ESPRESSO TUTORIALS

Bianca Folkerts

Praxishandbuch für die Risikoanalyse mit SAP® GRC Access Control

- Design und Ausprägung eines Risikokatalogs
- Wartung und Erweiterung des Regelwerks
- Risikoanalysen interpretieren
- Best-Practice-Ansätze zur Risikobereinigung

Inhaltsverzeichnis

Vorwort **7**

1 Risikokatalog **13**
1.1 Die Funktion 14
1.2 Das Risiko 38
1.3 Organisationsregeln 51
1.4 Zusatzregeln 53
1.5 Die Kontrolle 54

2 Definition und Anpassung des Risikokatalogs **59**
2.1 Tun Sie Gutes und reden Sie darüber – gute Gründe für ein Risikomanagement-System 60
2.2 Die Erstellung eines Risikokatalogs 62
2.3 Kontext »Transportsystem« 74
2.4 Rollout neuer Regelwerke 89
2.5 Risikokataloge von Drittanbietern 94

3 Risikoanalyse **97**
3.1 Anwendungsmöglichkeiten 98
3.2 Die Ad-hoc-Analyse 103
3.3 Die Simulation 112
3.4 Die Batch-Analyse 113
3.5 Risikoterminator 117
3.6 Ausführungsreports für »Alerts« 119
3.7 KPIs der Risikoanalyse 121

4 Risikobereinigung **123**
4.1 Definition der Projektziele 124
4.2 Die Beteiligten 125
4.3 Definition des Risikokatalogs 126

4.4 Schritte der Risikobereinigung 129
4.5 Umgang mit technisch und prozessuell nicht vermeidbaren Risiken 141

5 Integration der Risikoanalyse in den Rollen- oder Benutzerworkflow 147
5.1 Möglichkeiten der Integration 147
5.2 Vorarbeiten und Zeitpunkt der Integration 149
5.3 Was tun bei einer notwendigen Erweiterung oder Anpassung des Risikokatalogs? 151
5.4 Vor- und Nachteile einer Integration 152

6 Tipps & Tricks 153
6.1 Customizing und Co. 153
6.2 Hausmeistertätigkeiten 154
6.3 Berechtigungsobjekte im Access Risk Analysis 156

7 Fazit 159

A Die Autorin 162

B Index 165

C Disclaimer 169

2 Definition und Anpassung des Risikokatalogs

Ein Tool zur Risikoanalyse eingeführt zu haben, stellt nicht sicher, auch regelkonform – also »compliant« – zu agieren. Das Tool will richtig gefüttert und bedient werden. Dies geschieht bei GRC Access Control (u. a.) in der kundenangepassten Ausprägung des Risikokatalogs. Und genau dies stellt die meisten Firmen vor eine schier unüberwindbar anmutende Hürde. Zugegebenermaßen ist die Erstellung und insbesondere Wartung eines Risikokatalogs aufwendig. Jedoch kann der Katalog, zusammen mit den entsprechenden Prozessen zur Behandlung neuer oder offener Risiken sowie deren Review, einen enormen Benefit bringen.

Da dieser Aspekt für die Konfiguration eines Systems zur Risikoanalyse so enorm wichtig ist, möchte ich vorab noch einmal die Performance ansprechen. Je nach Anzahl der angebundenen Systeme und implementierten Risiken (bzw. der Anzahl der daraus generierten Regeln) kann es zu Performance-Problemen kommen. Eine generelle Aussage, »ab wie vielen Systemen« oder »ab wie vielen Regeln« dies passiert, kann kaum getroffen werden, da hier viele Komponenten wie etwa die Datenbank, das Sizing etc. hineinspielen. Daher sollte dem Design, der Pflege und der Zuordnung zu Funktionen von Konnektorgruppen (siehe Abschnitte 1.1.2 bzw. 1.1.4) besondere Sorgfalt zuteilwerden. Die oft von der IT und Beratern vorgeschlagene Lösung, zur Optimierung der Performance doch bitte ein paar Risiken zu löschen oder wenigstens zu deaktivieren, ist aus fachlicher Sicht nicht akzeptabel. Es ist schließlich das Ziel von Access Risk Analysis, alle möglichen Risiken aufzuzeigen, um diese zu behandeln. Von einem Buchhalter würde man auch nicht verlangen, doch bitte ein paar Buchungskreise zu löschen oder zusammenzufassen, damit die Batch-Verarbeitung etwas schneller läuft. Bei massiven Performance-Problemen müssen andere, technische Lösungen gefunden werden. Die regeloptimierte Anlage der Risikomatrizen ist dann unverzichtbar.

Deaktivierung von Risiken aus Performance-Gründen ist nicht zielführend

Ist ein Risikokatalog schon regeloptimiert (also die Anzahl der Regeln minimiert), so sollte dringend von einer Deaktivierung von Risiken aus Gründen der Performance abgesehen werden.

2.1 Tun Sie Gutes und reden Sie darüber – gute Gründe für ein Risikomanagement-System

Bei der Definition und Auswertung von Risiken höre ich immer wieder Phrasen wie:

- »Wer soll denn die ganze Arbeit machen?«
- »Da dauert ja die Bearbeitung eines Antrags Wochen!«
- »Das zu verstehen, benötigt Wochen!«

Sie spiegeln die heutzutage fast normale und auch gut nachvollziehbare Befürchtung von noch mehr Arbeit wider.

Ich beantworte diese Reaktionen gerne mit einer beratertypischen Gegenphrase »Ja, aber …«:

»GRC Access Control macht Risiken nur einfacher sichtbar. Theoretisch ist ein Unternehmen auch ohne SAP Access Control verpflichtet, Risiken transparent zu machen und zu minimieren!«

Oder auch:

»Wollten Sie nicht immer schon mal eine Auswertung auf Knopfdruck darüber haben, wer alles auf ihre Daten/Prozesse zugreifen kann?«

Spätestens dann wird der Kollege seine spontane erste Schutzreaktion überdenken und zum Einlenken neigen (auch wenn er das erst einmal nicht zugeben mag): Die Erfüllung der rechtlichen Anforderungen

ist ohne Tool nahezu unlösbar, da viel zu komplex, fehleranfällig und zeitraubend. Daher wurden entsprechende Maßnahmen (bis zur Einführung von SAP Access Control) in den Unternehmen einfach nicht umgesetzt. Eine Lösung? Wohl eher nicht.

Vermarkten Sie die Risikoanalyse als Erfolgsfaktor

Arbeiten Sie nicht mit erhobenem Zeigefinger, sondern vermarkten Sie die Zeitersparnis und den Transparenz-Gewinn. Dann werden Ihre Kollegen das Projekt schon nicht mehr ganz so argwöhnisch betrachten, sondern schnell begreifen, dass SAP Access Control ihnen eigentlich das Leben leichter macht und sie sich vor allem durch dessen Einsatz viel mehr um ihre eigentlichen Aufgaben kümmern können.

Oft werden GRC-Access-Control-Systeme ohne jegliches begleitendes »Marketing« eingeführt. Auslöser ist meist ein entsprechender Eintrag im Audit. Dort wird dann z. B. ein Tool für die Beantragung und Genehmigung von Benutzern oder auch die Implementierung eines Risikokatalogs gefordert. Sehr häufig verkommt dieses Tool anschließend zu einem reinen Werkzeug der »Auditorenbefriedigung«. Das dürfte nicht nur bei SAP GRC Access Control der Fall sein, sondern auch für jedes andere Tool mit entsprechenden Funktionalitäten gelten.

Compliance-Tools zur Auditorenbefriedigung?

Wenn Sie für die Einführung eines GRC Access Controls verantwortlich oder an ihr beteiligt sind, überlegen Sie sich genau, ob Sie das Argument »Die Auditoren fordern den Einsatz des Tools« wirklich zum Überzeugen nutzen wollen. Erinnern Sie vielmehr daran, dass dieses Tool die Zugriffsrisiken minimieren soll und somit die Sicherheit im Unternehmen zum Ziel hat. Der Einsatz und eine entsprechende Nutzung erhöhen somit – richtig begründet – das Vertrauen in das Unternehmen. Durch passgenaues Marketing erhöhen Sie den Nutzen und Benefit des Tools über dessen eigentliche Funktionalitäten hinaus!

2.2 Die Erstellung eines Risikokatalogs

Ich gehe hier zunächst darauf ein, wie Sie einen neuen Risikokatalog erstellen. Aus dieser Vorgehensweise lassen sich leicht die Schritte für die Anpassung eines bestehenden Risikokatalogs ableiten.

2.2.1 Geschäftsprozesse – Transparenz ist gefragt

Wie bereits in Abschnitt 1.1 erwähnt, ist der Risikokatalog an den genutzten Geschäftsprozessen orientiert. Daher ist eine Dokumentation dieser Geschäftsprozesse und der untergeordneten Schritte essenziell. Theoretisch sollte eine Dokumentation in jedem Unternehmen bereits vorliegen. Oft ist dies erstaunlicherweise jedoch nicht der Fall. In diesem Fall muss sie zunächst erstellt werden. Der für diesen Zweck notwendige Detaillierungsgrad kann variieren. Grundsätzlich empfehle ich eine ähnliche Granularität wie in Berechtigungskonzepten für Einzelrollen (bei geschäftsprozess- und arbeitsplatzorientierten Konzepten).

Die Definition kann im Rahmen von Workshops erfolgen.

2.2.2 Evaluation von Risiken – kriminelle Gedanken erwünscht!

Workshops zur Definition von konfliktären Geschäftsprozessschritten oder auch einzelnen Funktionalitäten können sowohl dem Moderator als auch allen anderen Beteiligten sehr viel Spaß bringen.

Was wäre, wenn … – der Moderator ist gefragt

Zu überlegen, wie man welchen Schaden herbeiführen kann, entspricht so gar nicht der normalen Alltags-Denkweise. Dem Moderator kommt hier die wichtige Aufgabe zu, den Teilnehmern das Gefühl zu geben, dass diese Gedanken erwünscht und okay sind.

Als Moderator sollten Sie sich zuvor ein oder besser mehrere zu den Aufgabengebieten der Teilnehmer passende Beispiele überlegen, was mit bestimmten Berechtigungskombinationen bewirkt werden kann. Machen Sie es anschaulich!

Anschauliche Verdeutlichung eines Risikos

zB

In einem Workshop mit Buchhaltern wäre die folgende Illustration angebracht:

»Sie haben die Berechtigungen, Bankdaten eines Kreditors zu ändern und dürfen gleichzeitig Rechnungen mit Bezug zu diesem Kreditor buchen. Sie könnten somit Ihre eigene Kontonummer hinterlegen, einen Wareneingang buchen und eine Eingangsrechnung auf diesen Kreditor erfassen, obwohl keine Leistungen erbracht wurden. Würde das jemandem auffallen?«

In einem Workshop mit IT- oder Basis-Kollegen würde hingegen Folgendes sicherlich besser ankommen: »Stellen Sie sich vor, jemand würde im Entwicklungssystem sämtliche Versionshistorien löschen. Was würden Sie beim nächsten Upgrade bei der SPAU machen?«

Einen Lageristen würden Sie wohl eher fragen: »Wenn Sie in der Lage sind, Warenbewegungen zu buchen und außerdem eine Inventur im System durchführen könnten – würde es auffallen, wenn Sie – weil Sie gerade ein Haus bauen – Baumaterialien aus dem Lager entwenden?«

Stellen Sie am Anfang eines Workshops nicht direkt Risiken im herkömmlichen Sinne (finanzieller, betrieblicher Verlust, Verstoß gegen Gesetze …) in den Mittelpunkt. Betrachten Sie zunächst ganz praktische Fragestellungen, wie z. B.:

- Auf welche Daten/Funktionalitäten sollen ausschließlich Mitarbeiter eines bestimmten Bereiches Zugriff haben?
- Welche Tätigkeiten im System würden den Monats-/Jahresabschluss gefährden?

B Index

A

Access-Risk-Verantwortlicher 49
Aktion 22, 23, 25
Aktionssynchronisation 154
Aktionsverwendung 137
Alarm 145. Siehe Alert
  Transaktionsaufruf 120
Alert 119
Analyseart 27
  Berechtigungsebene 27
  kritische Aktion 28
  kritische Berechtigung 28
Analyseumfang 20, 41
  Einzelsystem 20
  Systemgruppe 20
  systemübergreifendes Risiko 20
Änderungsbeleg 87
Änderungshistorie 87
Änderungsprotokolle 87
Änderungsworkflow 88

B

Batch-Analyse. Siehe Risikoanalyse
Benutzeränderungsworkflow 147
Benutzerantragsworkflow 98
Benutzerfreundlichkeit 15, 26, 27
  Performance 30
Benutzerzugriffsprüfung 154
Berechtigung 22, 23
  Status 31
Berechtigungsebene 27
Berechtigungsgruppe 24, 29
Berechtigungsobjekt 14, 156
Berechtigungssynchronisation 24
Boolescher Operand 28, 34

C

Cross-System-Funktion 21

D

Dashboard. Siehe Risikoanalyse
Download 78
  Download-File 80
  Modifikation 82, 84

E

Einzelrolle
  Mitigation 133

F

False Positive 31, 51
Finding 45
Funktion 14, 16, 45

G

Geschäftsprozess 18, 41, 62
  Geschäftsteilprozess 19
Geschäftsprozessschritt 14
Gewaltentrennungskonflikt 52, 128

H

Handlungsempfehlung 66

I

IKS 54, 65
Internes Kontrollsystem (IKS) 54, 65

K

Key Performance Indicator (KPI) 102
Konnektor
  physisches System 23
Konnektorgruppe 16, 23, 34, 59, 79, 96
  logische Systeme 34
Kontrolle 54, 142
  Art 144
  Mitigation 142
  Typ 144
Kontrollverantwortlicher 51, 57
  Genehmiger 57
Kontrollziel 44
Kontrollzuordnungsworkflow 106
kritische Aktion 27
kritische Berechtigung 26

M

Minderungsanalyse 106
  ungültige mindernde Kontrollen 106
Mitbestimmungspflicht 154
Mitigation 141
  generisch 94
  Vererbung 134

N

Namenskonvention 17, 40

O

Organisationseinheit 52
Organisationsregel 51

P

Performance 15, 21, 32, 59
Process Control 119
Projekt
  Beteiligte 125

R

Regel 45
Regelwerk 47, 90
  Vergleich 95
Repository-Synchronisation 103, 107
Risiko 38
  Bereinigung 90
  mindern 110
  SoD-Konflikt 38
  systemübergreifend 103
  Vermeidung 150
Risikoanalyse 27, 31, 97, 147
  Ad-hoc 103
  Anwendungsszenario 98
  Art 105. Siehe Zugriffsrisiko-bewertung; Siehe Minderungs-analyse
  Batch 101
  Batch-Analyse 113
  Bereinigung 123, 129
  Dashboard 101, 113
  Detaillierungsstufen 108

Format 104, 106
Interpretation 107, 116
KPI 121, 131
offline 107
Option 105
Risiko mindern 110
Risikoterminator 100, 117
Simulation 98, 112
Workshop 140
Risikoanalyse-Format
Ansicht zur Schwachstellenbehebung 104
Betriebswirtschaftliche Ansicht 104
Technische Ansicht 104
Risikoart 40, 46
Berechtigungsebene 40
Kritische Aktion 40
Kritische Berechtigung 40
Risikobewertung 66
Risikolevel 65, 67
Risikokatalog 13, 59
Definition 126
Drittanbieter 95
Matrix 13
Risikomatrix 13
SAP-Standard 129
Risiko-Status 43
Risikostufe 42
Risikoterminator 100, 117
Risikoverantwortlicher 49
Risiko-Workshops 140
Risk-Review 100
Rolle 97
Änderungsprozess 98
Kombination 98
Rollenzuordnung 97

S

Sammelrolle
Mitigation 133
Shared Service 18, 44, 55, 78, 157
Simulationsanalyse. Siehe Risikoanalyse
S_TCODE 24

T

Transaktion
FB01 109
PFCG 35, 117
SPRO 77
SU01 117
SU10 117
SU24 23, 33
Transport 36
Download 36
Transportauftrag 36
Upload 36

U

UAR. Siehe Benutzerzugriffsprüfung
Upload 85
Konsistenzprüfung 86

V

Verantwortlichengruppe 50
Verwendungsanalyse 138
Verwendungssynchronisation 145, 154

Z

Zugriffsrisikoanalyse. Siehe Risikoanalyse
Zugriffsrisikobewertung. Siehe Risikobewertung
Zusatzregel 53