Heft 36 | Dezember 2022 | 16. Jahrgang | ISSN 1864-6557

IT-GOVERNANCE

Fachzeitschrift des ISACA Germany Chapter e.V.

Alexander Koderman, Mirko Prehn

Der Einsatz von Graphdatenbanken in der Compliance-Automatisierung

Elektronischer Sonderdruck

ISACA Germany Chapter

dpunkt.verlag | it-governance.dpunkt.de | isaca.de

Elektronischer Sonderdruck
aus:

IT-Governance
Fachzeitschrift des ISACA Germany Chapter e.V.

http://it-governance.dpunkt.de/

16. Jahrgang – Heft 36 – Dezember 2022
Seiten 3 – 9

ISSN 1864-6557

Der Einsatz von Graphdatenbanken in der Compliance-Automatisierung

Alexander Koderman, Mirko Prehn

Moderne Graphdatenbanken eignen sich hervorragend zur Lösung typischer Herausforderungen im Compliance-Management. Sie lassen sich perfekt mit den aktuellen Entwicklungen bei maschinenlesbaren Formaten wie dem kürzlich fertiggestellten OSCAL-Standard kombinieren. Einige Herausforderungen bleiben jedoch bestehen.

1 Die Herausforderungen

Viele Unternehmen stehen vor der Herausforderung, eine Vielzahl an Implementierungssichten unterschiedlicher Standards und Best Practices zu konsolidieren: eine Prozessausrichtung nach COBIT und ITIL, die Implementierung eines effektiven internen Kontrollsystems in Anlehnung an COSO (Committee of Sponsoring of Organizations of the Treadway Commission) und weitere Anforderungen der Wirtschaftsprüfer und Aufsichtsorgane (Europäische Zentralbank (EZB), Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), U.S. Securities and Exchange Commission (SEC) etc.). In der Regel kommt dazu die Einrichtung eines sich kontinuierlich verbessernden Informationssicherheitsmanagements in Anlehnung an ISO 27001, BSI C5 und weiteren relevanten Industriestandards (U.S. National Institute of Standards and Technology (NIST), CSA etc.). Das Ergebnis sind oft nicht vergleichbare Reports von unterschiedlichen Scopes und meist auch redundante und voneinander isolierte Tätigkeiten im Sicherheits-, Risiko- oder Compliance-Umfeld. International agierende Unternehmen sehen sich zusätzlichen Herausforderungen ausgesetzt, begründet in unterschiedlichen und scheinbar inkompatiblen landesregulatorischen Vorgaben, Standards und Rahmenwerken.

Weitere erschwerende Faktoren sind:

- Regulatorische Anforderungen, Standards und Rahmenwerke werden weiterentwickelt und können sich manchmal auch wesentlich ändern.
- Standards, Rahmenwerke und regulatorische Anforderungen überschneiden sich in den Geltungsbereichen und können oft widersprüchlich sein, sodass sie nicht gemeinsam umsetzbar sind.
- Informationssysteme bzw. Informationsverbünde werden immer größer und komplexer und können nicht geeignet zugeschnitten werden.

Um Informations- und Datenschutzrisiken angemessen adressieren zu können, müssen Security und Privacy Controls (Maßnahmen) nachvollziehbar implementiert werden und deren Wirksamkeit ist durch verschiedene Experten und Verantwortliche zu beurteilen. Dies stellt eine ressourcenintensive Aufgabe dar und ist angesichts der Komplexität der Anforderung und der sich ständig ändernden Bedrohungslage oft schwierig innerhalb der vorgegebenen Budgetierung durchzuführen.

Eine Strukturierung der anwendbaren Standards und Normen in eine interoperable Spezifikation, die zugleich maschinell auswertbar und von Menschen lesbar ist, ist ein Ausweg. Eine maschinell unterstützte Analyse und Berichterstattung ermöglicht eine Bewertung über mehrere Regulierungswerke und Komponenten hinweg.

In diesem Beitrag werden wir anhand der jüngsten Initiative des NIST mithilfe von Graphdatenbanken (am Beispiel von Neo4j) zeigen, wie Unternehmen sich diesen Herausforderungen stellen können.

2 Die Open Security Controls Assessment Language (OSCAL)

Am 8. Juni 2021 veröffentlichte das verantwortliche NIST-Team den Beschreibungsstandard »Open Security Controls Assessment Language« (OSCAL) in der Version 1.0.1 und einige Wochen später die langerwartete NIST SP 800-53 in der Revision 5. Gleichzeitig mit der Textversion [NIST 2020] erschien diese Sonderveröffentlichung nun auch erstmalig im OSCAL-Format (JSON, YAML und XML). Bis zum heutigen Zeitpunkt folgten weitere Standards (wie etwa Federal Risk and Authorization Management Program (FedRAMP)) und es sind zukünftige Veröffentlichungen (wie COBIT und ISO 27001/2)[1] geplant. Am 17. Mai 2022 erschien die überarbeitete Version OSCAL 1.0.4.

Das Ziel von OSCAL ist die Automatisierung von Sicherheitsbewertungen, Controls-Compliance-Audits und maschinell unterstützte kontinuierliche Überwachung. Es soll die derzeit überwiegend manuelle Arbeit mit Tabellenkalkulationen und Textverarbeitungsprogrammen bei der Durchführung von Maßnahmenzuweisungen, Dokumentation, Analysen und Bewertungen sowie bei Sicherheits- und Compliance-Audits

1 *https://pages.nist.gov/OSCAL/concepts/layer/control/catalog/*

ersetzen und automatisieren. Schon »by Design« ist gleichzeitig die Übertragung der Ergebnisse in für Menschen lesbare Formen sichergestellt.

OSCAL gliedert sich in drei wesentliche Layer (vgl. Abb. 1). Der **Controls Layer** beinhaltet zum einen den oder die Catalog-Modelle. Beispiele sind hier NIST SP 800-53, ISO 27002 oder auch COBIT 5. Das Catalog-Modell stellt die Basis für die weitere Beschreibung dar und beinhaltet alle (Security und Privacy) Controls. Die Controls können Anforderungsdefinitionen, Parameter, Referenzen, Ziele und Bewertungsmethoden umfassen. Das Modell ermöglicht auch die Organisation von Controls. Werden mehrere Standards im Unternehmen eingesetzt, wird jeder Standard separat als ein Catalog-Modell beschrieben. Referenzierungen und Mappings zu anderen Standards (also zwischen den Catalog-Modellen) sind möglich, aber nicht notwendig.

Auch eigenentwickelte Standards können in OSCAL überführt werden. Bei der Modellierung einer Norm in einer maschinenlesbaren Form ist es wichtig, dass die Granularität der Beschreibung detailliert genug ist. Um mit einzelnen Paragrafen und Teilen eines Steuerelements arbeiten zu können, müssen diese als einzelne Knoten in der Datenbank identifizierbar und adressierbar sein.

Die zweite Komponente im Controls Layer stellt das Profil-Modell dar. Ein Profil-Modell beinhaltet die für das Unternehmen relevanten unternehmensspezifisch angepassten Kontrollen und kann aus einem oder mehreren Profil-Modellen (zur Berücksichtigung unterschiedlicher Schutzbedarfe) bestehen. Ein Profil-Modell kann aus mehreren Catalog-, aber auch Profil-Modellen die Kontrollen ableiten und weiter spezifizieren. Zum Beispiel kann aus dem »moderaten« Profil-Modell von NIST SP 800-53B Rev. 5 und den spezifischen Vorgaben aus dem FedRAMP-Profil für bestimmte Controls ein neues unternehmensspezifisches Profil »abgeleitet« werden (siehe hierzu auch die Ausführungen im späteren Verlauf).

Der **Implementation Layer** besteht aus dem Component- und dem Systemsicherheitsplan-Modell (SSP-Modell). In beiden werden aus dem gewählten relevanten Profil-Modell die tatsächlichen Implementierungen der Controls für die Informationssysteme (Informationsverbünde) dokumentiert. Wesentlicher Unterschied ist, dass man durch die Nutzung von einzelnen Komponenten eine Dekomposition komplexer IT-Systeme vornehmen kann. Im übergeordneten SSP (Informationssicherheitskonzept) kann dann auf ein oder mehrere Component-Modelle referenziert werden. Beispiele sind Kryptografie-Komponenten oder eine Rechenzentrumsumgebung.

Der letzte Layer (**Assessment Layer**) unterstützt die Auditierung und Auswertung. Das Assessment-Plan-Modell wird im kontinuierlichen Sicherheitsmonitoring entwickelt. Das Assessment-Results-Modell beinhaltet die für das regelmäßige Sicherheitsmonitoring notwendigen Informationen. Die Systemverantwortlichen nutzen die Assessment-Ergebnisse (überführt in von Menschen lesbare Formen), um sich ein Bild von der Risikolage ihrer Systemlandschaft zu machen, Risiken gezielt zu beheben und Maßnahmen zur Risikobehebung zu planen. Abweichungen und daraus resultierende potenzielle Risiken werden in dem PoA&M-Modell (*Plan of Action and Milestones* – Risikobehandlungsplan) dokumentiert. PoA&M-Ergebnisse fließen in das übergeordnete Information Risk Management zur weiteren Behandlung und Überwachung ein. Auch hier kann eine weitere Automatisierung der Quantifizierung von Informationen oder Cyberrisiken, zum Beispiel durch die Überführung in FAIR-CAM™ oder FAIR, erfolgen.[2]

Im Assessment Layer und Implementation Layer sind zukünftige Erweiterungen (Future) vorgesehen (vgl. Abb. 1).

2 FAIR – Open Group Standard: Factor Analysis for Information Risk; FAIR-CAM™ (FAIR Controls Analytics Model) ist die konsequente Weiterentwicklung zur Bestimmung der Wirksamkeit von Controls.

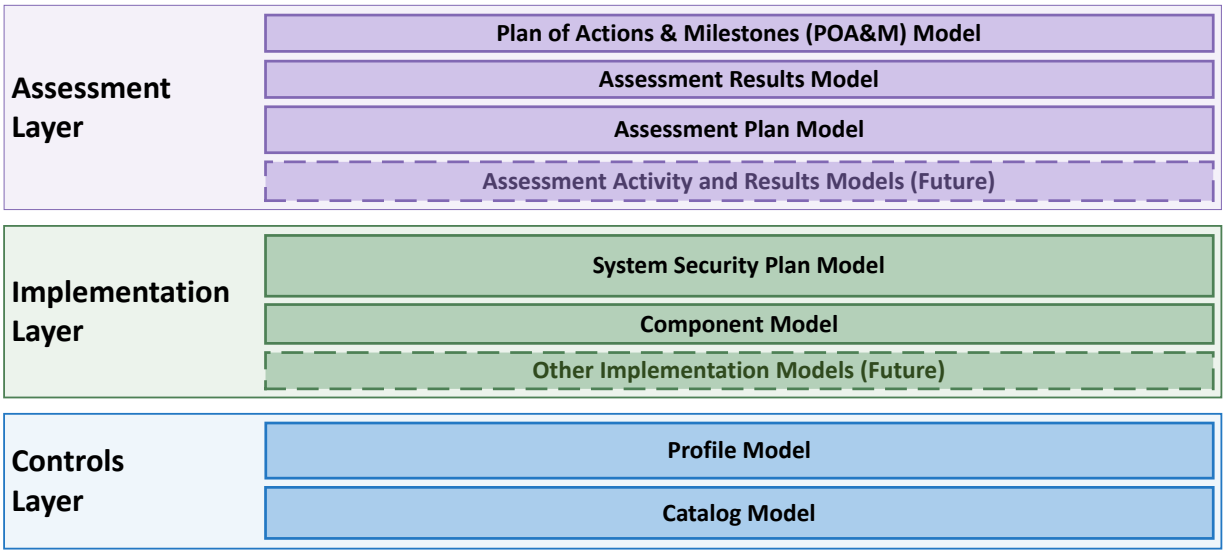


Abb. 1: Layer der Open Security Controls Assessment Language (OSCAL)

3 Der Einsatz von Graphen

Graphdatenbanken wie Neo4j[3] oder Memgraph[4] stellen eine technische Neuerung im Bereich der sogenannten NoSQL-Datenbanken dar. Die NoSQL-Datenbanken lösen sich vom bislang dominierenden Ansatz der relationalen Datenbanken, die mit der Abfragesprache SQL operieren. Speziell Graphdatenbanken wurden entworfen, um Abfragen besser zu bearbeiten, bei denen die Beziehungen zwischen Objekten im Vordergrund stehen.

Graphdatenbanken speichern Informationen in Form von Knoten und Kanten. Sie schneiden bei Abfragen der oben beschriebenen Art um Größenordnungen besser ab. Das liegt daran, dass sie den Graphen traversieren und nur die Knoten besuchen, die für das Endergebnis relevant sind. Graphdatenbanken können selbst in einem Graphen mit Zehntausenden von Knoten und komplexen Beziehungen schnell die gesuchten Pfade finden.

Tabelle 1 zeigt dies anhand des Beispiels eines Social-Network-Graphen. Die Graphdatenbank soll über Beziehungen des Typs »Freund-eines-Freundes« Verbindungen zwischen Personen aufdecken. Die Graphdatenbank schlägt die relationale Datenbank bei der Laufzeit um mehrere Größenordnungen, sobald die Abfrage vier bis fünf Ebenen tief in die Freundschaftsbeziehungen hineinreicht [Vukotic et al. 2015, S. 7].

Tiefe	Personen	Ø Freunde	MySQL (s)	Neo4j (s)
2	1.000.000	50	0,02	0,01
3	1.000.000	50	30,27	0,17
4	1.000.000	50	1.543,51	1,36
5	1.000.000	50	Nicht fertig nach 1 Stunde	2,13

Tab. 1: Abfrage »Freund-eines-Freundes«, Datenbank enthält 1 Mio. Personen mit je 50 Freunden [Vukotic et al. 2015, S. 8]

Die Verbindungen zwischen Richtlinien, Standards, Kontrollen und Layers stellen Beziehungen dar. Graphdatenbanken sind somit gut geeignet für die Modellierung von OSCAL-Datenstrukturen.

Nehmen wir an, wir wollen herausfinden, ob zwei Maßnahmen aus verschiedenen Standards in irgendeiner Weise miteinander verbunden sind. Bei herkömmlichen relationalen Datenbanken kommt es schnell zu einem exponentiellen Leistungsabfall, wenn die Abfragetiefe vier oder fünf Beziehungsebenen überschreitet. Eine relationale Datenbank muss vollständige Verknüpfungen mit zunehmender Tiefe durchführen, um dann das gewünschte Ergebnis herauszufiltern.

In einer Datenbank mit nur 100 Maßnahmen, die jeweils mit zehn anderen Maßnahmen verknüpft sind, enthält die Verknüpfungstabelle 1.000 Einträge. Wenn man diese Beziehungen fünf Ebenen tief verfolgt, erzeugt eine relationale Datenbank dafür fünfmal das kartesische Produkt sämtlicher Einträge. Daraus ergibt sich eine Ergebnismenge mit einer Billiarde Zeilen (1000^5), deren Untersuchung viel Zeit in Anspruch nimmt, um möglicherweise nur ein einziges übereinstimmendes Ergebnis daraus zu extrahieren.

Die OSCAL-Inhalte werden in XML-, YAML- und JSON-Notation veröffentlicht. Moderne Graphdatenbanken sind in der Lage, diese Formate direkt zu importieren und mit ihnen weiterzuarbeiten, ohne dass zusätzliche Tools erforderlich sind. Da sie direkt netzwerkfähig sind, kann die Datenbank angewiesen werden, den Control-Inhalt direkt aus dem öffentlichen Quellcode-Repository des NIST zu lesen. Die Autoren dieses Artikels haben hierfür eine Sammlung von Skripten erstellt, die bereits in der offiziellen Tool-Liste des NIST geführt werden.[5]

3.1 Suche nach in Beziehung stehenden Maßnahmen (Controls)

Wenn wir eine Verbindung von Control A zu Control B und von B zu C eingeben, ist die Graphdatenbank in der Lage, die transitive Beziehung von A zu C selbstständig zu finden. Die folgende Abbildung 2 zeigt, wie dies von einem Compliance-Beauftragten genutzt werden kann.

Wir können die Datenbank anweisen, eine Beziehung zwischen zwei Standards zu finden: z. B. »PCI DSS« und »COBIT 5«. Die Abfrage (vgl. Abb. 3) liefert einen Pfad zwischen den beiden Standards und ihren Maßnahmen, wobei eine Maßnahme aus dem NIST Cybersecurity Framework (NIST CSF) als Verbindungspunkt verwendet wird. Dabei wurde das NIST CSF in der Abfrage nie angegeben – die Datenbank hat mithilfe eines »Shortest Path«-Algorithmus eine Maßnahme aus diesem Standard als Möglichkeit identifiziert, selbst eine transitive Beziehung zu bilden (vgl. Abb. 2).

Die Datenbank konnte feststellen, dass die PCI DSS-Anforderung 11.4 *(Überwachung des Datenverkehrs und Einsatz von IDS/IPS zur Erkennung und Verhinderung von Eindringlingen in das Netzwerk)* mit den folgenden COBIT 5-Managementpraktiken in Verbindung steht:

- *DSS01.03: Überwachung der IT-Infrastruktur*
- *DSS03.05: Proaktives Problemmanagement durchführen*
- *DSS05.07: Überwachung der Infrastruktur auf sicherheitsrelevante Ereignisse*

Der Compliance-Manager kann diese Informationen nutzen, um die Bemühungen zur Umsetzung dieser Maßnahmen passend auszurichten und dabei das gesamte Spektrum der Ziele und Messgrößen zu nutzen, die der COBIT 5-Rahmen für die Ressourcenoptimierung bietet. Gegebenenfalls stellt er fest, dass durch die Erreichung des entsprechenden Reifegrads der DSS-Prozesse bereits ausreichende Maßnahmen

3 *https://neo4j.com/*
4 *https://memgraph.com/*
5 *https://github.com/usnistgov/OSCAL/blob/develop/docs/content/tools/_index.md*

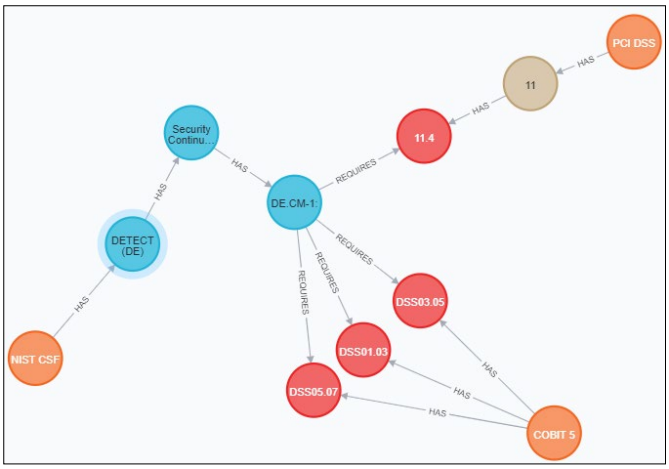


Abb. 2: Die Datenbank hat einen Weg zwischen PCI DSS und COBIT 5 gefunden – und dabei das NIST Cybersecurity Framework als Verbindungsmöglichkeit identifiziert.

implementiert sind und kein weiterer Handlungsbedarf in der Erreichung der PCI DSS-Anforderung besteht.

```
MATCH path=shortestPath(
  (pci:regime{name: 'PCI DSS'})-[*]-(cobit:regime{name:'COBIT 5'})
)
RETURN path
```

Abb. 3: Eine Graphenabfrage in der Abfragesprache Cypher: kürzeste Verbindung zwischen PCI DSS und COBIT 5

Um solche Schlüsse ziehen zu können, benötigt die Datenbank eine solide Grundlage von Standards, Maßnahmen, Rollen, Anforderungen, möglichen Kontrollparametern sowie Zuordnungsinformationen.

3.2 Bestimmung der Maßnahmenvoraussetzungen

Eine Frage, die sich bei der Planung des Projektzeitplans für die Implementierung von Security und Privacy Controls stellt, ist die Festlegung der richtigen Reihenfolge: Welche Maßnahmen sind am wichtigsten, welche Maßnahmen sind Voraussetzung für andere und welche Maßnahmen sind sogenannte »Low-Hanging-Fruits«, die mit dem geringsten Aufwand implementiert werden können?

Eine Abfrage am Beispiel von NIST-800-53 zeigt, welche Maßnahmen am häufigsten von anderen Maßnahmen referenziert werden. Wir können diese Abfrage auf einer Tiefe von zwei Ebenen durchführen (Anforderungen-von-Anforderungen).

Diese Abfrage liefert 1.221 Verweise auf die am meisten referenzierte Maßnahme (vgl. Abb. 4). Dies übersteigt bereits die Gesamtzahl der in diesem Katalog enthaltenen Maßnahmen von 1.189. Aufgrund der hohen Interkonnektivität der Maßnahmen sind also bereits nach zwei Sprüngen alle Maßnahmen mit bestimmten Maßnahmen in dieser Norm verbunden. Diese stark referenzierten Maßnahmen könnten als die wichtigsten angesehen werden, und tatsächlich erweisen sie sich als zentrale, grundlegende Aufgaben. An erster Stelle steht *SA-8: »Security and Privacy Engineering Principles«*. Auf diese Maßnahme folgen weitere weitreichende Themen wie *AC-3: »Access Enforcement«* und *AC-17: »Remote access«*.

Ein Projektleiter kann diese Informationen nutzen, um Prioritäten zu setzen und einen kritischen Pfad zu ermitteln, der bei der Festlegung des Zeitplans für die Umsetzung der Maßnahmen berücksichtigt werden muss.

Unsere Erfahrung in der Implementierung von Schutzbedarfen bei Informationssystemen zeigt, dass gerade die Überführung maschinell lesbarer »Hausstandards« und die Dokumentation der Maßnahmenumsetzung zu den zeitlichen und personalressourcenschonenden Effekten führt, die den anfänglichen scheinbaren Mehraufwand mehr als ausgleichen. Bereits in der ersten Runde der bei Banken und Versicherungen verpflichtenden jährlichen Aktualisierung des Soll-Ist-Abgleichs wird dieser Aufwand kompensiert.

3.3 Anpassung der Maßnahmen an die Organisation

Die Modellierung der Landschaft der GRC-Standards (Governance, Risk, Compliance) und Best Practices ist nur ein erster Schritt. Jede Organisation muss einen Standard auf der Grundlage der Unternehmensziele und der IT-bezogenen Ziele anpassen. Die Implementierungsstärke der Maßnahmen muss mit den Anforderungen an den Informationsschutz, den Ergebnissen der Risikoanalyse und den organisatorischen Gegebenheiten abgeglichen werden. Das Ergebnis dieses Anpassungsprozesses kann in der OSCAL-Syntax in Form von sogenannten »Profilen« dokumentiert werden.

Profile duplizieren die Informationen der Katalogebene nicht. Sie enthalten lediglich Verweise auf diese. Diese Verweise müssen aufgelöst werden. Dies geschieht automatisch, wenn das Profil zusätzlich zu einer bestehenden Katalogdarstellung in eine Graphdatenbank importiert wird.

Profile können spezifisch für eine Organisation sein. Es ist auch möglich, Profile zu veröffentlichen und anzuwenden, die Anforderungen von Dritten beschreiben. Ein Beispiel für solche Profile sind die vom FedRAMP veröffentlichten Profile, die 2011 eingeführt wurden, um Anforderungen für die Nutzung von Cloud-Diensten durch die US-Behörden festzulegen.[6] Je nach den Auswirkungen eines möglichen Verlusts der Vertraulichkeit, der Integrität oder der Verfügbarkeit werden unterschiedliche Profile für verschiedene Baselines veröffentlicht.

Höhere Auswirkungen erfordern eine strengere Auslegung der Maßnahmenparameter. Abbildung 5 zeigt, wie zwei Profile die Zeitspanne einer Maßnahme unterschiedlich festlegen. Bei dem fraglichen Absatz handelt es sich um die NIST 800-53-Maßnahmenerweiterung AC-2.2, die besagt, dass *»temporäre und Notfallkonten nach [vom Unternehmen festgelegter Zeitspanne] automatisch [entfernt/deaktiviert] werden«* sollen:

6 *https://github.com/GSA/fedramp-automation*

```
MATCH (c1)←[rx:RELATED*2{type:'related'}]-(c2)
RETURN c1.id, c1.title, COUNT(rx) AS numRequiredLv2
ORDER by numRequiredLv2 DESC
LIMIT 10;
```

neo4j$ MATCH (c1)←[rx:RELATED*2{type:'related'}]-(c2) RETURN c1.id, c1.title, COUNT(rx) AS numRequiredLv2 ORDER by numRequiredL…

Table | Text | Warn | Code

	c1.id	c1.title	numRequiredLv2
1	"sa-8"	"Security and Privacy Engineering Principles"	1221
2	"ac-3"	"Access Enforcement"	919
3	"ac-17"	"Remote Access"	826
4	"si-4"	"System Monitoring"	761
5	"sc-7"	"Boundary Protection"	710
6	"ac-2"	"Account Management"	697
7	…	…	…

Abb. 4: Die Abfrage von Control-Abhängigkeiten mit einer Tiefe von »zwei« zeigt Anforderungen-von-Anforderungen (NIST 800-53).

- das FedRAMP-Profil »hoch« verlangt die Entfernung/Deaktivierung von Konten nach nur »*24 Stunden nach der letzten Nutzung*«,
- das Profil »moderat« gewährt einen längeren Zeitraum von »*höchstens 30 Tagen*«.

Der wirkliche Nutzen von maschinenlesbaren Formaten ergibt sich, wenn sie zur Automatisierung der Anwendung und Bewertung von Maßnahmen eingesetzt werden können (vgl. Abb. 6). Eine einzige Maßnahme kann sich auf mehrere Umgebungen oder Informationssysteme innerhalb einer Organi-

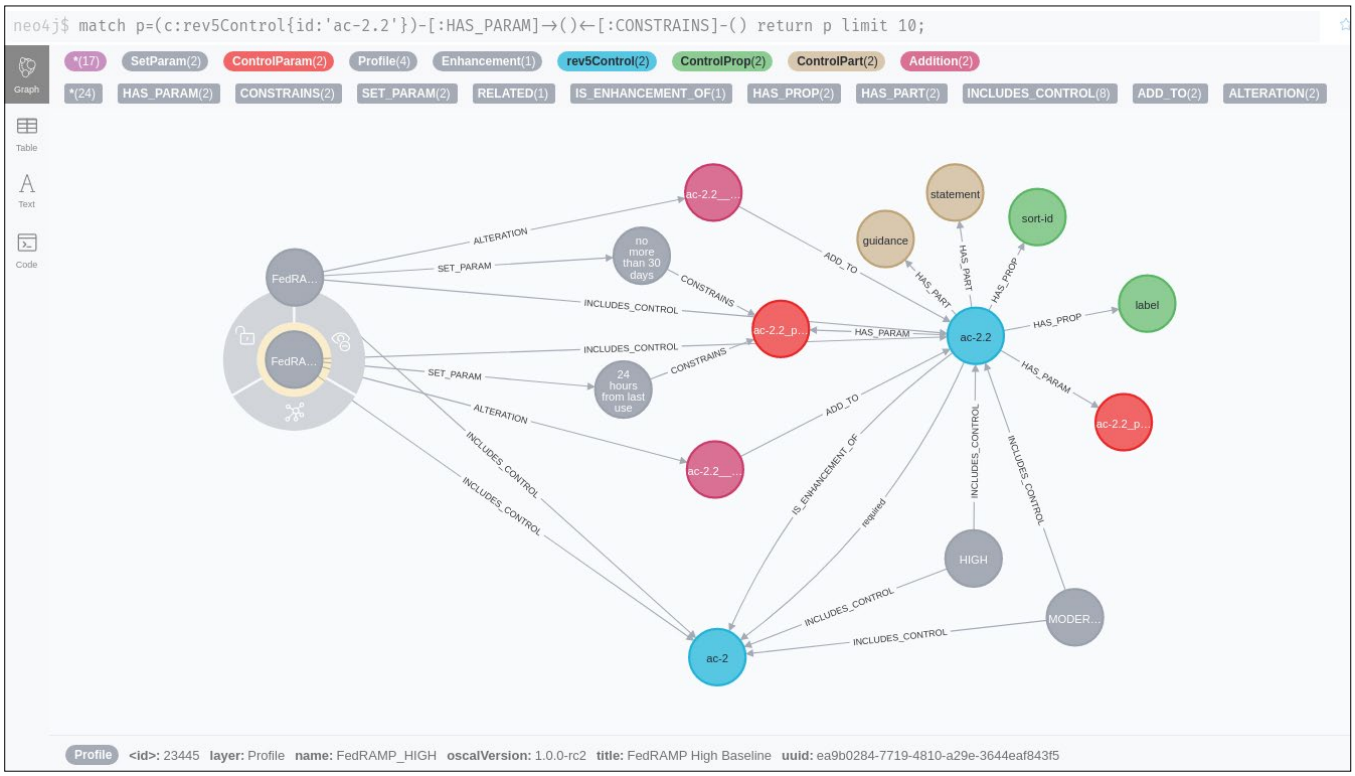
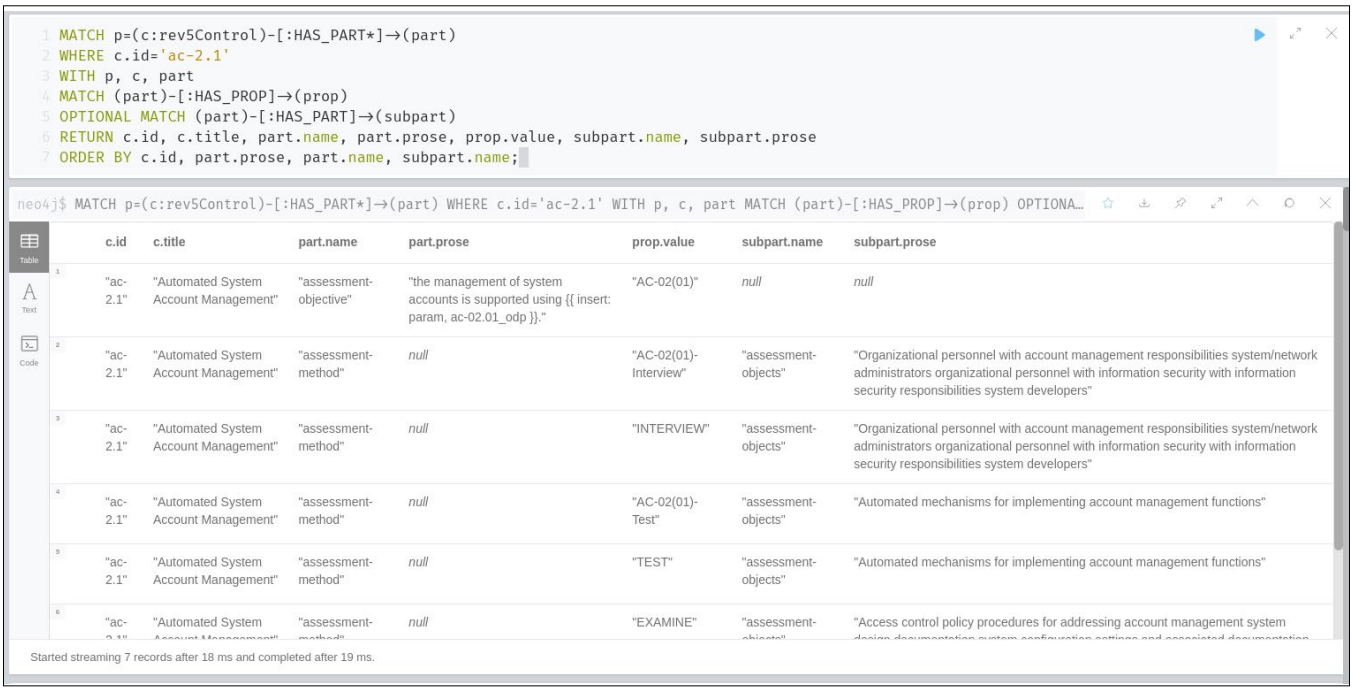


Abb. 5: Das FedRAMP-Profil »hoch« stellt strengere Anforderungen an die Maßnahmenparameter als das Profil »moderat«.



```
MATCH p=(c:rev5Control)-[:HAS_PART*]→(part)
WHERE c.id='ac-2.1'
WITH p, c, part
MATCH (part)-[:HAS_PROP]→(prop)
OPTIONAL MATCH (part)-[:HAS_PART]→(subpart)
RETURN c.id, c.title, part.name, part.prose, prop.value, subpart.name, subpart.prose
ORDER BY c.id, part.prose, part.name, subpart.name;
```

neo4j$ MATCH p=(c:rev5Control)-[:HAS_PART*]→(part) WHERE c.id='ac-2.1' WITH p, c, part MATCH (part)-[:HAS_PROP]→(prop) OPTIONA…

Table | Text | Code

	c.id	c.title	part.name	part.prose	prop.value	subpart.name	subpart.prose
1	"ac-2.1"	"Automated System Account Management"	"assessment-objective"	"the management of system accounts is supported using {{ insert: param, ac-02.01_odp }}."	"AC-02(01)"	*null*	*null*
2	"ac-2.1"	"Automated System Account Management"	"assessment-method"	*null*	"AC-02(01)-Interview"	"assessment-objects"	"Organizational personnel with account management responsibilities system/network administrators organizational personnel with information security with information security responsibilities system developers"
3	"ac-2.1"	"Automated System Account Management"	"assessment-method"	*null*	"INTERVIEW"	"assessment-objects"	"Organizational personnel with account management responsibilities system/network administrators organizational personnel with information security with information security responsibilities system developers"
4	"ac-2.1"	"Automated System Account Management"	"assessment-method"	*null*	"AC-02(01)-Test"	"assessment-objects"	"Automated mechanisms for implementing account management functions"
5	"ac-2.1"	"Automated System Account Management"	"assessment-method"	*null*	"TEST"	"assessment-objects"	"Automated mechanisms for implementing account management functions"
6	"ac-2.1"	"Automated System Account Management"	"assessment-method"	*null*	"EXAMINE"	"assessment-objects"	"Access control policy procedures for addressing account management system design documentation system configuration settings and associated documentation

Started streaming 7 records after 18 ms and completed after 19 ms.

Abb. 6: Liste der nötigen Prüfhandlungen, Prüfungsgegenstände und Interviewpartner für die Maßnahme AC-2.1 (Automated System Account Management)

sation mit unterschiedlichen Beteiligten beziehen. Die Details der Implementierung können zwischen diesen Systemen variieren. Der Bewertungs- oder kontinuierliche Überwachungsprozess muss diesen Unterschieden Rechnung tragen. In den meisten Fällen validieren und überprüfen die Prüfer die von den verschiedenen Beteiligten vorgelegten Bewertungsergebnisse manuell. Ziel muss es sein, so viele dieser Überprüfungen wie möglich zu automatisieren.

Durch die Einbeziehung von Assets und Stakeholdern in den Compliance-Graphen können Arbeitspakete für jeden Control-Verantwortlichen ermittelt werden, indem die Pfade zu seinen Maßnahmen verfolgt werden. Übergreifende Belange werden sichtbar – wenn ein Prozesseigentümer eine Anwendung in einem Rechenzentrum betreibt, wird er feststellen, dass viele Maßnahmen mit Bezug auf die physische und umgebungsbezogene Sicherheit bereits von den Eigentümern der Serviceprozesse des Rechenzentrums implementiert werden.

Die Bewertungsergebnisse für die verbleibende Gruppe von Maßnahmen können auf Vollständigkeit und Konsistenz validiert werden, d.h. auf unterschiedliche Umsetzungsreife bei mehreren Anwendungen derselben Maßnahmen in verschiedenen Bereichen. Auf der Grundlage der bestehenden maschinenlesbaren Formate werden bereits Validierungsrahmen entwickelt.[7]

Derzeit werden solche Bemühungen dadurch behindert, dass nur wenige maschinenlesbare Formate für Control-Kataloge, Assessment-Pläne und Assessment-Ergebnisse in der Praxis tatsächlich verwendet werden. Zudem müssen die Benutzerschnittstellen hier noch verbessert werden. Da nur fortgeschrittene Anwender in der Lage sind, ihre Arbeit direkt mit den Abfragefunktionen einer Graphdatenbank zu unterstützen, müssen benutzerfreundlichere Werkzeuge entwickelt werden. Sobald diese Hürden beseitigt sind, ist zu erwarten, dass sich der effizientere Austausch von Implementierungs- und Assessment-Daten in speziellen Formaten gegenüber unstrukturierten und nicht fachspezifischen Formaten wie Textverarbeitung und Tabellenkalkulation durchsetzt. Auch eine Überführung in einen zwischen den Unternehmen etablierten Threat-Intelligence-Prozess ist denkbar.

Literatur

[NIST 2020] *National Institute of Standards and Technology (NIST):* Security and Privacy Controls. NIST SP-800-53 Rev. 5. September 2020,

[Vukotic et al. 2015] *Vukotic, A.; Watt, N.; Abedrabbo, T.; Fox, D.; Partner, J.:* Neo4j in Action. Manning, 2015.

Alle Beispiele in diesem Artikel wurden mit der kostenlosen Community-Edition der Graphdatenbank Neo4j (https://neo4j.com/download-center/#community) erstellt. Der zur Erstellung der Ergebnisse verwendete Quellcode ist auf GitHub (https://github.com/Agh42/oscal4neo4j) verfügbar.

7 *https://github.com/GSA/fedramp-automation/tree/master/src/validations*

Alexander Koderman

berät zahlreiche Organisationen aller Größenordnungen in Fragen der Cybersicherheit, des Informationssicherheits-Risikomanagements und der IT-Governance. Er war Chief Security Officer bei Cassidian Communications und leitete das IT-Sicherheitsteam bei der Deutschen Kreditbank AG. Derzeit arbeitet er an der Entwicklung der nächsten Generation von GRC-Werkzeugen für die SerNet GmbH in Berlin. Er ist als CISA, PMP, ISO 27001 LA, RHCE und NCLP zertifiziert.

Dipl.-Inf. (FH) Alexander Koderman
SerNet GmbH
Bahnhofsallee 1b
37081 Göttingen
ak@sernet.de
https://sernet.de

Mirko Prehn

ist Experte in der Prüfung und Beratung von Unternehmen während und außerhalb der Jahresabschlussprüfung zu IT-Compliance-Fragestellungen. Seit über 15 Jahren berät er Unternehmen zu Berechtigungsfragen sowie zu Integrated Risk Management (IRM). In seiner Zeit als IT-Sicherheitsbeauftragter entwickelte er Methoden zur Vereinfachung des Audits von IT-Sicherheitsanforderungen. Er ist als ISACA CISA, CGEIT, CDPSE und als Open FAIR™ zertifiziert.

Diplom-Volkswirt Mirko Prehn
KPMG AG Wirtschaftsprüfungsgesellschaft
Digital Compliance
Klingelhöfer Str. 18
10827 Berlin
mprehn@kpmg.com
www.kpmg.com