



in&out

«EFFIZIENTE UND SICHERE
IT-INFRASTRUKTUREN...



IN&OUT AG

GESCHÄFTSBEREICH

IT SECURITY



INHALT

Portfolio Überblick	3
Fachbereich Security Management	9
Fachbereich Security Services	23
Kontakt	40

PORTFOLIO ÜBERBLICK

UNSERE LEITSÄTZE



*«Unabhängige Beratung.
Garantiert und zuverlässig.»*

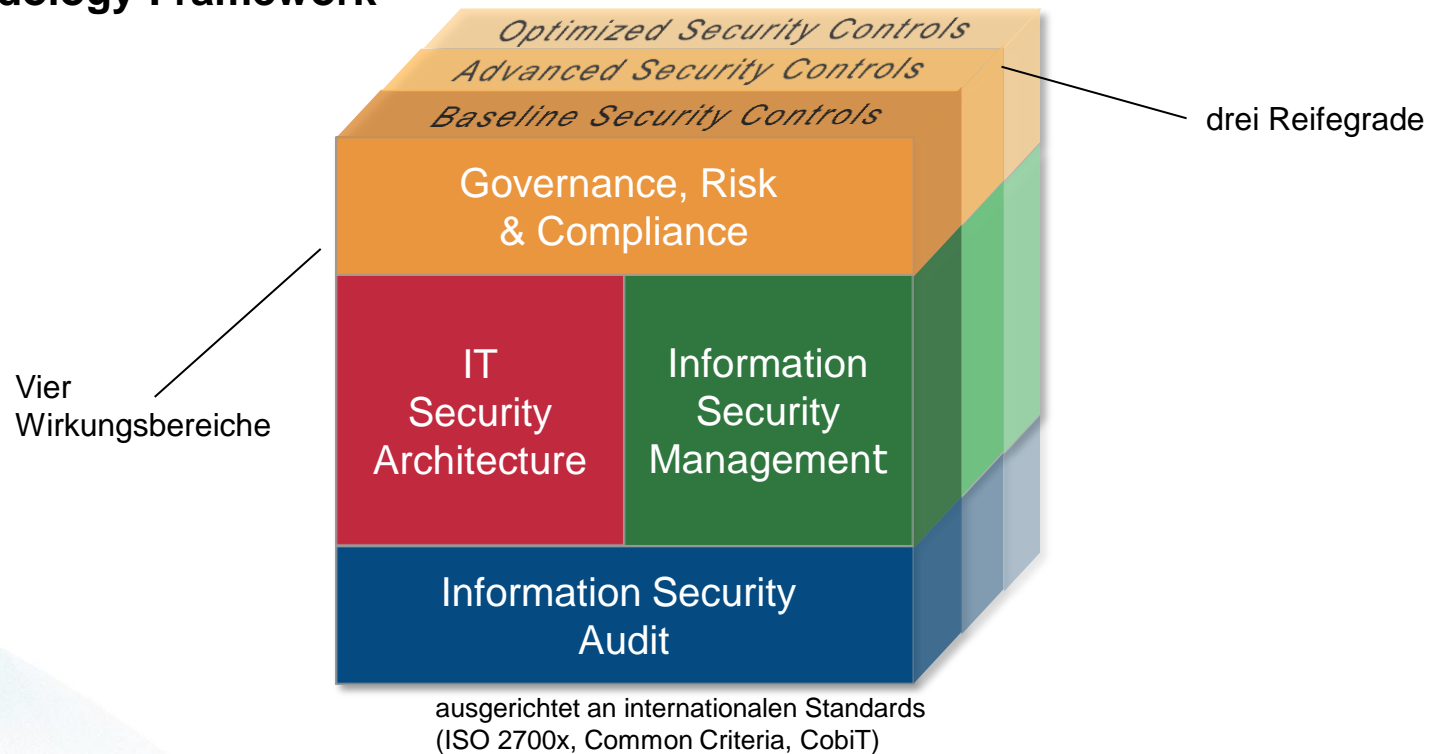
- Bei In&Out steht der **maximale Kundennutzen** an erster Stelle
- Unsere Lösungen zeichnen sich durch Nachhaltigkeit und ein **gutes Kosten/Nutzen-Verhältnis** aus
- Wir bieten unseren Kunden eine **umfassende, qualitativ hochstehende und neutrale Beratung**
- Unseren Mitarbeitenden bieten wir ein attraktives und motivierendes Arbeitsumfeld

PORTFOLIO ÜBERBLICK

UNSERE METHODE IO-ISMFC©



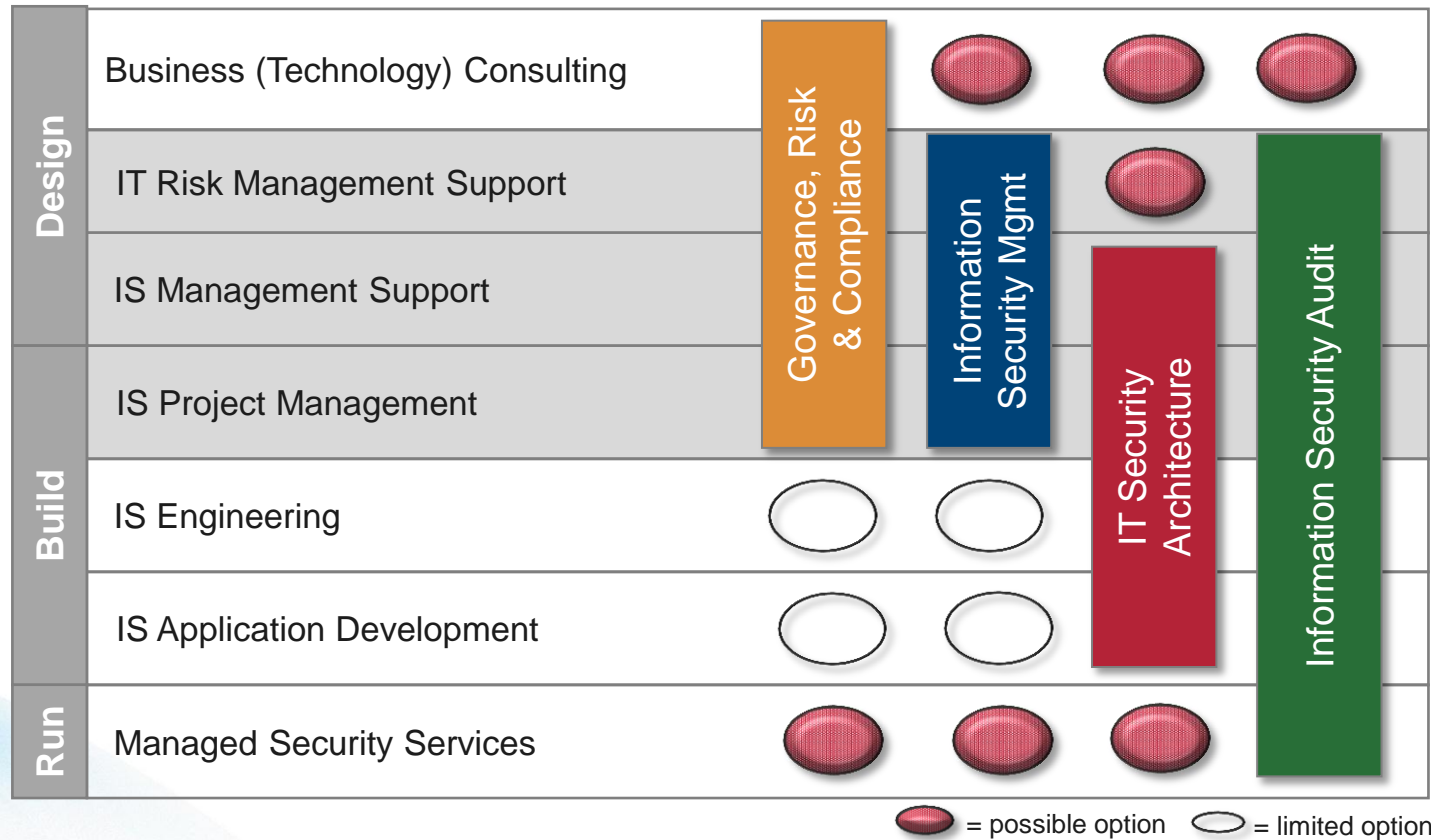
Information Security Methodology Framework





PORTFOLIO ÜBERBLICK

DIENSTLEISTUNG - DESIGN, BUILD & RUN



PORTFOLIO ÜBERBLICK

UNSERE STÄRKEN



- Mit viel **Erfahrung** bauen wir praxiserprobte Lösungen in diversen Branchen
- Wir besitzen **technisches Expertenwissen** auch in Spezialbereichen und sind dennoch Generalisten
- Die **termin-** und **kostengerechte** Lieferung der Ergebnisse ist uns ausgesprochen wichtig
- In unserer eigenen Organisation und bei unseren Kunden beweisen wir täglich **Sozialkompetenz** und **Teamfähigkeit**
- Wir arbeiten als **Sicherheitsarchitekten** und **-berater**, leiten gerne Projekte und unterstützen den sicheren IT-Betrieb
- Wir sind unabhängig, neutral und eigenfinanziert



INHALT

Portfolio Überblick	3
Fachbereich Security Management	9
Fachbereich Security Services	23
Kontakt	40



SECURITY MANAGEMENT

KERNKOMPETENZEN

IT Risk & Security Management

- Information Security Management
- IT Governance & Compliance
- Information Security Audits & IT Risk Analysis
- Security Testing

Security Architecture & Design

- Information Security Architecture
- Information Security Evaluation
- Information Security Process Design
- Information Security Application Design



SECURITY MANAGEMENT

IT RISK & SECURITY MANAGEMENT

Information Security Management

- Information Security Management Systems (ISO 2700x)

IT Governance & Compliance

- CobiT, ITIL, SOX, Basel II, FINMA regulations
- Codes of Practice (ISO, BSI, PCI, ICAO, ZertES)
- Data Privacy (Schweizerisches Datenschutzgesetz)
- Cross Border Transfer, Sourcing, Third Party Relations

Information Security Audits & IT Risk Analysis

- Security Reviews, Security Concepts, IT Risk Assessments

Security Testing

- Vulnerability Scanning, Compliance Checking, Quality Assurance
- Code Reviews, Penetration Testing (OWASP, OSSTMM)



SECURITY MANAGEMENT

IT RISK & SECURITY MANAGEMENT

- Aufbau und Optimierung **organisatorischer Strukturen** und **Prozesse** für das IT Risk & Security Management
- Identifizierung interner und externer Anforderungen an IT-Sicherheit und Compliance
- Identifizierung kritischer IT Services und Schutzobjekte (Assets) sowie relevanter Bedrohungen
- **Analyse und Auditierung** von IT Services und Systemen zur Ermittlung von Schwachstellen und Compliance-Abweichungen
- Identifizierung, Bewertung und Behandlung relevanter Risiken und Compliance-Abweichungen

« Sie erreichen ein effektives und effizientes Management Ihrer IT-Sicherheit sowie eine kontinuierliche Optimierung Ihres Sicherheitsdispositivs »



SECURITY MANAGEMENT

IT RISK & SECURITY MANAGEMENT

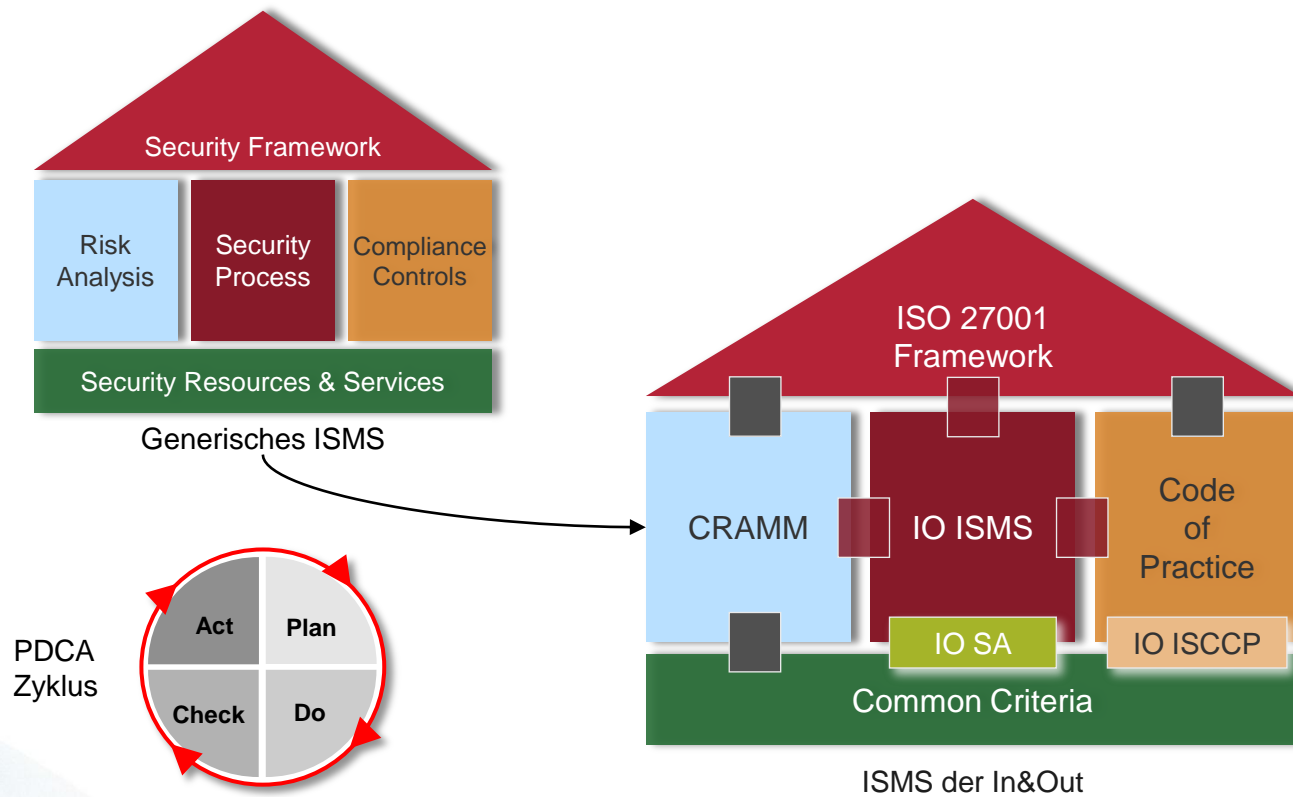
Das ISMS der In&Out basiert auf internationalen Standards und ermöglicht so eine **Zertifizierung nach ISO/IEC 27001**

- Das ISMS wird auf der **Prozess-und Systemebene** einer Organisation definiert und dokumentiert
- Auf der **Prozessebene** wird eine **Information Security Policy** erstellt (bzw. überprüft); basierend darauf werden die notwendigen Sicherheitsmassnahmen implementiert
- Auf der **Systemebene** werden die Organisationsstruktur und die Verantwortlichkeiten für das ISMS festgelegt sowie die notwendigen Prozesse definiert und eingeführt
- Dazu werden Risikobewertungen durchgeführt, die Sicherheitsorganisation bestimmt, Regelungen erlassen und Hilfsmittel erarbeitet



SECURITY MANAGEMENT

IT RISK & SECURITY MANAGEMENT





IT RISK & SECURITY MANAGEMENT

DIENSTLEISTUNGSPAKET

Die **IO Security Gap Analyse** ermöglicht die Ermittlung der aus Kundensicht relevanten **Handlungsfelder**

- Dokumentation des Ist-Zustands und von **Abweichungen** (Security Gaps) in Relation zum branchenüblichen Standard
- Priorisierte Massnahmenempfehlung zur Behebung der Security Gaps (Entscheidungsgrundlage z.Hd. Management)
- Vorgehen gemäss der von In&Out entwickelten, auf gängigen Standards (Common Criteria, ISO/IEC 2700x) abgestützten und praxiserprobten Methode (IO-ISMF[©])

«Sie erhalten rasch und kostengünstig eine Übersicht über die vorhandenen Security Gaps und über Ihren Handlungsbedarf in relevanten Gebieten der Informations- und IT-Sicherheit»

IT RISK & SECURITY MANAGEMENT PRODUKT



Das **IO Risk Cockpit Tool** ist ein Excel-basiertes Hilfsmittel mit folgenden Features:

- Anforderungskatalog an das Information Security Management gemäss ISO 27002 (Code of Practice, CoP)
- Dokumentation und Tracking von Massnahmen zur Behebung von Sicherheits-Schwachstellen und Compliance Gaps
- Nachweis der Risikobehandlung (Risk Treatment Plan, RTP) sowie Reporting des aktuellen Risiko-Status
- Erweiterungsoptionen: generischer Katalog von Schutzobjektgruppen für IT-Grundschatz zur Unterstützung des «kombinierten Ansatzes»; Bewertung und Reporting der Maturität gemäss IO-ISMF[©]

«Sie erhalten eine übersichtliche Darstellung der Risikosituation durch Mapping sowohl auf IO-ISMF[©] als auch auf ISO 27002»



IT RISK & SECURITY MANAGEMENT

REFERENZEN

Grossbank (2004 - 2006)	Durchführung regelmässiger Sicherheitsaudits produktiver IT-Systeme und Fachanwendungen (unter Federführung des IT Risk Departements)
Pharmakonzern (2006 - 2008)	Durchführung periodischer Due Diligence Audits und Risikobeurteilungen inklusive Vor-Ort-Überprüfungen von Outsourcing Providers
Grossbank (2007 - 2010)	Unterstützung des IT Risk Managements im internationalen Asset Management insb. Beratung zu grenzüberschreitenden Datentransfers
Versicherung (2008 - 2009)	Gestaltung und Aufbau eines ISMS nach ISO 27001 insb. Integration in die IT Governance, IT-Projektsteuerung und ITIL Serviceorganisation
Versicherung (2010)	Erstellung eines IT-Grundschutzkatalogs und der dazugehörigen Umsetzungsprozesse und Verantwortlichkeiten (AKVs)
Kantonsverwaltung (2010)	Erarbeitung eines ISDS-Konzepts mit Schutzobjekt-Inventar, Risikoanalyse und Massnahmenplanung für eine hochsensitive Rapportierungsdatenbank
Bundesamt (seit 2008)	Durchführung der internen Audit-Jahresprogramme einer nach ZertES klassifizierten PKI (zentrale Fachdienste und kantonale Registraturen)
Versicherung (seit 2009)	Sicherheitsüberprüfungen für die Integration des Lebensgeschäfts und des Rechtsschutzes in eine IT-Gesamtlösung
Bundesamt (seit 2010)	Einführung und Zertifizierung eines ISMS nach ISO 27001 für den erwei-terten Zugriffsschutz des biometrischen Passes und Ausländerausweises
Kreditkartenherausgeber (2011)	Überprüfung des bestehenden ISMS und der PCI-DSS Compliance, sowie der IT-Infrastruktur (aufgrund neuer Geschäftsbereiche und –Prozesse)
Grossbank (2011)	Prozessorientierte Risikoanalyse einer vom Rest des Netzwerks getrennten und hochsicheren IT-Plattform für die Formalitätenverwaltung



SECURITY MANAGEMENT

SECURITY ARCHITECTURE & DESIGN

Information Security Architecture

- Security Architecture Frameworks

Information Security Evaluation

- Evaluation/Proof of Concept of Security Technologies & Products

Information Security Process Design

- Security Administration & Access Management
- Security in Development & Support Processes
- Change Control, Information Leakage, Data Anonymisation

Information Security Application Design

- Information Access Restriction, Sensitive Data Isolation
- Session Control, Transaction Protection
- Java Security, .NET Security

SECURITY MANAGEMENT

SECURITY ARCHITECTURE & DESIGN



«Überprüfung und Konzeption der Sicherheitsarchitektur in Abstimmung mit IT-Strategie und Business-Anforderungen»

- Konsistente Umsetzung Ihrer IT-Strategie
- Beratung bei Planung und Einsatz von **Sicherheitstechnologien** (bezogen auf einen Zeitraum von 3 bis 5 Jahren)
- Identifikation der vorhandenen **Sicherheitsmechanismen**, -produkte und -anwendungen („Landkarte“)
- Ermittlung des Handlungsbedarfs zur Optimierung des Sicherheitsdispositivs
- Konsolidierung und Ausbau der Sicherheitsinfrastruktur entsprechend den definierten Schwerpunkten

«Umfassender Überblick der in Ihrer Organisation vorhandenen Sicherheitsmechanismen und „Interaction Domains“»



SECURITY ARCHITECTURE & DESIGN

DIENSTLEISTUNGSPAKET

- Die Erstellung einer (IT-) **Sicherheitsanalyse** umfasst folgende Schritte:
 - Erarbeiten einer Systembeschreibung (Infrastrukturanalyse)
 - Identifizieren von Schutzobjekten und Bedrohungen (Schutzbedarfsfeststellung)
 - Durchführen einer Schwachstellenanalyse mit Risikobewertung
 - Ausarbeiten von Sicherheitsmassnahmen zur Begrenzung der festgestellten Risiken
- Die Ausarbeitung des Sicherheitskonzepts orientiert sich an CRAMM (CCTA Risk Analysis & Management Method)
- Die Einhaltung des Verfahrens bei manuellen Sicherheitsanalysen bringt gemäss unserer Erfahrung gute Resultate
- Auf Wunsch kann ein Verfahren des Kunden eingesetzt werden



SECURITY ARCHITECTURE & DESIGN

DIENSTLEISTUNGSPAKET

- **IO SA:** ermöglicht die Erarbeitung und Erstellung einer **formalisierten und konsistenten** IT-Sicherheitsarchitektur
 - Eigene Methode auf der Basis der Common Criteria (ISO/IEC 15408)
 - Klare Struktur, transparente Methode: Abstraktion auf die relevanten Bereiche eines IT-Systems
 - Übersicht über alle Bereiche einer IT-Sicherheitsarchitektur
- **Workshops** dienen der Teambildung und verankern die IT-Sicherheit in verschiedenen Fachbereichen
- Workshops erhöhen das Verständnis und die **Awareness**
- Präsentationen zur Dokumentation der einzelnen Workshops liegen nach jedem Workshop vor; zum Schluss wird ein separates Abschlussdokument im Textformat erstellt



SECURITY ARCHITECTURE & DESIGN

REFERENZEN

Grossbank (2000/01 & 2003 (Update))	Erarbeitung der IT-Sicherheitsarchitektur erweitert um eine Produkte-Road-Map
Finanzdienstleister (2002)	Erstellung der IT-Sicherheitsarchitektur erweitert um eine Sourcing Architektur
Grossbank (2003/04)	Erstellung der IT-Sicherheitsarchitektur mit Schwerpunkt auf Netzwerk-separation und Anwendungslandschaft (strukturiert nach TOGAF)
Energiekonzern (2007)	Erarbeitung der IT-Sicherheitsarchitektur mit Schwerpunkt auf der Einführung einer PKI
Informatikdienstleister (2007/08)	Erstellung der IT-Sicherheitsarchitektur mit Schwerpunkt auf der Mandantenfähigkeit
Versicherung (2003 & 2008 (Update))	Erarbeitung der gruppenweiten IT-Sicherheitsarchitektur mit Schwerpunkt auf strategischen Kernaussagen (dargestellt in Hype-Diagrammen)
Versicherung (2008/09)	Erarbeitung von Design-Prinzipien für Storage-Area-Netzwerke, Server-Virtualisierung und den Umgang mit sensitiven Daten in separierten Zonen
Versicherung (2009)	Erarbeitung eines umfassenden Netzwerkzonenkonzepts mit Integration einer mandantenfähigen Citrix-Infrastruktur
Bundesamt (2010)	Erstellung der IT-Sicherheitsarchitektur mit Schwerpunkt auf der Integration des Identity & Access Managements
Privatbank (2011)	Umsetzung der Zonierung des weltweiten, internen Netzwerks (inkl. Systeminventar, Systemplatzierungsprozess und Systemplatzierung)
Bundesamt (2011)	Sicherheitsanalyse der gesamten Informatikinfrastruktur in Abstimmung mit Geschäftsprozessen, IT-Strategie und Sicherheitsarchitektur



INHALT

Portfolio Überblick	3
Fachbereich Security Management	9
Fachbereich Security Services	23
Kontakt	40



SECURITY SERVICES

KERNKOMPETENZEN

Identity & Access Management

- AAA-Services
- Ticketing & Federation
- Security Provisioning
- Web Entry Services

Communication Security & Crypto-Services

- Virtual Private Networks
- Secure E-Mail & Message Transport
- PKI & Digital Signature Services
- Smartcard & Token Support

Platform Security

- Virus & Malware Protection
- Network Zoning & Network Access Control
- Secure Logging, Monitoring, Backup, IT Continuity
- (Mobile) Client-, Server- & DB-Hardening



SECURITY SERVICES

IDENTITY & ACCESS MANAGEMENT

Triple-A-Services

- Authentication, Authorization, Accounting

Ticketing & Federation

- Secure Delegation, Secure Propagation
- SAML, Kerberos, Single Sign On

Security Provisioning

- Provisioning & Deprovisioning
- Rules & Roles
- User Management, Workflow Security

Web Entry Services

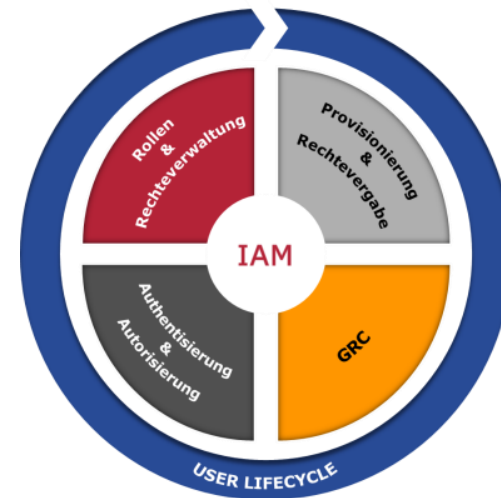
- WAF, WAM, Web Services Security (SOAP/XML)
- Application Server Security & Application Management



SECURITY SERVICES

IDENTITY & ACCESS MANAGEMENT

- Ermittlung organisatorischer und technischer Anforderungen und Rahmenbedingungen
- Etablierung einer einheitlichen und sicheren Registrierung und Verwaltung aller Benutzer von IT-Ressourcen
- Sichere, benutzerfreundliche Anmeldung (Identifikation und Authentisierung) der Benutzer auf allen Ebenen der Informationstechnik (Netzwerk, System, Anwendung)
- ordnungsgemäße Verwaltung von (Benutzer-) Rollen und Berechtigungen, sowie kontrollierte Zuweisung/Nutzung von Sonderrechten



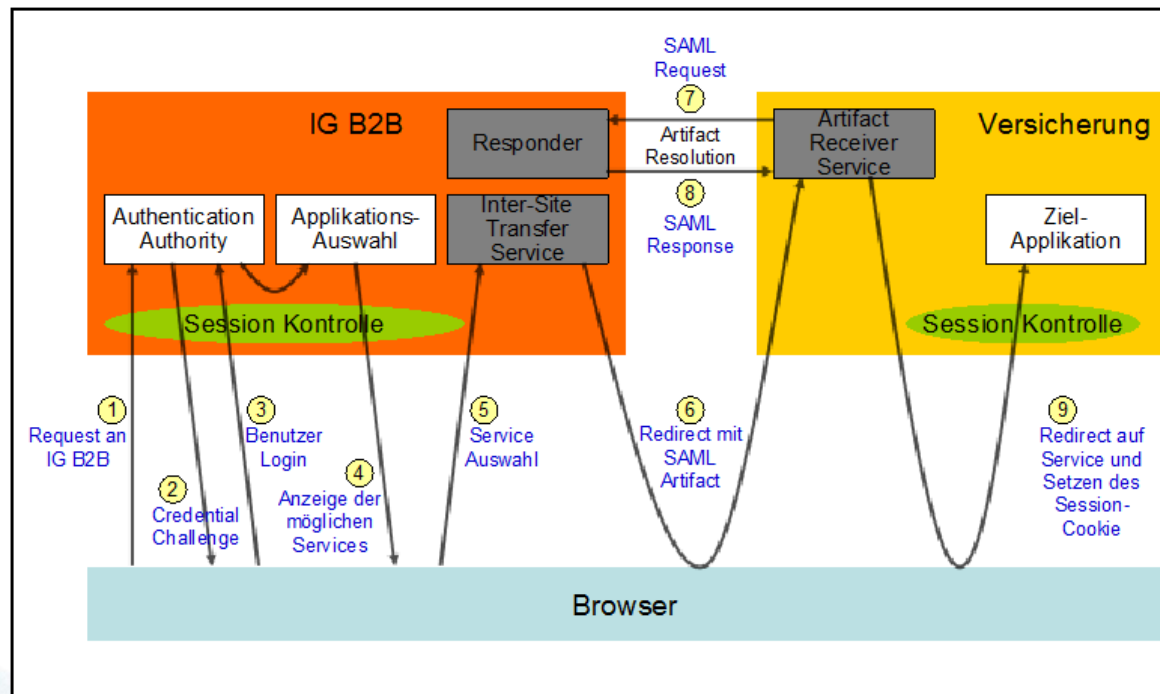
*«Alle Stadien im Lebenszyklus von Benutzerzugängen
– von der erstmaligen Registrierung bis zur endgültigen Löschung von
Benutzern – sind unter Kontrolle»*



SECURITY SERVICES

IDENTITY & ACCESS MANAGEMENT

Identity Platform: Ablauf Single Sign On (SAML Browser/Artifact Profil)





IDENTITY & ACCESS MANAGEMENT

DIENSTLEISTUNGSPAKET

- Das **Rollen- & Rechte-Konzept** als Bestandteil einer unternehmensweiten IAM-Lösung beinhaltet:
 - die Erarbeitung eines Rechte-Inventars durch die Berücksichtigung relevanter Prozesse, Tätigkeiten und Funktionen
 - die Konsolidierung und Kategorisierung einzelner Rechte in adaptierbare und sich ergänzende Rollen (hierarchisches Rollen-Inventar)
 - die Umsetzung des Rollen- und Rechte-Konzeptes in der Systemlandschaft (Provisionierung in die Zielsysteme) mit skalierenden Authentisierungs- und Autorisierungskomponenten
 - die Etablierung von Prozessen zur Rollen- und Rechte-Pflege
- Ein Rollen- & Rechte-Konzept hilft, IT-Verwaltungskosten zu senken und gleichzeitig die Sicherheit zu erhöhen
- Die Integration in ein bestehendes ISMS ist gut machbar



IDENTITY & ACCESS MANAGEMENT

REFERENZEN

Grossbank (2004/05)	Technisches Realisierungskonzept für eine auf Rollen und Regeln basierende Autorisierungslösung in der CRM-Applikation
Grossbank (2005)	Unterstützung bei der Einführung einer systemübergreifenden UNIX Zugriffskontrolle insb. Design eines sicheren Wartungszugangs
Grossbank (2005/06)	Fulltime-Mitarbeit im Web-Entry-Server-Engineering Team (inkl. Betreuung der B1-Schnittstellen und das Applikationsmanagements)
Transportunternehmen (2005/06)	Konzeption für die Ablösung des bestehenden IAM-Systems (inkl. Sicherstellung des laufenden Betriebs, Planung der optimalen Ersatzinvestition)
Grossbank (2006)	Sicherheitsreview der globalen IAM-Infrastruktur insb. Ist-Aufnahme und Inventarisierung bestehender Standard- und Insellösungen, Soll-Definition
Stadtverwaltung (2006 - 2009)	Konzeption und Aufbau der (Web-) Entry-Services Infrastruktur inkl. Virenschutz im Gateway-Bereich
Regulatorische Behörde (2009)	Aufbau eines einheitlichen Rollen- und Rechtekonzepts inkl. Abklärung der Compliance-Anforderungen, anwendungsspezifische Rollenmodellierung
Versicherungsbund (2007 - 2010)	Design und Aufbau einer Identitätsmanagement-Plattform für die Zugriffe von Brokern auf die Informatik-Infrastrukturen eines Versicherungsbundes
Bundesamt (2010)	Grobkonzept eines teilautonomen IAM-Systems für die Verrechnung von Online-Services inkl. Screening, Test und PoC potentieller Werkzeuge
Privatbank (seit 2005)	Planung, Konzeption, Evaluation, Realisierung und Einführung einer firmenweiten Identity & Access Management Infrastruktur
Versicherung (seit 2008)	Erstellung des Pflichtenhefts, Evaluation der Komponenten und technische Projektleitung bei der Einführung eines neuen Identitätsmanagements



SECURITY SERVICES

COMMUNICATION SECURITY & CRYPTO-SERVICES

Virtual Private Networks

- IPSec, SSL/TLS, Secure Remote Administration Access

Secure E-Mail & Message Transport

- Mail & Message Boundary Services, Spam Filtering

PKI & Digital Signature Services

- Secure Login Services
- Folder-, Disk- & File-Encryption
- CA Hierarchies, CP/CPS, Certificate Service Provisioning
- Secure Document-Transport, -Verification & -Archiving

Smartcard & Token Support

- Token Management Systems, High Security Moduls



SECURITY SERVICES

COMMUNICATION SECURITY & CRYPTO-SERVICES

- Gewährleistung der Vertraulichkeit, Integrität und Authentizität von Informationen – sowohl im gespeicherten Zustand als auch während des Transports über elektronische Medien und Kanäle
- Analyse, Konzeption und Umsetzungen von technischen und betrieblichen Prozessen zur Verschlüsselung und digitalen Signatur von Daten, Nachrichten und Dokumenten
- Aufbau von Infrastrukturen und betrieblichen Prozessen zur Bereitstellung und Verwaltung kryptografischer Schlüssel und Zertifikate

«Sensitive Informationen und Daten sind sowohl im gespeicherten Zustand als auch während des Transports vor unberechtigter Offenlegung und Manipulation geschützt»



SECURITY SERVICES

COMMUNICATION SECURITY & CRYPTO-SERVICES

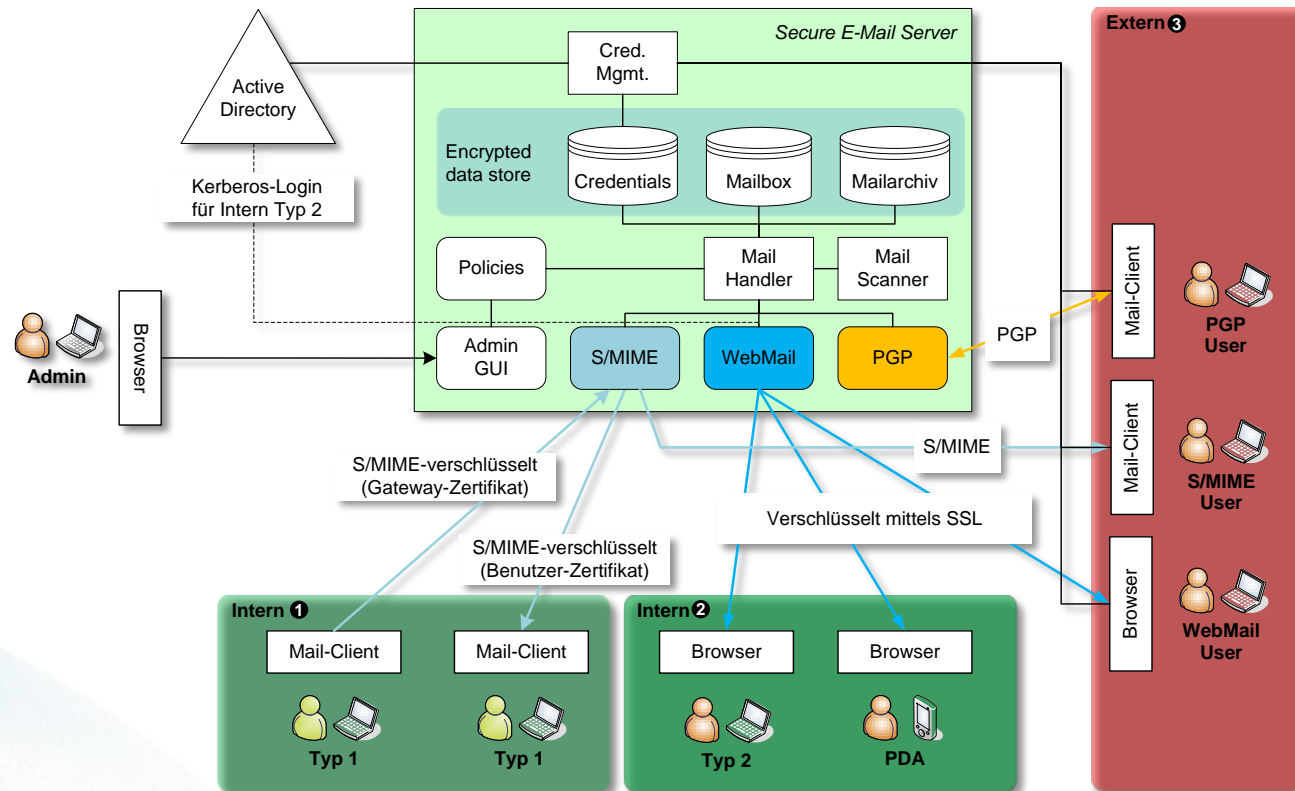
- Gesteigertes Bedürfnis nach **sicherer E-Mail Kommunikation** innerhalb eines Unternehmens, sowie nach „aussen“
- Dienstleistungsumfang **Secure E-Mail**:
 - Unterstützung beim Design und der Konzeption der Ziellösung (Gateway-resp. End-2-End-Ansatz, Berücksichtigung der firmeninternen Kommunikation, unterstützte Protokolle, etc.)
 - Evaluation der Produkte resp. der Lösungslieferanten
 - Realisierung, Testing und Einführung der Gesamtlösung inkl. Schulung der Mitarbeiter im sicheren Umgang (Awareness)
 - Befristete, selektive Betriebsunterstützung nach der Einführung
- Breite Erfahrung mit diversen Produkten, Lösungsansätzen und der Integration in Systemlandschaften (Customizing), bspw. hinsichtlich der Integration in die Exchange-Infrastruktur oder der Anbindung an die eigene PKI-Lösung



SECURITY SERVICES

COMMUNICATION SECURITY & CRYPTO-SERVICES

Secure E-Mail Infrastructure





COMM. SECURITY & CRYPTO-SERVICES

REFERENZEN

Bundesamt (2002)	Umfassendes Sicherheitskonzept für den Aufbau einer Services-PKI für die öffentliche Verwaltung beim Bund, in den Kantonen und Städten
Bundesamt (2003)	Erstellung von Prozessdefinitionen und WTO-Ausschreibungsunterlagen für ein bundesweites Smartcard Management System
Grossbank (2003 - 2006)	Erstellung von Sicherheitskonzepten und Spezifikationen bezüglich der Einführung von Maschinen- und Personenzertifikaten ins Online Banking
Pharmakonzern (2006)	Risikoanalyse bezüglich krypto-analytischer Attacken auf die Hash Funktionen der Algorithmen SHA1 und MD5
Bundesamt (2004 - 2008)	Konzeption, Evaluation und technische Leitung des Projekts für den „Relaunch“ des sicheren Austauschs von „E-Messages“ im Bundesnetz
Grossbank (2005 - 2009)	Erstellung von Zertifikatsspezifikationen, Sicherheitskonzepten und Einsatzrichtlinien beim weltweiten Rollout der Public Key Infrastruktur
Energiekonzern (2009)	Konzeption und Projektleitung beim Aufbau eines PKI-gestützten, konzern-weiten und mandantenfähigen Secure E-Mail Services
Energiekonzern (2009/10)	Business-Case, Architektur, Prozessdefinitionen, PoC, Pilotierung und Einführung einer Services-PKI (inkl. Zertifikatsträger, TMS, Middleware, HSM)
Energiekonzern (2009/10)	Analyse der PKI Marktsituation in Bezug auf Implementierungsstrategien (Produkte, Service Providers), PKI Anwendungsbereiche und Kosten
Versicherung (seit 2010)	Technische Projektleitung bei der Konzeption, Pilotierung, Einführung und Optimierung der Infrastruktur für die Verschlüsselung von E-Mails
Beratungsunternehmen (2011)	Durchführung eines Strategie-Workshops für die Konsolidierung und mögliche Erweiterung der bestehenden PKI (inkl. Produkte-Evaluation)



SECURITY SERVICES

PLATFORM SECURITY

Virus & Malware Protection

- Active Vulnerability & Emergency Management
- Network Zoning & Network Access Control

Network Zoning Concepts

- SAN/NAS Security
- Secure Virtualization, Secure Cloud Computing

Secure Logging, Monitoring, Backup, IT Continuity

- Base Line Security (Guidelines & Standards)
- Security Incident Management
- Secure Resource Utilization

(Mobile) Client-, Server- & DB-Hardening

- Systems Security (OS & Middleware)



SECURITY SERVICES

PLATFORM SECURITY

«IT-Systeme werden sicher geplant, gebaut und betrieben»

- Konzeption und Bereitstellung integrier IT-Plattformen (Client-, Server- und Datenbank-Betriebssysteme und Middleware)
- Design und Implementierung sicherer Server- und Speicherkonzepte (inkl. Virtualisierung und Cloud Computing)
- Schutz von IT-Systemen und Daten vor Schadsoftware (Malware) und Schwachstellen (Vulnerabilities)
- Analyse und Optimierung von Netzwerkzonenkonzepten zur Abschirmung sensibler IT-Dienste, -Systeme und Daten
- Durchsetzung von Standard-Sicherheitsmassnahmen (Baseline Security Controls) für einen verlässlichen IT-Grundschutz
- Überwachung sicherheitskritischer Aktivitäten sowie nachgelagertes Security Incident Management



PLATFORM SECURITY

DIENSTLEISTUNGSPAKET

- **Windows 7** bietet aus Business- und Sicherheitssicht neue zeitgemässe Funktionalitäten und ein breites Einsatzgebiet
- Wir bieten 3 Module zur **sicheren Einführung von Windows 7**
 - **Sicherheitsanforderungen:** Identifikation der Anforderungen an Windows 7 auf Basis von allgemein gültigen und systemspezifischen Weisungen und Vorschriften
 - **Umsetzungsrichtlinien:** Erstellung von systemspezifischen Policies und Umsetzungsvorschlägen (Systemkonfiguration)
 - **Sicherheitsprüfung:** Auditierung/Compliance-Check einer konkreten Umsetzung mit Risikoeinschätzung und adäquaten Massnahmen zur Risikoreduktion
- Ebenfalls verfügbar für Outlook und Office 2010, sowie für den Internet Explorer und Firefox
- Anwendbar für Desktops, Notebooks und virtuelle Clients



PLATFORM SECURITY

DIENSTLEISTUNGSPAKET

Ausgangslage: Neue Herausforderungen durch steigenden Bedarf an geschäftlicher Nutzung von Mobile Devices

- Lösung: **Einsatzkonzept für mobile Geräte**
 - **Analysephase:** Situations- & Anforderungsanalyse zur Identifikation der Ausgangslage und der Anforderungen
 - **Risikobetrachtung:** Risikogrobanalyse & Massnahmenkatalog
 - **Machbarkeitsstudie:** techn. & org. Lösungsansätze, Kosten/ Nutzen-Schätzung mit Empfehlung als Entscheidungsgrundlage
 - **Aufwandschätzung:** Grobkostenschätzung & -konzept mit Vorschlag für das Projektvorgehen
- **Nutzen:** Auf die individuellen Kundenbedürfnisse zugeschnittene Sicherheit; Kenntnis der Risiken und Gefahren; Transparenz über die Integration von iPhone & Co.



PLATFORM SECURITY

REFERENZEN

Bauzulieferer (2003)	Erarbeitung eines umfassenden Sicherheitsdispositivs für alle stationären und mobilen Rechner (inkl. Hardening-Vorgaben für Betriebssysteme)
Finanzdienstleister (2005)	Sicherheitskonzept für den Einsatz von mobilen Geräten (Blackberry)
Grossbank (2006)	Erstellung eines Regulativs und von Betriebshandbüchern für die Auslagerung von Teilen der Anwendungsentwicklung nach Indien
Grossbank (2007)	Definition der IT-Sicherheitsanforderungen (inkl. physischer Schutz und Zutrittskontrolle) für die weltweit verteilten Representative Offices
Regionalbanken (2007/08)	Verfassen der Log-Policy, Erstellung des Logging-Konzepts und Design eines zentralen Log-Hosts
Kantonsspital (2008)	Definition von Werkzeugen und Prozessen für das Malware- und Virenschutz-Dispositiv
Pharmabetrieb (2008)	Erstellung einer generisch gefassten Richtlinie für den sicheren Einsatz von Microsoft Sharepoint Instanzen
Energiekonzern (2009)	Evaluation eines Produkts für Network Access Control und Beratung bei dessen Einführung
Versicherung (2009)	Sicherheitsanalyse für die Anbindung eines extern betriebenen Anti-Virus Anti-Spam Filters an das interne E-Mail-System
Grossbank (2010)	Erstellung der Baseline Security Standards und der dazugehörigen technischen Implementation Guidelines für den Einsatz von MS-Windows 7
Versicherung (2011)	Erstellung eines Grobkonzepts „Zentrales Logging“ für die automatisierte Auswertung von Log-Daten für IKS-relevante Systeme und Datenbanken



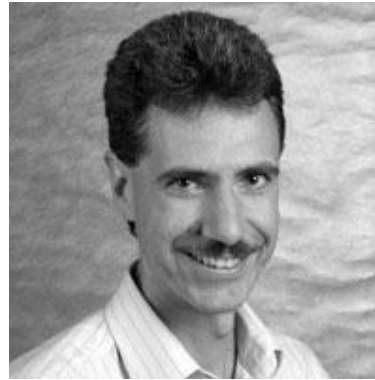
INHALT

Portfolio Überblick	3
Fachbereich Security Management	9
Fachbereich Security Services	23
Kontakt	40

KONTAKT



Tomaso Vasella
Leiter Geschäftsbereich
IT Security
+41 79 339 29 38
tomaso.vasella@inout.ch



Marcel Hausherr
Leiter Fachbereich
Security Management
+41 79 216 75 50
marcel.hausherr@inout.ch



Christoph Aumayer
Leiter Fachbereich
Security Services
+41 79 311 26 54
christoph.aumayer@inout.ch



EFFIZIENTE UND SICHERE IT-INFRASTRUKTUREN.
IHR VORTEIL. UNSER VERSPRECHEN.

In&Out AG IT Consulting & Engineering
Kilchbergsteig 13, CH-8038 Zürich, Phone +41 44 485 60 60, Fax +41 44 485 60 68
info@inout.ch, www.inout.ch