

Heft 39 | Juli 2024 | 18. Jahrgang | ISSN 1864-6557

IT-GOVERNANCE

Fachzeitschrift des ISACA Germany Chapter e.V.

AUSZUG
AUS HEFT 39

IT-Governance genormt – die neue ISO/IEC 38500 (revolutions)

Michael Klotz

 **ISACA**[®]
Germany Chapter

IT-GOVERNANCE

Fachzeitschrift des ISACA Germany Chapter e.V.

Inhalt

Fachthemen

- 3** **Cloud Governance und Compliance im Lifecycle einer Cloud-Nutzung**
Thorsten Hennrich

- 9** **Mehr als ein gezielter Austausch von Nachrichten**
Informationssicherheit für alle Kommunikationsprozesse einer Organisation
Petra Haferkorn

- 14** **Das Konzept der COBIT® Focus Area anwenden, um regulatorische Anforderungen zu ergänzen (am Beispiel der VAIT)**
Markus Gaulke

Rubriken

- | | |
|--|--|
| <ul style="list-style-type: none">19 Standards IT-Governance genormt – die neue ISO/IEC 38500 (revolutions) Michael Klotz 25 Aus den ISACA-Fachgruppen Geldwäscheprävention und das Digital Trust Ecosystem Framework | <ul style="list-style-type: none">32 Veranstaltungen IT-GRC Kongress 2024 des ISACA Germany Chapter 34 ISACA Foundation Interview mit der Masterstudentin und Stipendiatin Somaye Hoseinpur 36 Inserenten 36 Vorschau 36 Impressum |
|--|--|

Standards

IT-Governance genormt – die neue ISO/IEC 38500 (revolutions)

Michael Klotz

In dieser Rubrik wurde bisher zweimal über die ISO/IEC 38500 berichtet – in [Klotz 2008] über ihr erstmaliges Erscheinen, in [Klotz 2016] über die zweite Version der Norm und die Entwicklung zur Normenreihe ISO/IEC 3850x. Dabei wurde der Titel des Artikels stets beibehalten, beim letzten Mal jedoch – in Anlehnung an eine bekannte SF-Filmreihe – mit dem Zusatz »reloaded« versehen. Die Fortführung dieser Praxis mit dem diesmaligen Zusatz »revolutions« weist darauf hin, dass die Norm grundlegende Änderungen erfahren hat. Diese sind im Wesentlichen darauf zurückzuführen, dass sich die ISO/IEC 38500:2024 nunmehr am allgemeinen Governance-Verständnis der »ISO 37000 Governance of Organizations – Guidance« ausrichtet. Aus diesem Grund wird im Folgenden die dritte Version der ISO/IEC 38500 in all ihren Elementen überblicksartig beschrieben.

1 Institutioneller Hintergrund

In dem von den Normungsorganisationen International Standards Organization (ISO) und International Electrotechnical Commission (IEC) gemeinsam gebildeten technischen Komitee »ISO/IEC JTC 1« ist der 2013 eingerichtete Unterausschuss »SC 40 IT Service Management and IT Governance« für die Norm zuständig. Dieser Ausschuss ist in Arbeitsgruppen untergliedert, eine davon ist mit »Governance of Information Technology« befasst. Deutschland ist durch den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) vertreten, allerdings nur als beobachtendes Mitglied (vgl. [ISO 2024]).

2 Zielgruppe und Anwendungsbereich

Die Zielgruppe der Norm ist im Vergleich zur zweiten Version weniger spezifisch und umfasst primär die Leitungsorgane (governing body)¹ und die sie unterstützenden Akteure, letztlich aber alle Organisationsmitglieder, denen eine Anleitung für die Praxis der IT-Governance geboten werden soll (vgl. [ISO/IEC 38500:2024, S. vi]). Dies entspricht dem grundlegenden Verständnis der Norm, dass Governance-Maßnahmen in der gesamten Organisation durchgeführt werden können (vgl. [ISO/IEC 38500:2024, S. 3]). Die Norm soll, wie bisher auch, von Organisationen aller Art und jeder Größen-

ordnung und unabhängig vom Umfang des IT-Einsatzes angewendet werden können (vgl. [ISO/IEC 38500:2024, S. 1]).

3 Begriff der IT-Governance

Erste deutliche Anpassungen an die ISO 37000 zeigen sich bereits im dritten Kapitel mit den Definitionen, die in ihrer Anzahl (von 25 auf 10) deutlich reduziert wurden. Governance wird nun als ein System verstanden, das Leitung, Aufsicht und Verantwortung umfasst (vgl. [E DIN ISO 37000:2024, S. 11]). Im Hinblick auf die »Governance of IT« (die Begriffe »Corporate«, »Enterprise« bzw. »Organizational Governance of IT« werden weiterhin als gleichbedeutend betrachtet) beziehen sich diese drei Bereiche nach wie vor auf die aktuelle und künftige Nutzung der IT. Diese umfasst die Planung, das Design, die Entwicklung, die Einführung, den Betrieb, das Management und die Anwendung von IT zur Erfüllung der Geschäftsziele und zur Wertschöpfung für die Organisation (vgl. [ISO/IEC 38500:2024, S. 2]). Dass IT-Governance einen Teilbereich der Corporate Governance darstellt, zeigt sich in der Norm jetzt auch inhaltlich durch die Ausrichtung an der ISO 37000.

4 Gute IT-Governance

Auf die ersten drei Kapitel zum Anwendungsbereich, zu den normativen Verweisungen und zu den Begriffen folgt das vierte Kapitel der Norm, das sich in Anlehnung an die ISO 37000 den Auswirkungen (Outcomes) einer »guten IT-Governance« widmet. Diese werden in drei Gruppen unterteilt: effektive Leistung, verantwortungsvolle Leitung und ethisches Verhalten.

- Wie sich die Effektivität der IT ausprägt, ist von den Leitungsorganen unter Berücksichtigung des Organisationsumfelds und der Erwartungen der Anspruchsgruppen bzw. Stakeholder zu bestimmen. Eine Bewertung der Effektivität kann sich auf die erreichte Unterstützung des Organisationszwecks durch IT, die Angemessenheit der IT-Investitionen, die durch Einsatz der IT-Ressourcen erzielte Wertschöpfung, die Qualität der Entscheidungsfindung sowie den Beitrag der IT zur Agilität und Anpassungsfähigkeit der Organisation richten.
- Die Erwartungen an eine verantwortungsvolle Leitung sollten klar formuliert werden. Sie können sich z.B. auf die Angemessenheit und Rechtfertigung automatisierter

¹ Für die Übersetzung der englischsprachigen Begriffe wird – soweit möglich – der DIN-Entwurf E DIN ISO 37000:2024 [E DIN ISO 37000:2024] genutzt. Bei darüber hinausgehenden Übersetzungen wird in der Regel der englische Begriff mit angegeben. Es sei jedoch dringend angeraten, den englischen Originaltext zu lesen.

Entscheidungen, den geeigneten Schutz und die angemessene Nutzung von Daten, die Datensicherheit, die Resilienz digitaler Fähigkeiten und die Beherrschung von IT-Risiken beziehen.

- Ein ethisches Verhalten in Bezug auf die Nutzung von IT ist durch die Leitungsorgane zu fordern und zu fördern. Entsprechende Anforderungen umfassen die Beachtung von Rechten und Pflichten im Umgang mit Daten, Befugnisse für den Zugang zu und die Nutzung von Daten, soziale und umweltbezogene Anforderungen, die Wahrung von Vertraulichkeit, die Gewährleistung von Transparenz und die Compliance mit gesetzlich-regulatorischen Bestimmungen (nach [ISO/IEC 38500:2024, S. 3 f.]).

5 Grundsätze der IT-Governance

Die auffälligste Änderung gegenüber der zweiten Version der Norm ist die Ersetzung der bisherigen sechs Grundsätze (Verantwortlichkeit, Strategie, Beschaffung, Performanz, Konformität, Verhalten) durch die elf Governance-Grundsätze, die den Inhalt der ISO 37000 ausmachen. Die diesbezüglichen Ausführungen sind dafür verantwortlich, dass der Umfang der ISO/IEC 38500:2024 von 12 auf 21 Seiten angewachsen ist. Entsprechend der ISO 37000 sind die Grundsätze in drei Kategorien eingeteilt: primär (primary), grundlegend (foundational) und unterstützend (enabling) (vgl. Abb. 1).

- Primär:** Ein Grundsatz dieser Kategorie bildet den zentralen und wichtigsten Angelpunkt für alle anderen Grundsätze. Diese sind im Kontext des primären Grundsatzes zu verstehen und zu befolgen.

- Grundlegend:** Grundsätze dieser Kategorie sind wesentlich für die Sicherstellung einer wirksamen IT-Governance.

- Unterstützend:** Grundsätze dieser Kategorie adressieren Governance-Verantwortlichkeiten, die heutzutage für Organisationen relevant sind (nach [ISO/IEC 38500:2024, S. 6]).

Für jeden der Grundsätze wird beschrieben, wie er sich in Bezug auf die IT-Nutzung der Organisation ausprägt. Diesbezüglich werden je Grundsatz zwei bis vier konkrete Governance-Auswirkungen dargestellt (im Folgenden nach [ISO/IEC 38500:2024, S. 6-14]):

- Zweck:** Die Leitungsorgane haben zu ermitteln, ob und ggf. wie mittels – insbesondere innovativer – IT der Zweck und die Werte der Organisation besser erfüllt und der Nutzen der Leistungsangebote erhöht werden kann. Hierdurch wird der IT-Einsatz mit dem Organisationszweck abgestimmt. Den Einsatz neuer oder aufkommender IT-Lösungen an den Zweck zu binden, befähigt zudem die Mitarbeitenden, Entscheidungen im Einklang mit dem Zweck und den Werten der Organisation zu treffen und entsprechend zu handeln.
- Wertschöpfung:** Auf Basis der festgelegten und an die relevanten Stakeholder kommunizierten Wertschöpfungsziele hat die Organisation zu entscheiden, wie sie IT zur Unterstützung und Umsetzung ihres Wertschöpfungsmodells einsetzen will. Technologische Entwicklungen sind regelmäßig zu identifizieren und hinsichtlich ihrer Auswirkungen auf das Wertschöpfungsmodell der Organisation zu bewerten. Diese Bewertung hat sich sowohl auf Chancen als auch auf Risiken zu richten.

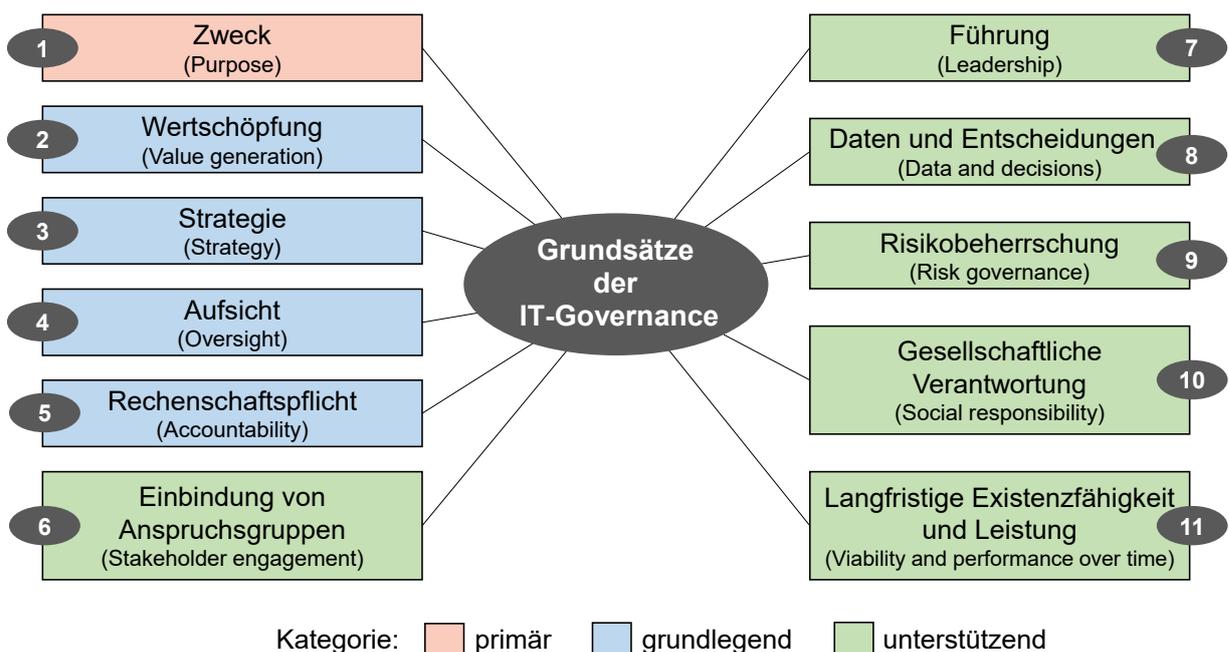


Abb. 1: Die elf Grundsätze der IT-Governance nach ISO 38500:2024 (eigene Darstellung nach [ISO/IEC 38500:2024], Übersetzung nach [E DIN ISO 37000:2024])

3. **Strategie:** Die IT-Strategie sollte auf die Strategie der Organisation abgestimmt und in diese integriert werden. Die Nutzung und Bereitstellung von IT, Daten und digitalen Fähigkeiten muss sich an der Organisationsstrategie ausrichten. Diese muss umgekehrt das Potenzial digitaler Innovationen angemessen nutzen, um sich durch entsprechende Investitionen an interne und externe Bedarfe anzupassen. Dies beinhaltet auch Strategien zur Behebung von Ausfällen von IT-Systemen und zum Umgang mit Obsoleszenz der Informationstechnik.
4. **Aufsicht:** Im Rahmen ihrer Aufsichtsverantwortung haben die Leitungsorgane sicherzustellen, dass die Zielsetzungen in Bezug auf die IT und die Umsetzung der IT-Strategie erreicht werden. So sind insbesondere die internen und externen Compliance-Vorgaben an die IT und die damit verbundenen IT-Risiken zu identifizieren. Dies gilt ausdrücklich auch für den Einsatz von IT-Dienstleistern. Die Leitungsorgane sind bei wesentlichen Pflichtverletzungen zeitnah zu informieren. Für eine effektive Aufsicht muss Transparenz gewährleistet und dafür gesorgt werden, dass Informationsfluss und Leistungsmessung die Steuerung und Entscheidungsfindung der Leitungsorgane unterstützen.
5. **Rechenschaftspflicht:** Die Leitungsorgane haben für klare Verantwortlichkeiten und Pflichten in Bezug auf die Bereitstellung und Nutzung von IT zu sorgen. Hierbei sind diejenigen, denen Verantwortung im Rahmen der Delegation übertragen wurde, bei der Entscheidungsfindung und an Überwachungsmaßnahmen adäquat zu beteiligen. Auch bei einer entsprechenden Delegation verbleibt die Rechenschaftspflicht für die IT-Governance letztendlich bei den Leitungsorganen, die hierüber einen geeigneten Nachweis zu erbringen haben.
6. **Einbindung von Anspruchsgruppen:** Der IT-Einsatz sollte generell den Anforderungen der Stakeholder (d.h. Kunden, Lieferanten, Aufsichtsbehörden, Personal), die mittels oder in Bezug auf IT mit der Organisation interagieren, entsprechen. Nur wenn Vertrauen in die IT und Zufriedenheit mit der IT erreicht werden, sind Investitionen in die IT aus Sicht der Stakeholder gerechtfertigt. Durch die Einbindung der Stakeholder wird auch eine Kultur geschaffen, die die Bereitstellung und Nutzung von IT fördert.
7. **Führung:** Die Leitungsorgane sollen eine ethische und effektive Führung hinsichtlich der Nutzung von IT in Übereinstimmung mit den Werten der Organisation sicherstellen. Eine dadurch erforderliche Organisationsentwicklung kann durch IT unterstützt werden; organisatorischer und informationstechnischer Wandel, beispielsweise durch neue IT-Services, müssen für die digitale Transformation Hand in Hand gehen. Um dies zu erreichen, benötigt die Organisation eine Lernkultur, die im Rahmen einer Qualifizierungsstrategie die Entwicklung von IT-Kompetenz fördert.
8. **Daten und Entscheidungen:** Daten sind als wertvolle Ressourcen für die Entscheidungsfindung anzuerkennen. Eine strategische Nutzung von Daten richtet sich auf die Klärung ihrer Rolle, ihres Wertes und ihrer Risiken für die Organisation. Eine verantwortliche Datennutzung wird vor allem durch eine klare Datenstrategie erreicht und zielt insbesondere auf die Anforderungen an Datenqualität und -sicherheit, aber auch auf die Beachtung von Verpflichtungen, z.B. bezüglich Datenschutz und Urheberrechten.
9. **Risikobeherrschung:** Ein Verständnis für die IT-bezogenen Risiken, Bedrohungen und Chancen ist essenziell für die IT-Governance. Die Risikoüberwachung hat kritische und strategische IT-Risiken, z.B. Cyberrisiken oder Risiken neuer Technologien, zu fokussieren. Basis hierfür ist die Festlegung des Risikoappetits in Bezug auf die IT-Nutzung. Die Organisation muss eine digitale Resilienz erreichen, sodass sie im Einklang mit den Erwartungen der Stakeholder auf interne Ausfälle oder negative externe Beeinträchtigungen der IT reagieren und sich davon erholen kann (nach [ISO/IEC 38500:2024, S. 13]).
10. **Gesellschaftliche Verantwortung:** Alle IT-bezogenen Entscheidungen müssen der gesellschaftlichen Verantwortung der Organisation gerecht werden. Die Auswirkungen des IT-Einsatzes, insbesondere automatisierter, IT-gestützter Entscheidungen, müssen vor der Implementierung berücksichtigt und geplant werden. Wo erforderlich, sind Transparenz und angemessener Zugang zu gewährleisten. Durch ethische »Checks and Balances« ist eine akzeptable Nutzung von IT, Daten und Algorithmen sicherzustellen.
11. **Langfristige Existenzfähigkeit und Leistung:** Die langfristige Existenzfähigkeit und Leistungserbringung einer Organisation hängt heute notwendig von ihren digitalen Fähigkeiten ab. Die Bereitstellung von IT-Systemen muss den sich ändernden Geschäftsanforderungen und Prioritäten der Organisation entsprechen. Hierbei muss die Effektivität der – auch von externen Dienstleistern betriebenen – IT-Infrastruktur kontinuierlich sichergestellt werden. Dies betrifft auch ihren Schutz in einem zunehmend komplexen und gefährdeten Umfeld.

6 Modell der IT-Governance

Das Modell der IT-Governance hat in der ISO/IEC 38500:2024 eine abermalige Umgestaltung erfahren. Nach wie vor wird die Unterscheidung von Governance und Management betont, wobei insbesondere auf die beteiligten Akteure abgestellt wird. So hat das Management die gesetzten Ziele zu erreichen, indem Entscheidungen innerhalb der von den Leitungsorganen festgelegten Parameter getroffen werden (nach [ISO/IEC 38500:2024, S. 14]). Die drei übergeordneten Governance-Aufgaben Evaluieren, Steuern und Überwachen (evaluate, direct, monitor) wurden um die vierte Aufgabe der Stakeholder-Einbindung ergänzt.

Optisch wurde das Modell der IT-Governance vereinfacht (vgl. Abb. 2). Die von außen einwirkenden Triebkräfte (Erwartungen der Stakeholder, Compliance-Verpflichtungen etc.) tauchen nicht mehr auf. Gleiches gilt für die explizite Benennung der Kommunikation zwischen der Governance- und der Managementebene. Letztere wird zudem nicht mehr in Personen und Managementsysteme untergliedert (vgl. [ISO/IEC

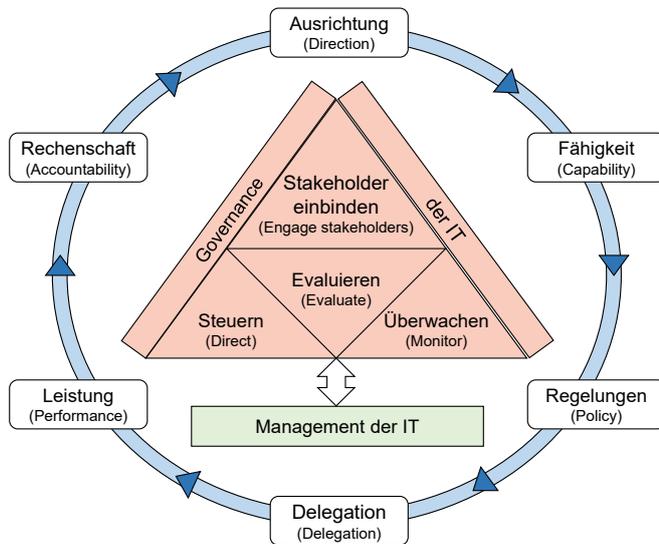


Abb. 2: Modell der IT-Governance nach ISO 38500:2024 (eigene Darstellung nach [ISO/IEC 38500:2024, S. 15, 17])

38500:2015, S. 6 f.]). Allerdings werden Governance- und Managementebene jetzt von einem Kreis eingefasst, der für das Framework für die IT-Governance steht.

Die vier übergeordneten Governance-Aufgaben sind von den Leitungsorganen wahrzunehmen (im Folgenden nach [ISO/IEC 38500:2024, S. 15 f.]):

- **Stakeholder einbinden:** Die relevanten internen und externen IT-Stakeholder sind zu identifizieren, zurate zu ziehen und geeignet einzubinden. Insbesondere ist sicherzustellen, dass es eine klare Festlegung der Pflichten in Bezug auf die Nutzung von IT und Daten gibt. Verstöße sind unmittelbar zu kommunizieren, sodass die Organisation bzw. die Stakeholder die Möglichkeit erhalten, mit den Folgen umzugehen.
- **Evaluieren:** Die Leitungsorgane haben die aktuelle und künftige Nutzung der IT zu bewerten. Hierfür sind Planungen, Vorschläge und Liefervereinbarungen heranzuziehen. Bei der Bewertung sind die internen und externen Triebkräfte, die auf die Organisation einwirken, ebenso wie die Geschäftsanforderungen zu berücksichtigen.
- **Steuern:** Die Leitungsorgane haben die Erarbeitung und Umsetzung von Strategien und Richtlinien zu steuern. Hierbei beziehen sich die strategischen Festlegungen auf die Ausrichtung der IT-Investitionen und die Zielsetzungen für die IT der Organisation, während die Richtlinien ein angemessenes Verhalten bei der Nutzung von IT vorgeben. Hierzu gehört, dass die Leitungsorgane vom Management eine rechtzeitige Informationsweitergabe und das Befolgen der elf Governance-Grundsätze einfordern.
- **Überwachen:** Die Überwachung durch geeignete Kontrollsysteme richtet sich zum einen auf die Leistungsmessung der IT. Hierdurch soll sichergestellt werden, dass Strategien umgesetzt und Geschäftsziele erreicht werden. Zum anderen ist die Compliance der IT mit gesetzlichen,

regulatorischen und vertraglichen Verpflichtungen ebenso wie mit internen Vorschriften zu gewährleisten.

7 Framework für die IT-Governance

Das Framework für die IT-Governance beinhaltet sechs für die Praxis der IT-Governance grundlegende Elemente. Diese umfassen die Festlegung und Fortschreibung von Regelungen, Entscheidungsfindungsstrukturen, Verhaltensmustern und Rechenschaftspflichten, die sicherstellen, dass das operative Betriebsmodell einen Mehrwert erbringt, die Risiken beherrscht und die Erwartungen der Stakeholder erfüllt werden (nach [ISO/IEC 38500:2024, S. 16]). Mittels der organisationsspezifischen Umsetzung des Frameworks soll insbesondere die effektive Zusammenarbeit aller Akteure in Bezug auf die IT-Governance sichergestellt werden.

Die kreisförmige Darstellung der sechs Elemente (vgl. Abb. 2) ist als Zyklus einer kontinuierlichen Verbesserung aufzufassen. Er beginnt mit der Bewertung der Ausrichtung und der benötigten Fähigkeiten und ermöglicht es der Organisation letztlich, ihre Ausgestaltung der IT-Governance an das interne und externe Umfeld anzupassen. Im Einzelnen stellen sich die sechs Elemente wie folgt dar (im Folgenden nach [ISO/IEC 38500:2024, S. 18-20]):

- **Ausrichtung:** Die Leitungsorgane legen die Ausrichtung für die Nutzung der IT fest. Diese Ausrichtung basiert auf definierten Strategien und ihrer kontinuierlichen Überwachung. Die Strategien wiederum berücksichtigen grundlegend den Zweck, die Ziele und das Wertschöpfungsmodell der Organisation. IT-seitig sind aufkommende Informationstechnologien, die digitalen Fähigkeiten der Organisation, externe Stakeholder und Möglichkeiten der Wertgenerierung durch eingebettete IT zu beachten.
- **Fähigkeit:** Governance- und Management-Akteure müssen zusammenarbeiten, um die im Hinblick auf den Organisationszweck aktuell und künftig erforderlichen digitalen Fähigkeiten zu identifizieren. Diese Fähigkeiten können sowohl intern vorhanden als auch extern bezogen werden. Auf Ebene der Governance ist zu klären, warum eine konkrete digitale Fähigkeit benötigt und von wem sie operativ erbracht wird. Die Managementverantwortung konzentriert sich auf die Art und Weise, wie diese digitale Fähigkeit funktioniert, mit welchen anderen Fähigkeiten sie verknüpft ist und wie über ihre Leistung und Konformität berichtet wird.
- **Regelungen:** Mittels Regelungen werden die Nutzung, die an die IT gerichteten Erwartungen und die Auswirkungen der IT in der Organisation gesteuert. Dabei kann eine Regelung verschiedene Formen annehmen und von einer allgemeinen Zielsetzung bis hin zu einer detaillierten Beschreibung einer digitalen Fähigkeit reichen. Regelungen sind zu dokumentieren und nach erstmaliger Erstellung fortzuschreiben. Eine Überwachung der Regelungen hat sicherzustellen, dass sie korrekt, angemessen und in Übereinstimmung mit strategischen Festlegungen angewendet werden.

- ▶ **Delegation:** Die Delegation richtet sich auf die Übertragung von Befugnissen und Verantwortlichkeiten für die Nutzung von IT. Allerdings können sich Delegation und Überwachungsmaßnahmen durch den Einsatz innovativer IT verändern. In diesem Fall ist darauf zu achten, dass Befugnisse und Verantwortlichkeiten durch IT-Funktionalitäten nicht überschritten werden. In Bezug auf die Beziehungen zu Kunden, Lieferanten und Aufsichtsinstitutionen kann dies bedeuten, dass die Regelungen zu Delegation und Überwachung über die üblichen Grenzen der Organisation hinaus ausgedehnt werden müssen, z. B. wenn Lieferanten den Bestand durch Zugriff auf die IT-Systeme der Organisation automatisiert überprüfen.
- ▶ **Leistung:** Die Leitungsorgane haben ihre Erwartungen an die Leistung der IT klar zu formulieren. Die Leistungsbeurteilung sollte sich auf das Ausmaß, in dem die IT die Organisation als Ganzes unterstützt, richten. Beispiele sind Messungen der Informations- und Betriebssicherheit, der Resilienz und der Fähigkeit, sich an veränderte Bedingungen anzupassen. In hoch dynamischen Bereichen, z. B. Cybersicherheit oder künstlicher Intelligenz (KI), sollte die Leistungsmessung auch proaktive oder vorausschauende Benachrichtigungen umfassen.
- ▶ **Rechenschaft:** Die Leitungsorgane müssen sicherstellen, dass die Regelungen für die Nutzung der IT den Erwartungen der Stakeholder entsprechen, verstanden und befolgt werden und dass ihre Einhaltung angemessen berichtet oder offengelegt wird. Hierfür bedarf es geeigneter IT-Prozesse und eines entsprechenden Berichtswesens in Verbindung mit Überwachungs- und Warnsystemen. Auch die verschiedenen IT-Managementsysteme, z. B. für Compliance- und Risikomanagement, unterstützen die Erfüllung von Rechenschaftspflichten.

8 Bewertung

Die Überarbeitung der ISO/IEC 38500 nach neun Jahren war sicherlich (über)fällig. Die Anknüpfung der ISO/IEC 38500 an die ISO 37000 ist zu begrüßen, da hierdurch IT-Governance nachdrücklich als Teil der Corporate Governance positioniert wird. Durch die erweiterten Grundsätze und insbesondere das Framework für die IT-Governance ist der in der ISO/IEC 38500:2024 beschriebene Ansatz der IT-Governance im Vergleich zu den beiden vorherigen Versionen der Norm deutlich komplexer geworden.

Anzeige

ADVISORI

Unternehmensberatung in Frankfurt am Main

INFORMATION SECURITY

Beratung in allen Aspekten der Cyber- und IT-Security bis hin zu IT-Audit und IT-Compliance

RISK MANAGEMENT

Aufbau eines verlässlichen Risikomanagement-Systems, Umsetzung und Optimierung Ihrer Risikostrategie



DIGITAL TRANSFORMATION

Maßgeschneiderte Lösungen und Expertenberatung für Ihre AI-gestützte Zukunft

REGULATORY REPORTING

Unterstützung bei Anbindung, Verarbeitung & Bereitstellung der regulatorischen Melde- und Offenlegungspflichten

WIR STELLEN EIN!
[advisori.de](https://www.advisori.de) / *karriere*

Im Vergleich zur ISO/IEC 38500:2015 fällt auf, dass die Grundsätze nicht mehr nur aus normativen Aussagen bestehen, sondern durch Erläuterungen zum jeweiligen Governance-Grundsatz ergänzt werden. Im Hinblick auf die normativen Aussagen entfällt in der aktuellen Version ihre Zuordnung zu den Governance-Aufgaben Evaluieren, Steuern und Überwachen (evaluate, direct, monitor), wodurch die Ausführungen weniger strukturiert erscheinen.

Das Modell der IT-Governance wurde umfangreich überarbeitet, blieb aber in seiner Grundstruktur erhalten. Die Einbeziehung der Stakeholder-Einbindung als Governance-Aufgabe erscheint aus COBIT-Sicht ungewöhnlich, da die Stakeholder-Einbindung dort einen Prozess darstellt, während Evaluierung, Steuerung und Überwachung Bestandteile der Praktiken aller Governance-Prozesse sind (vgl. [ISACA 2018, S. 49 f.]).

Im Vergleich mit der ISO 37000 fällt auf, dass viele – und auch wichtige – Aspekte der Grundsätze nicht in den Ausführungen der ISO/IEC 38500 berücksichtigt werden. So fordert z.B. der Strategie-Grundsatz die Einrichtung eines internen Kontrollsystems, eines Risiko- und eines Compliance-Managementsystems sowie die Nutzung externer Prüfungen (vgl. [E DIN ISO 37000:2024, S. 34 f.]), was natürlich ebenso für die IT einer Organisation gelten muss. Ein noch deutlicheres Beispiel ist der Grundsatz »Daten und Entscheidungen«, der in der ISO 37000 wesentlich umfassender behandelt wird, was die Rolle von Daten bei der Entscheidungsfindung, die Anerkennung von Daten als strategische Ressource und die Sicherstellung einer verantwortungsvollen Datennutzung betrifft (vgl. [E DIN ISO 37000:2024, S. 43-46]).

Die ISO/IEC 38500:2024 stellt die grundlegende und momentan die aktuellste Norm der ISO/IEC-3850x-Normenreihe dar. Mit ihren bedeutenden Veränderungen besteht nun die Herausforderung, die weiteren Dokumente der Normenreihe (d.h. Normen, technische Spezifikationen und technische Reports) entsprechend anzupassen. Dies zeigt sich bereits daran, dass in der ISO/IEC 38500:2024 zwar auf die ISO 37000 verwiesen wird, aber auf kein einziges Dokument der Normenreihe ISO/IEC 3850x (vgl. [ISO/IEC 38500:2024, S. 1]). Der Aufwand für die Überarbeitung der gesamten Normenreihe dürfte nicht unbeträchtlich sein. Beispielsweise ist in der ISO/IEC TR 38502 bereits ein Framework beschrieben, dessen Ausrichtung und Struktur jedoch deutlich vom dem in der ISO/IEC 38500:2024 beschriebenen Framework abweicht. Im Implementierungsleitfaden, der ISO/IEC TS 38501, ist noch auf das alte Modell der IT-Governance Bezug genommen und es werden demgemäß lediglich die bisherigen drei Governance-Aufgaben behandelt. Die Norm ISO/IEC 38507 zu den Governance-Implikationen des KI-Einsatzes stammt aus dem Jahr 2022 und referenziert dementsprechend noch die ISO/IEC 38500:2015. Im Moment sind die Dokumente der Normenreihe also alles andere als aufeinander abgestimmt. Ob die weitere Entwicklung der ISO/IEC 38500 und der gesamten Normenreihe bei der nächsten Darstellung in dieser Zeitschrift den Titelzusatz »resurrections« verdient, bleibt abzuwarten. ▀

Literatur

[E DIN ISO 37000:2024] Anleitung für Governance von Organisationen (ISO 37000:2021), Norm-Entwurf, DIN, 2024-01.

[ISACA 2018] *Information Systems Audit and Control Association (ISACA): COBIT® 2019 Governance and Management Objectives*. ISACA, Schaumburg, 2018.

[ISO 2024] *International Organization for Standardization (ISO): ISO/IEC JTC 1/SC 40 – Participation*; <https://www.iso.org/committeel/5013818.html?view=participation>; Zugriff am 19.03.2024.

[ISO/IEC 38500:2015] *ISO/IEC: Information technology – Governance of IT for the organization*, International Standard ISO/IEC 38500:2015, second edition 2015-02-15.

[ISO/IEC 38500:2024] *ISO/IEC: Information technology – Governance of IT for the organization*, International Standard ISO/IEC 38500:2024, third edition 2024-02-23.

[Klotz 2008] *Klotz, M.: IT-Governance genormt – die neue ISO/IEC 38500*. IT-Governance 2 (2008), 4, S. 21-22.

[Klotz 2016] *Klotz, M.: IT-Governance genormt – die neue ISO/IEC 38500 (reloaded)*. IT-Governance 10 (2016), 24, S. 25-27.



Michael Klotz

ist seit 1999 Professor für Betriebswirtschaftslehre, insb. Informationsmanagement, Organisation und Datenverarbeitung an der Hochschule Stralsund. Davor war er 15 Jahre in der IT-Branche als Berater, Projektmanager und Geschäftsführer tätig. Seine fachliche Arbeit dokumentiert sich in über 100 Publikationen zu IT-Governance, IT-Compliance und Projektmanagement.

Prof. Dr. Michael Klotz
Hochschule Stralsund
Fakultät für Wirtschaft
Zur Schwedenschanze 15
18435 Stralsund
michael.klotz@hochschule-stralsund.de
www.hochschule-stralsund.de