

Thema	<u>Information Risk Management</u>	<u>Compliance & Zertifizierung</u>	<u>Umsetzung von Informationsbezogenen Sicherheitsmaßnahmen</u>
Zielgruppe	<ul style="list-style-type: none"> ▪ CISO (Chief Information Security Officer) ▪ CFO (Chief Financial Officer) ▪ Revision ▪ Datenschutzbeauftragter ▪ Sicherheitsbeauftragter ▪ CIO (bedingt) 	<ul style="list-style-type: none"> ▪ CISO (Chief Information Security Officer) ▪ Compliance Officer ▪ CIO ▪ Sicherheitsbeauftragter ▪ Revision ▪ CFO (bedingt) 	<ul style="list-style-type: none"> ▪ CISO (Chief Information Security Officer) ▪ Fachabteilungen („Data-Owner“) ▪ IT Datacenter ▪ IT Anwendungsentwicklung ▪ Datenschutzbeauftragter ▪ Sicherheitsbeauftragter ▪ CIO (bedingt)
Schlagwörter	<ul style="list-style-type: none"> ▪ Ganzheitliche Sicherheitsstrategie ▪ Berücksichtigung von organisatorischen, prozessualen, personellen und technischen Aspekten ▪ Sicherheitsanalysen/-Beratung ▪ Erstellen von Sicherheitsrichtlinien (Policy) ▪ Identifizieren und Klassifizieren von sensiblen Daten ▪ Mitarbeitersensibilisierung 	<ul style="list-style-type: none"> ▪ Einhaltung von gesetzlichen oder branchenspezifischen Vorgaben wie SOX, „EuroSOX“, Basel II, Bundesdatenschutzgesetz, PCI (Payment Card Industry) ▪ Umfassendes Compliance- und sicherheitsbezogenes Reporting ▪ Anwenden von IT- und Sicherheitsstandards wie ISO27000-Familie, BSI Grundschutz 	<ul style="list-style-type: none"> ▪ Identifizieren und Überwachen von sensiblen und geschäftskritischen Daten ▪ Mitarbeitersensibilisierung ▪ Datenverschlüsselung <ul style="list-style-type: none"> ▪ Medium: SAN, NAS, Backups/Tapes ▪ Server: Fileshares, Datenbanken, Anwendungen ▪ Clients: Laufwerk, Verzeichnis, Datei ▪ Email-Verschlüsselung und –Signatur (PKI – Public Key Infrastructure) ▪ Dokumentensicherheit, DRM (Digital Rights Management), IRM (Information Rights Management) ▪ Zentrales Schlüssel-Management
Business-zweck	<ul style="list-style-type: none"> ▪ Risiko-Minimierung ▪ Kostensenkung durch angemessene (Risiko-basierte) Sicherheitsinvestitionen ▪ Sicherheit im Einklang mit den Geschäftszielen ▪ Schutz von Wettbewerbsvorteilen ▪ Schutz von Unternehmens-Know-how 	<ul style="list-style-type: none"> ▪ Absicherung und Risikominimierung gegenüber gesetzlicher oder vertraglicher Verpflichtungen ▪ Nutzen von Synergieeffekten: Geschäftsprozessoptimierung, Standardisierung ▪ Kundenbindung durch Nachweis der Einhaltung vertraglicher Pflichten (z.B. SLA's) ▪ Reports als Vertriebswerkzeug 	<ul style="list-style-type: none"> ▪ Schutz vor Informationsmissbrauch ▪ Schutz von Kunden- und personenbezogenen Daten ▪ Schutz von geistigem Eigentum ▪ Schutz vor Mediendiebstahl/Verlust ▪ Umsetzung von Sicherheitsvorschriften (Compliance) ▪ „Datensafe“ z.B. für Vorstand oder HR ▪ „Separation of Duties“: Kein Generalzugriff für Administratoren ▪ Unternehmensweite Koordination und Verwaltung von Verschlüsselung
Produkte / Lösungen	RSA Information Security Services Group (Consulting), RSA Risk Advisor, RSA Executive Security Assessment	RSA Information Security Services Group (Consulting), RSA Executive Security Assessment, RSA enVision, alle weiteren RSA Lösungen zur technischen Umsetzung von Compliance-Vorschriften	RSA Information Security Services Group (Consulting), RSA Data Loss Prevention Suite, RSA Encryption Suite, RSA Key Manager, RSA SecurID, EMC PowerPath, EMC Connectrix, EMC Documentum Authentica)
Quali-Fragen	<ul style="list-style-type: none"> ▪ Sagt Ihnen "Information Risk Management" etwas? ▪ Kennen Sie die Risiken, welche Ihrem Unternehmen durch die Verarbeitung von Informationen entstehen? ▪ Kennen Sie Ihre sensiblen Informationen und Datenbestände? ▪ Wissen Sie wer mit diesen Daten arbeitet, darauf zugreift usw.? 	<ul style="list-style-type: none"> ▪ Müssen Sie Ihre Infrastruktur nach Sicherheitsstandards zertifizieren oder verlangen Ihre (potentiellen) Kunden eine Zertifizierung? ▪ Untergliedern Sie Compliance-Anforderungen hinsichtlich der Verarbeitung von Informationen (z.B. SoX, Basel II, ...)? 	<ul style="list-style-type: none"> ▪ Sichern Sie die Infrastruktur oder die Information selbst? ▪ Kennen Sie Ihre sensiblen Informationen und Datenbestände? ▪ Bestehen Anforderungen hinsichtlich Datenverschlüsselung? ▪ Wollen Sie die Verarbeitung sensibler Informationen überall überwachen?

Thema	<u>Absichern der IT-Infrastruktur</u>	<u>Zugriffs- und User-Management</u>	<u>Zentrales Log-Management</u>
Zielgruppe	<ul style="list-style-type: none"> ▪ CISO (Chief Information Security Officer) ▪ Datenschutzbeauftragter ▪ Sicherheitsbeauftragter ▪ IT Netzwerk ▪ IT Betrieb ▪ IT Anwendungsentwicklung ▪ CIO (bedingt) 	<ul style="list-style-type: none"> ▪ IT-Betrieb ▪ IT-User-Management ▪ IT-Anwendungsentwicklung ▪ IT-Help-Desk ▪ CIO ▪ HR ▪ Fachabteilungen 	<ul style="list-style-type: none"> ▪ IT-Betrieb ▪ IT-Help-Desk
Schlagwörter	<ul style="list-style-type: none"> ▪ Überwachen von sicherheitsrelevanten Systemen ▪ Erkennen von Angriffen ▪ Erstellen von Sicherheitsreports ▪ SIEM: Security Information and Security Event Management ▪ Schwachstellenanalyse ▪ Sicherer Zugriff auf Netzwerk- und Systemumgebung (z.B. VPN Einwahl, Portalsicherheit) ▪ Mehrfaktor-Authentifizierung ▪ OTP – One Time Password ▪ Zertifikatsbasierte Authentifizierung ▪ Absichern von Transaktionen 	<ul style="list-style-type: none"> ▪ IAM: Identity + Access Management ▪ Web- & Enterprise Single Sign On (SSO) ▪ Belastung der Mitarbeiter durch (komplexes) Passwort-Management ▪ Belastung des IT-Betriebs durch komplexe Benutzerverwaltung ▪ Aufbau von Rollenkonzepten ▪ OTP (One Time Password) ▪ Zertifikatsbasierter Systemzugriff ▪ User-Self Service Portale ▪ Systemzugriff für temporäre Kräfte z.B. durch Zugangs-Codes per SMS oder Email ▪ Unternehmenszugang im Katastrophenfall/Pandemie 	<ul style="list-style-type: none"> ▪ Zusammenführen aller Log-Informationen aus unterschiedlichsten Quellen an einer zentralen Plattform ▪ Zentrale Log-Auswertung ▪ Zentrale Log-Archivierung ▪ Zentrale Systemüberwachung und Alarmierung im Fehlerfall ▪ Information Lifecycle Management (ILM) für Systeminformationen ▪ Netzwerkoptimierung
Businesszweck	<ul style="list-style-type: none"> ▪ Einhaltung von gesetzlichen oder regulativen Vorgaben ▪ Kostensenkung ▪ Effizienzsteigerung/Automatisierung ▪ Forensische Analysen zur Vermeidung und Nachvollziehung von Sicherheitsvorfällen 	<ul style="list-style-type: none"> ▪ Gesteigerte Benutzerfreundlichkeit ▪ Mitarbeiter-Produktivitätssteigerung ▪ Help-Desk-Entlastung ▪ Vermeidung „kryptischer“ Passwörter ▪ Weniger vergessene Passwörter (Single-Sign-On) ▪ Neue Geschäftspotenziale erschließen, z.B. durch Zugriff von externen Partnern auf Unternehmensdaten ▪ Business Continuity Unterstützung für K-Fall Szenarien ▪ Sichtbare Sicherheit - Gewinnung von Neukunden 	<ul style="list-style-type: none"> ▪ Einhaltung von gesetzlichen Datenaufbewahrungsvorschriften ▪ Optimierung von Systemressourcen durch konsolidiertes Accounting und Reporting ▪ Effiziente und kosteneffektive Speicherung von Logs ▪ Effizienzsteigerung/Automatisierung im System-Management ▪ Schnellere Störungsbehebung ▪ Verbesserte Fehleranalyse ▪ Help-Desk Support
Produkte / Lösungen	RSA SecurID, RSA Access Manager, RSA Certificate Solutions, RSA enVision, RSA Consumer Solutions	RSA Information Security Services Group (Consulting), RSA SecurID, RSA Authentication OnDemand, RSA Access Manager, RSA Certificate Solutions	RSA enVision
Quali-Fragen	<ul style="list-style-type: none"> ▪ Haben Sie den vollen Überblick über alle sicherheitsrelevanten Infos in der IT-Infrastruktur? ▪ Wissen Sie wer auf die Infrastruktur zugreift? ▪ Setzen Sie eine Mehrfaktor-Authentifizierung ein 	<ul style="list-style-type: none"> ▪ Wie komplex sind Ihre Passwort-Richtlinien? ▪ Wie viel Arbeitszeit verschwenden Mitarbeiter beim Umgang mit bestehenden Passwort-Policies ▪ Besteht Bedarf an einer Single-Sign-On Infrastruktur? ▪ Welches Help-Desk-Aufkommen entsteht durch Passwort-Fehler? ▪ Wie gehen Sie mit temporären Usern um? 	<ul style="list-style-type: none"> ▪ An wievielen Stellen müssen Ihre Sys-Admins nach wichtigen Log-Informationen suchen? ▪ Wie werten Sie Ihre Log-Daten derzeit aus? ▪ Wie lange müssen Sie Log-Daten archivieren und wie setzen Sie dies um? ▪ Haben Sie im Fehlerfall eine zentrale Anlaufstelle? ▪ Wieviel Arbeitszeit geht Ihren Sys-Admins durch Log-Management verloren?