) erfordern die Implementierung eines ISMS auch ohne die Erreichung der KRITIS-Schwellenwerte

Fazit

Viele Organisationen haben noch kein ISMS gemäß den Anforderungen implementiert oder sind erst dabei, ein ISMS aufzubauen. Sicherheitslücken sind nicht auszuschließen!

Compliance ohne ein vollständiges ISMS ist nicht nachweisbar. Nur die ganzheitliche Implementierung eines ISMS gemäß ISO 27001 oder eines angelehnten Standards stellt einen umfassenden Schutz für Informationen auf der Basis von Anweisungen, einer dedizierten Security Organisation, dedizierten Security Prozessen, Dokumentation und unterstützenden technischen Security-Systemen dar.

DSP IT Service GmbH

Tel.: 06172 - 679 460 I Email: sales@dsp-eu.de

www.dsp-eu.de

DSP More IT-Value

ISMS

Risiken und Chancen / Roadmap zu Ihrem ISMS

Risiken

Sicherheitslücken gefährden Kunden, den Ruf sowie den Betrieb und verursachen erhebliche Kosten.

Ohne ein funktionierendes ISMS System kann keine Organisation mehr existieren.

Chancen

Die Bundesregierung hat die Defizite im Bereich Informationssicherheit erkannt und gehandelt.

Ständige Verschärfung der Anforderungen mit Vorschrift zur Implementierung eines ISMS.

Bereitstellung von Investitionsmitteln und Zuschüssen über KFW und KHSFV.

Empfehlung

Professionalisierung & Zertifizierung der IT Abteilung im ersten Schritt.

Ausbau des ISMS / Roll Out des ISMS in weitere Abteilungen.

Standardisierung, Digitalisierung, Automatisierung von Anträgen, Genehmigung, Einrichtung, Überwachung und Entzug von Zugriffsberechtigungen auf das Netzwerk und informationsverarbeitende Services (IAM). IAM bei häufig wiederkehrenden Geschäftsanforderungen und Operationalisierung mit Services.

ISMS Roadmap

Einführung und Zertifizierung

1. Analyse der Ausgangslage und Benchmark mit ISO 27001 („GAP-Workshop“)
2. Projektierungs-Workshop
3. Genehmigung Projektplan und Budget
4. Implementierung DSP ISMS System
5. Projektplan umsetzen
6. Zertifizierung in 6 bis 36 Monaten

DSP IT Service GmbH

Tel.: 06172 - 679 460 I Email: sales@dsp-eu.de

www.dsp-eu.de

DSP More IT-Value

DSP ISMS Enterprise Management System

Zielgruppe

Security Organisationen, die an ISO 27001 / B3S / TISAX o.ä. Standard orientiert ein ISMS implementieren wollen.

Kurzbeschreibung

Das **DSP ISMS Enterprise Management System** unterstützt die Risiko- und Security-Organisation ganzheitlich bei dem Betrieb eines zertifizierungsfähigen Information Security Management Systems **gemäß Best Practices** und der Norm **ISO 27001** und abgeleiteten Standards.

Mit den im Standard ausgelieferten Funktionen, Prozessen und Verfahren erfüllt das System alle normativen Anforderungen und dokumentiert alle Security relevanten Vorgänge. Im **Security-Dashboard** hat die Security Organisation einen sofortigen **Überblick über die Sicherheitslage**.

Mit den im ISMS-Dashboard im Standard ausgelieferten Statistiken und Reports mit Drill-Down-Funktion, kann die Security-Organisation sehr schnell **sicherheitsrelevante Vorgänge identifizieren**, den Status feststellen und steuernd eingreifen.

Das Risikomanagement sowie das Dokumentenmanagement sind nahtlos integriert. Ihr Zertifizierungs-Audit bestehen Sie auf dieser Basis mit überschaubarem Aufwand und stellen sicher, dass Sie keine wichtige Anforderung übersehen haben.

Häufig wiederkehrende **sicherheitsrelevante Vorgänge** wie z.B. Mitarbeiter Onboarding werden vom System prozessorientiert digitalisiert und automatisiert.

Mit den nützlichen DSP-Add-On Modulen wie **DSP IAM** werden Zugangsberechtigungen für AD-gesteuerte Systeme voll automatisiert beantragt, genehmigt, umgesetzt und bei Bedarf wieder entzogen.

Mit dem **DSP Prüfungsmodul** werden vergebene **Zugangsberechtigungen gemäß ISO 27001 Anhang A 9.2.5 und 9.2.6** automatisiert geprüft und bei Bedarf entzogen. Dadurch wird Information Security in den Prozessketten integriert hergestellt und gleichzeitig sinkt der manuelle Aufwand der gesamten Organisation signifikant.

Das System basiert auf der **Matrix42-Applikation** und ist ein datenbankgestütztes ERP-System, adaptiert auf die Bedürfnisse des Information Security Managements.

Mit dem System werden Information Assets (Informationswerte) prozessorientiert gemanaged. Meldewege für **Information Security Incidents** werden genau so effizient unterstützt wie Security Changes und Security Service Requests.

Mit dem integrierten **Rollen- und Rechte-Konzept** bildet die Applikation Ihre Security-Organisation ab. **So wird sichergestellt, dass Informationssicherheit umfassend in Ihrer Organisation unterstützt wird.**

DSP IT Service GmbH

Tel.: 06172 - 679 460 I Email: sales@dsp-eu.de

www.dsp-eu.de

DSP More IT-Value

Standard-Funktionen des DSP ISMS Enterprise Management Systems

Standard-Funktionen:

- Security Organisation mit Rollen und Rechten
- Integriertes ISMS Portal & ISMS Dashboard
- Dokumentenmanagement & Risikomanagement
- Information Asset Management
- Incident, Change, Service Request Management
- Reporting
- QM und KVP Management
- Standardverfahren für alle normativ geforderten, regelmäßigen ISMS Pflegearbeiten
- Service Katalog & Service Desk
- Security Operation Center (SOC)
- Matrix42: Ticket- und Workflow-Engine

Vorhandene und vom Kunden bereitzustellende Systeme können integriert und ein SIEM aufgebaut werden, z.B.:

Monitoring

Identity & Access Management

Firewall, Viruswall

Network Access Control (NAC)

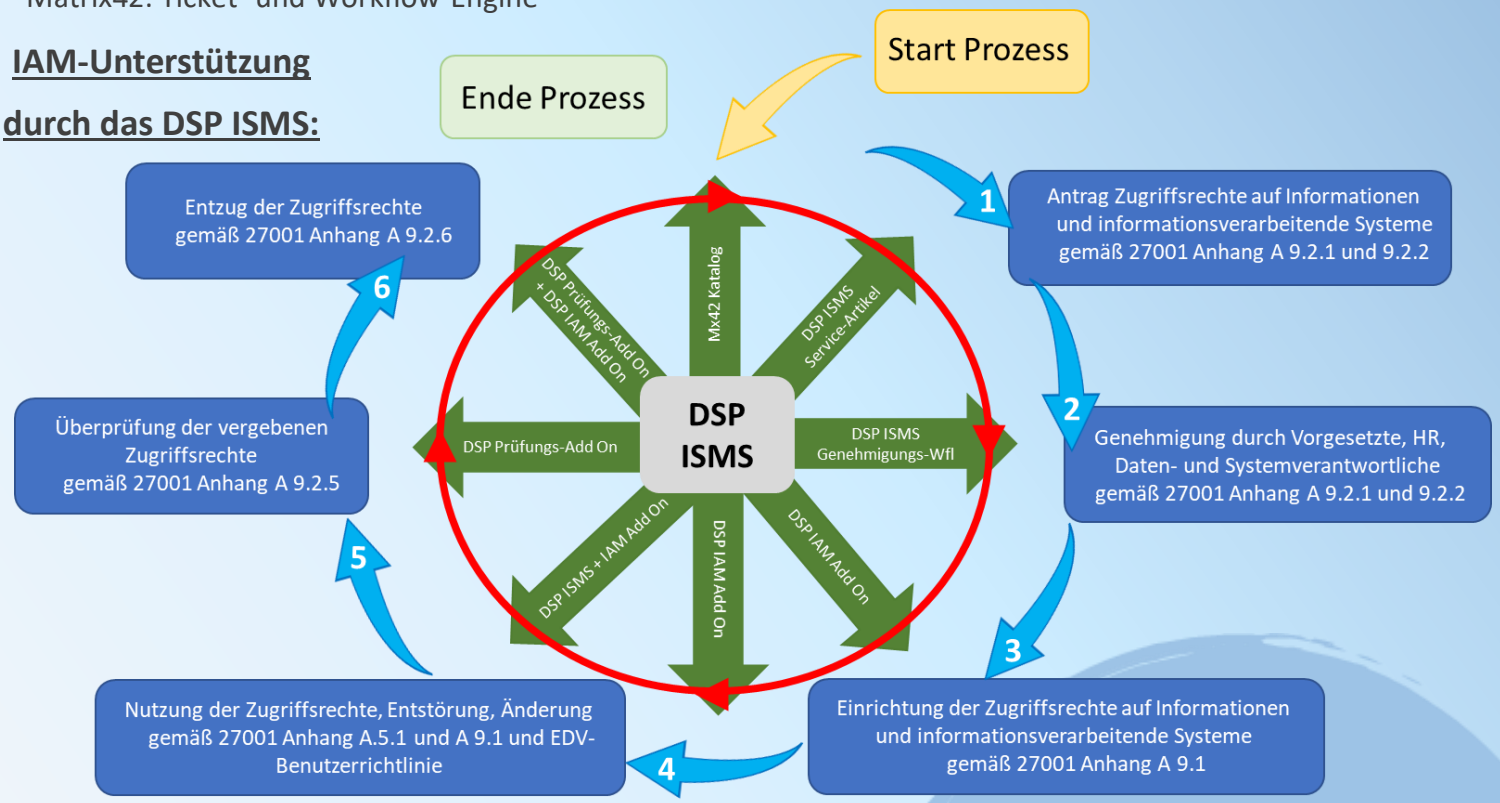
Endpoint Security

Mobile Device Management

...

Voraussetzung: Bereitstellung der Matrix42-Applikation durch den Kunden (Alternativ: Lieferung und Basis-Implementierung durch DSP). Durch Integration weiterer technischer Systeme kann das DSP ISMS Enterprise Management System zu einem Security Incident and Event Management System (SIEM) ausgebaut werden.

IAM-Unterstützung durch das DSP ISMS:



DSP IT Service GmbH

Tel.: 06172 - 679 460 I Email: sales@dsp-eu.de

www.dsp-eu.de

DSP More IT-Value

Nutzen für die ISMS-Stakeholder

Management

ISO & ISB

Management:

1. Sicherstellung, dass die Security-Vorgaben der Leitung strukturiert und prozessorientiert umgesetzt werden
2. Bereitstellung einer geeigneten Ressource zur Unterstützung des ISMS
3. Etablierung eines Rollen und Rechte-Konzeptes für die Security-Organisation
4. Bereitstellung einer Plattform zur Veröffentlichung der von der Leitung vorgebebenen Security-Regelungen
5. Sicherstellung, dass Security relevante Aufgaben und Vorgänge transparent gemäß der Normvorgaben bearbeitet werden
6. Schneller Überblick über die Sicherheitslage im Unternehmen durch aussagekräftige Security-Reports
7. Reports weisen die Einhaltung der Vorgaben gemäß ISO 27001, DSGVO nach (Compliance) bzw. zeigen Defizite, Bearbeitungsstatus u. Ursachen auf
8. Das DSP ISMS unterstützt die regelmäßigen internen u. externen Audits durch digitale Geschäftsaufzeichnungen aller Security-relevanten Vorgänge im Unternehmen

ISO (Information Security Officer) und ISB (Informations-Sicherheits-Beauftragte):

1. Bereitstellung einer professionellen Applikation zur Unterstützung des Information Security Managements gemäß ISO 27001/B3S/TISAX und abgeleiteter Standards
2. Etablierung eines vorgegebenen Rollen- & Rechte-Konzeptes für die Security-Organisation, das die Zusammenarbeit und Trennung von Verantwortung („SOD“) unterstützt
3. Unterstützung von Dokumentenmanagement und Dokumentenlenkung mit Veröffentlichung von selektierten Dokumenten im Security-Portal
4. Unterstützung des Risikomanagements mit einer Risiko-Datenbank, zugewiesenen Risiko-Verantwortlichen und einem prozessorientierten Management von Risiken (inklusive der Genehmigung von Restrisiken)
5. Erfassung jedes Security-relevanten Vorgangs mit einem digitalen Geschäftsvorgang (Ticket)
6. Erstellung von elektronischen Security-Aufgaben (Tasks) mit Delegation an Mitarbeiter (m/w/d) mit Netzwerkzugriff (AD-Konto) in der Organisation zur transparenten, nachverfolgbaren, auditierbaren Bearbeitung von Security-Vorgängen
7. Erfassung, Inventarisierung, prozessorientiertes Management, Reporting der Information Assets
8. Unterstützung der Security-Prozesse Incident Management, Change Management und Service Request Management
9. Standardisierung, Digitalisierung und Automatisierung der häufig wiederkehrenden und normativ geforderten Pflegearbeiten und Vorgänge
10. Bereitstellung einer Applikation zur Unterstützung der Prozesse für das Zugriffsmanagement auf zu schützende Informationen und informationsverarbeitende Systeme (IAM) mit Antrag, Genehmigung, Einrichtung, Überwachung der Nutzung, Überprüfung von Zugriffsrechten, Entziehung von Zugriffsrechten sowie Auditierung von vergebenen Zugriffsrechten
11. Security Reporting
12. Umfassende Unterstützung von Audits durch standardisierte Reports, individuell gestaltete Systemabfragen, digitale Aufzeichnungen zu Security-relevanten Vorgängen und Auditnachweisen von normativ geforderten Prüfvorgängen
13. Signifikante Reduktion des Aufwands der Security-Organisation bei gleichzeitiger Qualitätserhöhung und Herstellung der Auditierfähigkeit

DSP IT Service GmbH

Tel.: 06172 - 679 460 I Email: sales@dsp-eu.de

www.dsp-eu.de

DSP More IT-Value

Nutzen für die ISMS-Stakeholder

Fachbereichs-Management

IT Service Organisation

Fachbereichs-Management:

1. Unterstützung der Rolle des Information Security Beauftragten der Abteilung bei der Erledigung seiner bereichsspezifischen Security-Aufgaben
2. Gleichzeitige Einbindung des ISB in die Security-Organisation und Prozesse
3. Standardisierung, Digitalisierung, Automatisierung von Anträgen, Genehmigungen, Einrichtung, Überwachung, Überprüfung u. Entzug von Zugriffsrechten auf zu schützende Informationen u. informationsverarbeitende Services (IAM)
4. Standardisierung, Digitalisierung von normativ geforderten, häufig wiederkehrenden Pflegearbeiten
5. Erfassung, Inventarisierung, prozessorientiertes Management, Reporting der Information Assets des Bereichs
6. Unterstützung der Security-Prozesse Incident Management, Change Management und Service Request Management
7. Security Reporting
8. Umfassende Unterstützung von Audits durch standardisierte Reports, individuell gestaltete Systemabfragen, digitale Aufzeichnungen zu Security relevanten Vorgängen und Auditnachweisen von normativ geforderten Prüfvorgängen
9. Signifikante Reduktion des Aufwands der Security-Organisation bei gleichzeitiger Qualitätserhöhung und Herstellung der Auditierfähigkeit

IT Service Organisation:

Zu den genannten Vorteilen für die IT-Security-Organisation bietet das DSP ISMS der IT-Abteilung folgende Vorteile:

1. Bereitstellung eines integrierten Systems für das Service Mgmt. gemäß ITIL®/ISO 20000-1 u. Information Security Managements gemäß ISO 27001 in der IT-Abteilung
2. Vermeidung von Doppelerfassung u. Mehrarbeit von allen Security-relev. Vorgängen in der IT-Abtlg.
3. Erweitertes Asset-Management um eine Security-Klassifizierung von Services und IT-Ressourcen
4. Erweiterung der Standard Service Mgmt.-Prozesse (Incident-, Change-, Service Request-, Asset-Management) um die normativ geforderten Security-Prozess-Anforderungen
5. Standardisierung, Digitalisierung von Anträgen, Genehmigungen, Einrichtung, Überwachung, Überprüfung, sowie Entzug von Zugriffsrechten auf zu schützende Informationen und informationsverarbeitende Services
6. Automatisierung von Prozessen u. Prozessschritten durch vielseitige Integrationsmöglichkeit mit weiteren technischen IT-Systemen
7. Signifikante Reduktion des Service- & Supportaufwands in der IT-Abteilg. bei gleichzeitiger Verbesserung des Kundenservice durch Bereitstellg. eines zentralen Service- & Security-Portals mit einem Katalog für die Beantragung, Genehmigung, Einrichtung, Überwachung, Überprüfung sowie Entzug von Zugriffsrechten auf zu schützende Informationen u. informationsverarbeitende Services (IAM)
8. Sicherstellung, dass alle organisatorischen, prozessualen u. normativ geforderten Verfahren gemäß der ISO 27001 nachweislich u. nachweisbar in der IT-Abteilung eingehalten u. umgesetzt werden, bei gleichzeitiger Hebung von Synergieeffekten mit dem Service Mgmt. System der IT-Abteilung durch ein integriertes DSP ISMS Mgmt. System
9. **Das DSP ISMS Management System ist die Basis für eine auditierfähige Dokumentation des Tagesgeschäftes u. eine Zertifizierung gemäß ISO 27001 im IT-Bereich**

DSP IT Service GmbH

Tel.: 06172 - 679 460 I Email: sales@dsp-eu.de

www.dsp-eu.de

DSP More IT-Value