SKyPRO

GRC

Governance, Risk & Compliance

Beratung und praxisorientierte Implementationen rund um die Themen Governance, Risk Management und Compliance (GRC) aus Sicht der Informatik.

LEARN MORE

SKyPRO AG
Gewerbestrasse 7
CH-6330 Cham

+41 41 741 4770

info@skypro.ch

www.skypro.ch

Governance, Risk & Compliance

Governance, Risk & Compliance (oder kurz GRC) fasst die drei wichtigsten Handlungsebenen eines Unternehmens für dessen erfolgreiche Führung zusammen. Die Stärken der SKyPRO liegen in der lösungs- und praxisorientierten Beratung rund um die Themen IT Governance, IT Risk Management und Compliance (GRC), welche die Grundlage einer durchgängigen Informationssicherheit im Unternehmen bilden.

IT Governance

Die IT-Governance besteht aus den Strategien, der Führung und den Prozessen, welche sicherstellen, dass die Informationstechnik (IT) die Unternehmensstrategien und -ziele unterstützt. Dabei muss beachtet werden, dass die angewandte Methodik zur Umsetzung und Planung der notwendigen Ressourcen für das Erreichen der Ziele pragmatisch und ergebnisorientiert ist.

IT Risk Management

Bekannte und unbekannte Risiken werden dabei durch definierte Risikoanalysen entdeckt. Ein wichtiger Faktor dabei ist das frühzeitige Auseinandersetzen mit den möglichen Risiken, der Bereitstellung von Strategien zur Risikominimierung und dem Vorbereiten von Schadensfallpuffern bei Risikoeintritt.

Compliance

Compliance bedeutet das Einhalten von interner wie externer Normen für die Informatik. Diese beinhaltet unter anderem Vorgaben aus Normierungsbestrebungen und die Zugriffsreglementierung für die Daten sowie die gesetzlichen Rahmenbedingungen für deren Verwendung. Das Management und auch die IT-Abteilungen müssen sich heute mit einer immer komplexeren Verteilung von multinationalen Geschäftsbeziehungen, gesetzlichen und gesellschaftlichen Regeln, mit Zielen und deren Vorgaben sowie mit der Umsetzung, Kontrolle und Einhaltung aller diesbezüglichen Prozesse beschäftigen.

IAG - Sicherheit durch Automatisierung

Die SKyPRO erarbeitet, realisiert und b etreibt vollständige I dentity Lifecycle Prozesse zur Verwaltung von Identitäten und deren Berechtigungen über alle IT relevanten Systeme und Anwendungen innerhalb des Betriebes und in der Cloud.

Diese Prozesse beinhalten nicht nur die Verwaltung eines Lebenszyklus, sondern auch die Steuerung von Berechtigungen und Berechtigungsanfragen inklusive deren Genehmigungsprozesse und die Definition von Gewaltentrennungen. Wir konzipieren dabei firmenweite Rollenmodelle, mit dem Ziel, so viele Berechtigungen wie möglich automatisch einem Mitarbeiter auf Grund seines Firmenprofiles zuzuweisen.

SKyPRO

Staatliche Compliance Anforderungen

Auch staatliche Institutionen reagieren mit verschärften Gesetzen und höheren Strafen. Für ein Unternehmen bedeutet dies immer mehr Aufwand um den Compliance-Anforderungen gerecht zu werden. Die im Unternehmen eingesetzten Massnahmen und Prozesse, die zum Ziel haben, die Einhaltung von Gesetzen, Regeln und Richtlinien zu gewährleisten, werden immer aufwendiger. Firmen fangen an zu verstehen, dass eine klare und strukturierte Sicherheitsstrategie auch für das Datenzugriffsmanagement der Benutzer notwendig wird.

Informatik-Effizienz im Unternehmen

In grösseren Betrieben ist ein manuelles Benutzermanagement personell sehr aufwendig und kostenintensiv und zudem eher fehleranfällig. Durch die Automation von Eintritten, Austritten und Mutationen (Identity Life Cycle) erhöhen Sie die Sicherheit und reduzieren gleichzeitig die Kosten.

Durch die zusätzliche Integration eines rollenbasierenden Berechtigungsmodells (RBAC), in welchem dem Mitarbeiter nur minimale Zugriffsberechtigungen zugewiesen werden, unterstützt dabei den Sicherheitsgedanken. Real-Time-Dashboards und regelmässig vorgefertigte Sicherheitsberichte ergänzen eine gute und sichere Identity and Access Governance-Lösung (IAG), welche den Kern einer durchgängigen Informationssicherheit im Unternehmen im Sinne einer lösungsorientierten GRC-Strategie bildet.

SKyPRO

Mit unseren Lösungen sorgen wir für die Prüfung und Durchsetzung von Unternehmensrichtlinien und Prozessen. Wir senken die Gefahr von Sicherheitslücken, verkürzen die Reaktionszeiten, erhöhen die Transparenz und vereinfachen die Compliance Aufgaben.

Mit unserer Hilfe können Sie die Einhaltung von internen und externen Richtlinien, Kosten und Ressourcen schonend nachweisen und die eingesparten Mittel in den Ausbau des Unternehmens investieren.

Durchgängige Transparenz

Compliance Management Lösungen schöpfen das Potential der Infrastrukturlösungen aus: Sie verringern die Business Governance und die Risiken und sorgen damit für Compliance im gesamten Unternehmen.

Mitarbeiter Übertritt

Wechselt ein Mitarbeiter seine Funktion, in eine neue Abteilung, an einen neuen Standort oder übernimmt eine neue Führungsfunktion usw. muss sichergestellt werden, dass über das Rollenmodell Berechtigungen seiner alten Funktion, die er nicht mehr benötigt, automatisch entzogen werden. Auf der anderen Seite müssen neue Rollen, die er aufgrund seiner neuen Funktion gemäss Rollenmodell benötigt, automatisch zugewiesen werden. Ausserdem müssen individuelle Rechte, die der Mitarbeiter zusätzlich zum Rollenmodell besitzt, überprüft und ggf. entzogen werden. Übergangsfristen, in welchen sowohl der neue als auch der alte Vorgesetzte einbezogen sind, müssen geregelt werden.

Mitarbeiter Eintritt

Beim Eintritt erhält der Mitarbeiter automatisch alle notwendigen Accounts und Berechtigungen, die er für die Durchführung seiner täglichen Arbeiten benötigt. Auf Grund seiner Profildaten wie Firma, Division, Abteilung, Funktion, Standort, Führungsstufe usw. werden ihm automatisch Berechtigungsrollen auf Basis eines firmenweiten Rollenmodells zugewiesen. Hierbei gilt das «least privilege» Prinzip. Das bedeutet so viel wie nötig aber so wenig wie möglich.

Der Identity Life Cycle Prozess

Das Fundament von Identity & Access Governance

Mitarbeiter Austritt

Verlässt ein Mitarbeiter den Betrieb muss sichergestellt werden, dass am Ende seines letzten Arbeitstages (nicht am Austrittsdatum) alle seine Konten und Berechtigungen auf allen Anwendungen umgehend gelöscht oder zumindest deaktiviert werden. Danach müssen automatische Prozesse garantieren, dass persönliche Daten, wie Emails oder Dateien (Home Folder) korrekt archiviert werden.

Rollenmodellierung

Das firmenweite Rollenmodell bildet die Basis für sämtliche Berechtigungen aller Mitarbeiter. Die Konzeption und der Unterhalt des Rollenmodells ist anspruchsvoll und verlangt nicht nur ein fundiertes applikatorisches und internes Sicherheits-Fachwissen, sondern auch nach unterstützenden Arbeitsmitteln, die den Rollenfindungs- und Bildungsprozess vereinfachen. Mit was-wäre-wenn Analysen helfen Sie das Rollenmodell den stets wechselnden Anforderungen des Unternehmens schnellstmöglich gerecht werden zu können.

SKyPRO

User Self Service

Zusätzliche Berechtigungen (Rollen), die ein Mitarbeiter ggf. benötigt, werden über ein Self Service Kiosk den Mitarbeitern zur Verfügung gestellt. So kann der Helpdesk, ein Vorgesetzter für seine Mitarbeiter oder der Mitarbeiter für sich selbst neue Rollen beantragen. Entsprechende Genehmigungsprozesse stellen sicher, dass die Berechtigungen erst nach genauer Überprüfung und Genehmigung durch die verantwortlichen Personen (durch den Vorgesetzten, Application Owner, Sicherheitsbeauftragten etc.) automatisch zugeteilt werden.

Passwort Selbstbedienung

Passwörter unterliegen strengen Richtlinien. Mitarbeiter müssen regelmässig Ihre Passwörter ändern und Passwörter müssen eine gewisse Komplexität erfüllen. Die mehrfache Verwendung gleicher Passwörter ist nicht erlaubt. Das alles führt dazu, dass Passwörter vergessen werden. Die Mitarbeiter müssen eine einfache aber sichere Möglichkeit erhalten, vergessene Passwörter wiederherzustellen oder neu zu setzen.

Stellvertretung und Delegation

Sobald elektronische Prozesse ins Spiel kommen, müssen auch Vertretungs- und Delegationsfragen gelöst werden. Was geschieht bei ferien- oder krankheitsbedingten Abwesenheiten? Wer darf im Namen von wem welche Anfragen beantworten. Wie wird die Nachvollziehbarkeit sichergestellt, wenn Aufgaben delegiert oder stellvertretend genehmigt wurden.

Rezertifizierung

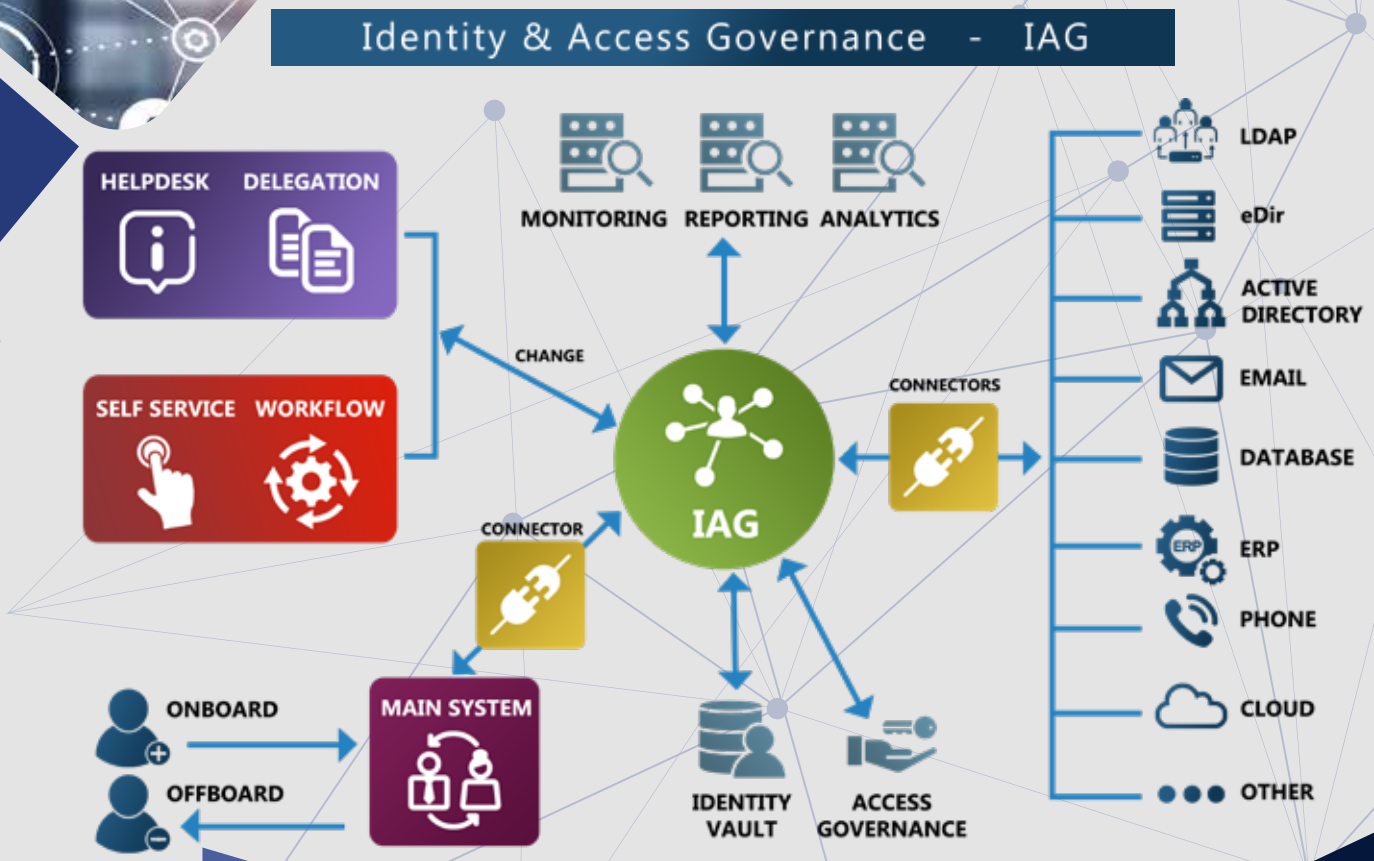
Rollen und deren Berechtigungen, die einem Mitarbeiter zugewiesen wurden, müssen regelmässig kontrolliert werden. Risiko Analysen helfen Mitarbeiter mit hohem Sicherheitsrisiko zu ermitteln. Berechtigungen oder Mitarbeiter mit hoher Risikoeinstufung müssen in kürzeren Perioden kontrolliert werden als weniger kritische. Diese Prozesse müssen automatisiert durchgeführt und kontrolliert werden, damit regulatorische Anforderungen wie auch eigene Sicherheitsrichtlinien so einfach wie möglich eingehalten werden können. Aber auch das Rollenmodell selbst muss regelmässig überprüft werden, da z.B. auf Grund von Restrukturierungen das Berechtigungskonzept angepasst werden muss.

Reporting

Regelmässig und automatisiert ausgeführte Berichte über aktuelle und vergangene Berechtigungszuweisungen aus Sicht der Rolle (welche Rolle wurde welchen Benutzern zugewiesen) wie auch aus Sicht der Benutzer (welcher Benutzer besitzt welche Rollen) erleichtern den Compliance Nachweis. Reports über durchgeführte Berechtigungsanträge, Änderungen am Rollenmodell oder Änderungen an den Benutzerdaten unterstützen Sie bei den täglichen Sicherheitsanforderungen.

Die Grundlagen einer wirksamen Identity & Access Governance-Lösung

Durch die Zentralisierung von Identitätsdaten, Rollen, Geschäftsrichtlinien und Risikomodellierung werden Compliance-Initiativen sowie die Verwaltung des Lebenszyklus von Benutzerkonten unterstützt. Sie dient zur Erfassung von Geschäftsrichtlinien, zur Rollenmodellierung und zur proaktiven Verwaltung von Daten und Risiken, die mit Benutzern und Ressourcen verbunden sind.



SKyPRO

Die 3 Funktionspfeiler einer guten IAG-Lösung

1. Identity Management

Zu den Kernfunktionen einer IAG-Lösung gehören die Integration unterschiedlicher firmeninterner Systeme und die Synchronisation derselben. Das Resultat ist eine vollautomatisierte Provisionierung der Identitäten in die Umsysteme über sogenannte Konnektoren.

Weitere Funktionen umfassen die Einbindung von Cloud Lösungen und externen Benutzern. Des Weiteren sollten möglichst viele Self-Service-Systeme umgesetzt werden wie White-Pages und Passwort-Reset.

2. Access Governance

Wer seine IAG-Lösung mit einer rollenbasierten Rechteverwaltung RBAC verknüpft, sichert sich Vorteile nicht nur im Hinblick auf Sicherheit. Es winken zusätzlich Kosteneinsparungen und transparentere Prozesse. Dabei helfen beim Rollenmanagement der Einsatz sogenannter Role-Mining-Werkzeuge. Diese analysieren sowohl die Prozesse wie auch die Strukturen des Unternehmens. Die Einrichtung einer rollenbasierten Rechteverwaltung sollte zunächst mit einem grundlegenden Aufräumen beginnen. Dieser „Cleansing" genannte Vorgang schafft die Voraussetzung für ein künftig sauberes Rollenmanagement und besteht aus einer Bereinigung aller Daten.

Besonders auch im Hinblick auf eine aktive Unterstützung des Risk-Managements hat die Definition von Business- und IT-Rollen zur Einhaltung spezifischer Compliance-Anforderungen eine zentrale und tragende Aufgabe.

3. Compliance Monitoring, Analytics & Reporting

Die SKyPRO führt bei Ihren Kunden regelmässige Risiko-Analysen durch. Diese bilden die Grundlage zur Definition und Durchführung von Rezertifizierungen bestehender Berechtigungen.

Die Erfahrung zeigt auch, dass Vorgaben nur durch permanente Überwachung, durch regelmässige Analysen und Kontrollen durchgesetzt werden können. Die SKyPRO-Lösungen verfügen über ein Audit and Compliance Dashboard (ACD). Das SKyPRO ACD verfügt über konfigurierbare Real-Time-Dashboards, Past-Activity (historical) Dashboards sowie detaillierte Reports und ein Activity-Logging.

Eine identitätsbasierende Sicherheitslösung reduziert die Risiken

Die Datensicherheit ist eine der fundamentalsten Grundvoraussetzungen eines modernen Unternehmens. Milliarden werden aufgewendet für Firewall-Lösungen, VPNs und Fingerabdruckscanner und trotzdem, all dies genügt noch nicht: 2018 gab es immer noch 6,515 Datenpannen und über 5 Milliarden gestohlene Datensätze. Will man Daten effektiv schützen, so muss man den Weg zu ihnen absichern. Hier kommen Identitäten und Berechtigungen ins Spiel. Der Weg zur Sicherheit führt folglich unausweichlich über die digitale Identität und deren Management.

Was Sie jetzt tun sollten

1. Prozess- & Workflow Automatisation

Stellen Sie sicher, dass alle Prozesse, welche automatisiert sein können, auch effektiv automatisiert sind. Setzen Sie Self- Service- Systeme für Prozesse wie den Passwort-Reset und die Datenzugriffs-Berechtigung ein.

2. Rollenbasierende Rechteverwaltung

Erstellen Sie ein firmenweites Rollenmodell, mit dem Ziel möglichst alle Berechtigungen (Daten und Anwendungen) automatisiert zuweisen zu können. Gruppieren und klassifizieren Sie alle Daten innerhalb Ihres Betriebes. Stufen Sie diese bezüglich des Gefahrenpotentials ein und weisen der jeweiligen Datengruppen eine verantwortliche Person zu.

3. Kontinuierliches Monitoring (Reporting & Auditing)

Führen Sie ein regelmässiges Reporting und Auditing durch. Jeder Zugriff auf Ihre Systeme und die Daten des Unternehmens muss überwacht werden. Eine gute Governance Lösung erkennt und präsentiert zu jedem Zeitpunkt anhand von Dashboards den momentanen Zustand Ihres Systems.

SKyPRO

Andreas Fuhrmann
CEO SKyPRO Switzerland

Horst Fuhrmann
CEO SKyPRO USA / SKyPRO Ukraine

Wer sind wir

Die SKyPRO AG ist ein IT Dienstleistungsunternehmen mit über 30 Jahren Erfahrung. Hierbei bieten wir innovative IT Lösungen unter der Verwendung modernster Technologien. Seit über 19 Jahren konzentriert sich die SKyPRO AG auf die Realisierung komplexer Identity & Access Governance und Security Lösungen in Banken, Versicherungen, Industrie und Verwaltungen.

Was ist unser Ziel

Ziel ist die vollständige Erfüllung all Ihrer Identity Governance, IT Risk Management und Compliance Anforderungen (GRC) sowie die weitgehende Automatisierung aller Identitäts-Prozesse. Die automatisierte Vergabe von Berechtigungen, klar definierte Antrags- und Genehmigungsprozesse und übersichtliche Reports vereinfachen den Nachweis der Einhaltung aller externen wie auch internen Regulatorien und Richtlinien.

SKyPRO AG
Gewerbestrasse 7
CH-6330 Cham

+41 41 741 4770

info@skypro.ch

www.skypro.ch