# IST IT-FACHAUFSICHT DAS GLEICHE WIE IT-GOVERNANCE IN DER ÖFFENTLICHEN VERWALTUNG?

Der Begriff „IT-Governance“ ist zwar geläufig, seine Inhalte bleiben indes oft vage. Manche verbinden IT-Governance mit IT-Steuerung, IT-Strategie oder umfassenden Prozessmodellen, andere mit kennzahlbasierter Überwachung oder IT-Controlling. Dabei gibt es bereits seit zehn Jahren eine internationale Norm ISO/IEC 38500, die Governance der IT als Teil der Corporate Governance definiert.

**| von ROGER FISCHLIN**

In diesem Artikel stellen wir die Norm ISO/IEC 38500 vor, erläutern die zum Verständnis erforderlichen Konzepte zur Corporate Governance und beschreiben die Grundsätze, wie Unternehmen den Einsatz der Informationstechnik strukturieren sollten. Wir kombinieren die Empfehlungen an eine gute Governance der IT mit den Anforderungen in der öffentlichen Verwaltung und zeigen: Der Vergleich zwischen ISO/IEC 38500 und IT-Fachaufsicht liefert eine bemerkenswerte Erkenntnis.

## CORPORATE GOVERNANCE

### Erwartung an eine gute Unternehmensführung

Corporate Governance (aus dem Englischen für Unternehmensführung und/oder Unternehmensverfassung) soll bei Stakeholdern Transparenz und Vertrauen in die Integrität und Stabilität des Unternehmens sowie dessen Erfolg schaffen. Erwartungen und Einflüsse an die Corporate Governance sind vielschichtig und resultieren aus verschiedenen Blickwinkeln:

- Die **finanziell-wirtschaftliche Sicht** spiegelt die klassische Forderung der Eigentümer nach wirtschaftlichem Handeln (Erfolg) und die der Gläubiger nach Sicherheit für ihre Investitionen wider.
- Die **Beziehungssicht** soll das Zusammenspiel und die Wahrung der einzelnen Interessen aller Beteiligten regeln.
- Die **Stakeholdersicht** zeigt die teilweise widersprüchlichen Erwartungen der Parteien und deren Berücksichtigung, die Einfluss auf die Unternehmensführung haben.
- Aus **gesellschaftlicher Sicht** soll Corporate Governance sicherstellen, dass Unternehmen bei ihrem Streben den sozialethischen Ansprüchen der Gesellschaft gerecht werden.
- Aus der **operativen Sicht** soll Corporate Governance den Rahmen (Struktur), die Binnenordnung vorgeben, wie das Unternehmen arbeitet.

Die verschiedenen Sichten können nicht isoliert betrachtet werden, sondern liefern ein Gesamtbild. So kann zum Beispiel die Binnenordnung eines Unternehmens nicht losgelöst von den Erwartungen der Stakeholder betrachtet werden.

Unter Corporate Governance versteht man ein System zum Lenken und Kontrollieren eines Unternehmens. Diese Definition mit Fokus auf der operativen Sicht geht auf den Cadbury-Bericht aus dem Jahr 1992 zurück. Als Folge eines Finanzskandals erstellte damals eine britische Kommission unter Leitung von Sir Cadbury einen der ersten Kodexe für gute

Unternehmensführung. Dieser Bericht enthält die relevanten Aspekte zum Verständnis des heutigen Governance-Konzepts und legt die Verantwortung für die Corporate Governance in die Hände eines Aufsichtsgremiums (nicht in die der obersten Manager), das

- für die Governance zuständig ist,
- über die Einhaltung von Vorgaben der Stakeholder wacht,
- aus den Vorgaben der Stakeholder Rahmenbedingungen für die strategischen Ziele des Managements ableitet,
- die Umsetzung der Strategie an die Manager delegiert und
- die Umsetzung kontrolliert.

Die Einhaltung der Vorgaben nennt man „Konformität". Geläufiger ist jedoch der Begriff „Compliance", auch wenn der sich im eigentlichen Sinne nur auf gesetzliche und regulatorische Anforderungen bezieht. Getrieben durch Finanzskandale, lag der Fokus von Governance auf der Compliance zum Schutz der Investoren und Geldgeber. Anfang der 1990er-Jahre rückte mit dem Shareholder-Value-Gedanken die Performance in den Fokus der Unternehmensführung: Ein Unternehmen, das nur nach Konformität strebt, verliert seinen eigentlichen Zweck aus dem Blick – nämlich die Ziele der Kapitalgeber zu erfüllen. Die moderne Auslegung von Corporate Governance verbindet die beiden Kernanforderungen:

- Konformität: Das Unternehmen soll die relevanten Regeln nachweislich einhalten (Prinzipien).
- Performance: Das Unternehmen soll erfolgreich sein (Ziele).

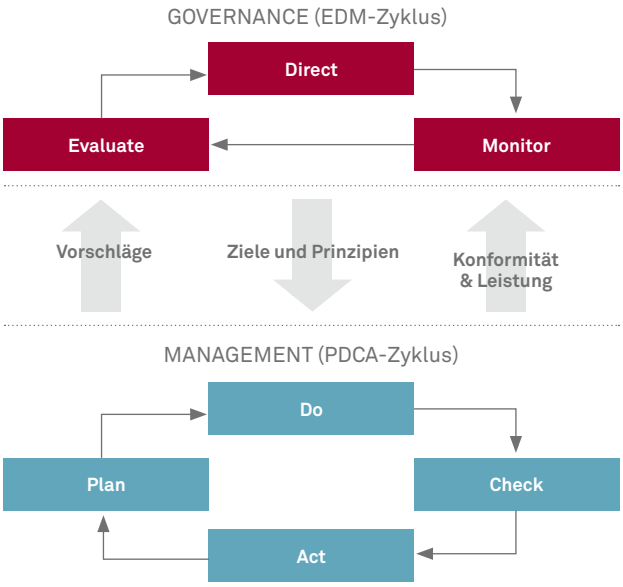


Abbildung 1: Modell des Zusammenspiels der Systeme von Governance und Management

Die ISO/IEC 38500 enthält ein Governance-Modell, das aus drei Aufgaben besteht:

- Bewerten (Evaluate): Analysieren der Situation und Entscheiden über künftiges Vorgehen
- Anweisen (Direct): Delegieren der Umsetzung
- Überwachen (Monitor): Beobachten des Umfelds und Kontrollieren der Ausführung

Governance ist also mehr als nur Kontrolle. Man spricht hier vom EDM-Kreislauf in Abgrenzung vom PDCA-Zyklus[1] des Managements. Das Aufsichtsgremium plant nicht, sondern entscheidet über Vorschläge der obersten Manager. Das Aufsichtsgremium führt nicht aus, sondern weist die obersten Manager an, den Vorschlag innerhalb ihrer Befugnisse unter Beachtung der gewünschten Verhaltensmuster umzusetzen.

Die EDM- und PDCA-Aufgaben sind nicht in einem Prozess verbunden. Vielmehr beziehen sich die Governance-Aktivitäten auf das Managementsystem in Gänze. Das Aufsichtsgremium ist nicht in die operative Arbeit der obersten Manager involviert, sondern überblickt deren Arbeit. Das Aufsichtsgremium ist auf fachliche Zuarbeiten der Manager angewiesen, sollte aber zusätzlich externe Fachmeinungen (Berater, Prüfer usw.) zurate ziehen.

Die in der Literatur häufig vorgenommene eingängige Gleichsetzung von Governance und (langfristigem) Management (Strategie) ist allerdings irreführend. Eine gute Governance gewährleistet, dass das Unternehmen eine sachgerechte und Erfolg versprechende Strategie verfolgt. Aber sie ist nicht die Strategie.

## CORPORATE GOVERNANCE DER IT

Vor rund zehn Jahren haben ISO/IEC die erste internationale Norm ISO/IEC 38500 zur Governance der IT vorgestellt, eine redaktionell überarbeitete Fassung erschien 2015. ISO/IEC interpretieren Governance der IT als Teil der Corporate Governance und orientieren sich an den Konzepten zur Unternehmensführung, wie oben vorgestellt. Angelehnt an den Cadbury-Bericht, definieren sie:

*„[Corporate Governance der IT ist das] System zum Leiten und Kontrollieren, wie die IT heute und in Zukunft eingesetzt wird."*

ISO/IEC verwenden den Begriff „Governance der IT" und grenzen sich gegen „IT-Governance" ab – als ein Schlagwort, das übermäßig und unpräzise genutzt wurde.[2] Der Ansatz als Teil der Corporate Governance bedeutet, dass das Aufsichtsgremium für die Governance der IT zuständig ist und nicht etwa eine Stabsstelle oder Abteilung in der IT.

1 PDCA-Zyklus: Planen (Plan), Ausführen (Do), Überprüfen (Check), Verbessern (Act)
2 So ist die Definition umfassender als die erste bekannte und heute oft noch genutzte Interpretation von Weill und Ross (2004), wonach IT-Governance lediglich die Festlegung von Zuständigkeiten für die Informationstechnik sei, nicht aber von Zielen und Verhaltensweisen.

| Nr. | Handlungsfelder | Grundsätze für eine gute Corporate Governance der IT |
|---|---|---|
| 1 | Verantwortung (Responsibility) | Individuen und Gruppen kennen und übernehmen ihre Verantwortung für IT-Angebot und Nachfrage. Verantwortliche haben entsprechende Befugnisse (Kompetenzen). |
| 2 | Strategie/Planung (Strategy) | In der Gesamtstrategie werden Leistungsfähigkeit und Potenziale der Informationstechnologie berücksichtigt. Die IT-Strategie ist an der allgemeinen Strategie des Unternehmens ausgerichtet. |
| 3 | Beschaffung/Bereitstellung (Acquisition) | Investitionen in Informationstechnik werden bedarfsgerecht in einem transparenten und fundierten Entscheidungsprozess getroffen. Vorteile, Möglichkeiten, Kosten und Risiken werden sowohl auf kurze als auch auf lange Sicht abgewogen. |
| 4 | Leistung (Performance) | Die IT unterstützt das Business durch Services entsprechend den heutigen und zukünftigen Leistungs- und Qualitätsanforderungen. |
| 5 | Konformität (Conformance) | Beim Einsatz der Informationstechnologie werden rechtliche Vorgaben, relevante Normen, Standards sowie ethische Grundsätze und die Selbstverpflichtung des Unternehmens berücksichtigt. |
| 6 | Menschen (Human Behaviour) | Beim Einsatz der Informationstechnologie werden Verhalten und Bedürfnisse der Menschen berücksichtigt. |

Tabelle 1: Grundsätze einer guten Governance der IT nach ISO/IEC 38500

Der Begriff „Einsatz der Informationstechnik" umfasst Planung, Design, Entwicklung, Rollout, Betrieb, Management und Anwendungen der Informationstechnik, um jetzt und künftig die Geschäftsziele zu erreichen und Werte für das Unternehmen zu schaffen. Governance der IT bedeutet, einen angemessenen Einsatz der Informationstechnik sicherzustellen.

### Governance der IT lenkt und kontrolliert den Einsatz der Informationstechnik

ISO/IEC brechen mit der verbreiteten Praxis (etwa in COBIT 4.1), Governance der IT nur als Aufsicht über die IT und ihre Arbeit zu sehen. Vielmehr müssen IT und Fachseite berücksichtigt werden:

- IT-Demand (Nachfrage): IT-Unterstützung in Geschäftsprozessen
- IT-Supply (Angebot): Realisierung der IT-Unterstützung

Eine gute Governance der IT bedeutet, beide Seiten so zu lenken und zu kontrollieren, dass das Management die Informationstechnik konform zu Regeln einsetzt und im Zusammenspiel (Alignment) Werte für das Unternehmen schafft. Die ISO/IEC 38500 enthält Empfehlungen, wie der Einsatz der Informationstechnik strukturiert werden sollte.

### Grundsätze einer guter Corporate Governance der IT

ISO/IEC fassen in der ISO/IEC 38500 Grundsätze für eine gute Governance der IT zusammen. Sie beschreiben Strukturen als Voraussetzung für einen konformen und erfolgreichen Einsatz der Informationstechnik, aber nicht, wie ein Unternehmen die IT in seinen Geschäftsprozessen einsetzen soll. So finden sich in der Norm weder Empfehlungen für Organisationsformen oder IT-Architekturen noch technische Vorgaben. Jedes Unternehmen trifft solche Entscheidungen im Wettbewerb mit Anderen in dem von der Governance der IT gesteckten Rahmen.

Tabelle 1 fasst die in sechs Handlungsfeldern geordneten Grundsätze aus der ISO/IEC 38500 zusammen. Die Handlungsfelder überschneiden sich, Querschnittsaspekte wie Risikomanagement finden sich in allen Themen. Die Prinzipien gelten für alle Organisationen. Wir werden sie im Folgenden auf die öffentliche Verwaltung und ihre Besonderheiten anpassen.

## FACHAUFSICHT UND CORPORATE GOVERNANCE DER IT

Auch wenn so nicht bezeichnet, gibt es auch in der öffentlichen Verwaltung eine Corporate Governance: Eine übergeordnete Behörde überprüft als Fachaufsicht das fachliche Handeln der ihr nachgeordneten Behörden in Hinblick auf Zweck- und Rechtmäßigkeit. Beide Seiten sollen vertrauensvoll zusammenarbeiten, die beaufsichtigte Behörde soll im Grundsatz ihre Aufgaben in eigener Zuständigkeit wahrnehmen. Das BMI stellt in den „Grundsätzen zur Ausübung der Fachaufsicht der Bundesministerien" (2008) klar, dass die Fachaufsicht nicht nur nachträgliche Kontrolle ausüben soll, sondern sieht die Verständigung auf strategische Ziele und die Steuerung über Zielvereinbarungen alternativ zu klassischen Steuerungselementen wie Weisungen oder Erlasse. Die Fachaufsicht der öffentlichen Verwaltung entspricht also der Corporate Governance, Konformität und Leistung der beaufsichtigten Behörde sicherzustellen.

Um Verwaltungsaufgaben heute zweckmäßig wahrzunehmen, ist der sachgerechte und erfolgsdienliche Einsatz der Informationstechnik unumgänglich. So betrifft die Fachaufsicht ebenso Aspekte des IT-Einsatzes: Es soll sichergestellt werden, dass die nachgeordnete Behörde die Informationstechnik konform zu Regeln der Verwaltung und des Geschäftsbereichs sowie effektiv zur Aufgabenerfüllung nutzt.

### Grundsätze einer guten Governance der IT in der öffentlichen Verwaltung

Wir formulieren Grundsätze für eine gute Governance der IT in der öffentlichen Verwaltung, indem wir die ISO/IEC 38500 mit Anforderungen an die Informationstechnik in der öffentlichen Verwaltung verknüpfen. Zur Vereinfachung beschränken wir uns auf die Bundesebene, die Empfehlungen können jedoch ohne Weiteres auf Länder- und kommunaler Ebene angewendet werden.

Die bereits genannten Grundsätze zur Ausübung der Fachaufsicht der Bundesministerien haben keinen expliziten Bezug zum Einsatz der Informationstechnik. Die gemeinsame Geschäftsordnung der Bundesministerien (GGO) enthält unter § 5 „Elektronische Informations- und Kommunikationssysteme" zwei Anforderungen:

(1) Die Bundesministerien schaffen die Voraussetzungen, um Informationen in elektronischer Form bereitzustellen, ressortübergreifend auszutauschen und zu nutzen.

| Nr. | Handlungsfelder | Grundsätze einer guten Governance der IT in der öffentlichen Verwaltung |
|---|---|---|
| 1 | Verantwortung (Responsibility) | Die beaufsichtigte Behörde hat einen Beauftragten für IT (Chief Information Officer, CIO) als Bindeglied zwischen politischer Führung und IT. CIO und Führungskräfte der beaufsichtigten Behörde sind für das IT-Management verantwortlich. Das IT-Management stellt sicher, dass sich die IT an der IT-Strategie und den Zielen der Behörde ausrichtet (strategisches IT-Management) und dass die IT-Ressourcen optimal eingesetzt werden (operatives IT-Management). |
| 2 | Strategie/Planung (Strategy) | Der Einsatz der Informationstechnik ist an den Zielen und Aufgaben der beaufsichtigten Behörde ausgerichtet. Die strategischen und organisatorischen Anforderungen leiten sich aus dem Gebot eines ordnungsgemäßen, sicheren und wirtschaftlichen Verwaltungshandelns ab.<br>Die IT-Strategie der Behörde ist im Einklang mit der IT-Strategie der übergeordneten Behörde und mit übergreifenden IT-Strategien der Verwaltung. Es werden die Voraussetzungen geschaffen, um Informationen in elektronischer Form bereitzustellen, behördenübergreifend auszutauschen und zu nutzen.<br>Die beaufsichtigte Behörde erstellt die operative IT-Planung auf Grundlage der strategischen und organisatorischen IT-Anforderungen. Die operative Planung ist ziel- und zukunftsorientiert, angemessen detailliert, aktuell und lückenlos. Sie wird kontinuierlich überprüft, fortgeschrieben und kommuniziert. |
| 3 | Beschaffung/Bereitstellung (Acquisition) | Die IT-Beschaffung gewährleistet die bedarfs- und nutzergerechte Versorgung der Dienststellen mit den zur Aufgabenerfüllung benötigten IT-Komponenten und IT-Dienstleistungen. Die beaufsichtigte Behörde beachtet den Grundsatz der Wirtschaftlichkeit und Sparsamkeit, behördenübergreifende Erbringung der IT-Leistung soll geprüft werden. Die beaufsichtigte Behörde nutzt Rahmenverträge. Technische und wirtschaftliche Abhängigkeiten von einzelnen Externen vermeidet sie möglichst. Das Personal wird entsprechend fachlicher Anforderungen und des technischen Fortschritts qualifiziert, um für die Kernprozesse und eingesetzten Technologien ausreichende Kompetenzen aufzubauen und zu pflegen. |
| 4 | Leistung (Performance) | Der Einsatz der Informationstechnik der beaufsichtigten Behörde unterstützt sowohl serviceorientiert als auch wirtschaftlich die Ziele der Verwaltung. Zur Steuerung und Kontrolle der Zielerreichung hat die beaufsichtigte Behörde ein angemessenes IT-Controlling. |
| 5 | Konformität (Conformance) | Beim Einsatz der Informationstechnologie hält die beaufsichtigte Behörde alle Gesetze, Haushaltspläne, Verwaltungsvorschriften und Grundsätze ein. Es werden insbesondere die Regelungen zum E-Government, zur Revisionsfähigkeit, zur Informationssicherheit, zum Datenschutz, zum Arbeitsschutz beachtet. Maßnahmen der internen Kontrolle werden dokumentiert. |
| 6 | Menschen (Human Behaviour) | Beim Einsatz der Informationstechnologie berücksichtigt die beaufsichtigte Behörde die Bedürfnisse der betroffenen Menschen, etwa zum Arbeits- und Datenschutz, Barrierefreiheit und Ergonomie. Ein Akzeptanzmanagement stellt sicher, dass die Organisationseinheiten und die Anwender hinreichend eingebunden werden. |

Tabelle 2: Grundsätze einer guter Governance der IT in der ÖV (angelehnt insbesondere an die IuK-Mindestanforderungen)

(2) Zur Gewährleistung einer geschützten elektronischen Kommunikation zwischen den Bundesministerien wird eine sichere ressortübergreifende Kommunikationsinfrastruktur betrieben.

Des Weiteren hat § 3 Abs. 4 einen Bezug zum IT-Angebot: „(4) Gleichartige Aufgaben, wie zum Beispiel aus dem Bereich der internen Servicebereiche, sollen zentral durch ein Ressort wahrgenommen werden, soweit dies zweckmäßig und wirtschaftlich ist."

Eine weitere Quelle sind die Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik (2016). Die Rechnungshöfe adressieren in ihrer Leitlinie implizit die Themenfelder der Norm, weisen allerdings Informationssicherheit als Teil der Governance der IT aus.[3] Im Anhang der Mindestanforderungen referenzieren die Prüfer auf Standards und Normen für die Umsetzung.

In Tabelle 2 sind die Grundsätze für den Einsatz der Informationstechnik in der öffentlichen Verwaltung basierend auf der ISO/IEC 38500 zusammengefasst. Sie können als Ausgangsbasis für die Fachaufsicht dienen, welche Strukturen sie bei der nachgeordneten Behörde für den Einsatz der Informationstechnik erwartet. Unter Umständen kommen Themenfelder hinzu, Grundsätze werden erweitert oder detailliert. Wichtig ist, dass es Rahmenbedingungen sind und nicht operative Entscheidungen, denn die beaufsichtigte Behörde soll ihre Aufgaben in eigener Zuständigkeit wahrnehmen. Die Grundsätze sollten langfristig gelten und allgemeingültig sein; man sollte beispielsweise die Einhaltung aller relevanten Gesetze und Vorschriften als Prinzip vorgeben und nicht einzelne, aktuell relevante Regelungen aufführen.

Viele Unternehmen haben bis heute noch kein klares Bild von „IT-Governance" und berufen sich auf Standards wie COBIT, genauer auf umfangreiche IT-Prozessmodelle. Hier heben sich die Grundsätze zur Ausübung der Fachaufsicht der Bundesministerien in Verbindungen mit den Mindestanforderungen der Rechnungshöfe zum Einsatz der Informationstechnik wohltuend ab. Die öffentliche Verwaltung ist nah am Konzept der ISO/IEC 38500 und der Grundsätze für eine gute Governance der IT – näher als die meisten Unternehmen noch heute.

## FAZIT

Nachdem im Artikel das Konzept der ISO/IEC 38500 für die Governance der IT aus der Corporate Governance hergeleitet und sowohl das EDM-Modell als auch die Grundsätze für eine gute Governance der IT vorgestellt wurden, zeigte sich: Das Konzept kann auf beliebige Institutionen angewendet werden – auch auf die öffentliche Verwaltung.

Dabei fällt auf, dass sich die öffentliche Hand mit der IT-Fachaufsicht und den Grundsätzen zum IT-Einsatz inhaltlich bereits erfreulich nah an modernen Governance-Ansätzen wie die der ISO/IEC 38500 orientiert. ●

## LITERATUREMPFEHLUNGEN


- Bundesministerium des Innern (BMI): „Grundsätze zur Ausübung der Fachaufsicht der Bundesministerien", 2008. Online verfügbar auf https://www.verwaltung-innovativ.de
- Bundesministerium des Innern (BMI): „Gemeinsame Geschäftsordnung der Bundesministerien (GGO)", 2011. Online verfügbar auf http://www.verwaltungsvorschriften-im-internet.de
- Bundesrechnungshof: „Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik – Leitlinien und gemeinsame Maßstäbe für IT-Prüfungen – (IuK-Mindestanforderungen 2016)", 2016. Online verfügbar auf https://www.bundesrechnungshof.de
- Committee on the Financial Aspects of Corporate Governance: „Financial Aspects of Corporate Governance" (Cadbury-Report), 1992. Online verfügbar unter http://www.ecgi.org/codes/documents/cadbury.pdf
- ISACA: „COBIT 5 – Rahmenwerk für Governance und Management der Unternehmens-IT", 2012. Online erhältlich auf http://www.isaca.org/COBIT/Pages/COBIT-5-german.aspx
- International Organization for Standardization (ISO): „ISO/IEC 38500: Corporate Governance of Information Technology", 2008.
- Tricker, B.: „Corporate Governance: Principles, Policies and Practices", Oxford University Press, Oxford, 2015.
- Weill, P.; Ross, J.: „IT Governance", Harvard Business School Press, Boston, 2004.


3 ISO/IEC sehen Governance der Informationssicherheit als separate Disziplin, da diese auch Informationen erfasst, die nicht elektronisch verarbeitet werden, und stärker den Umgang mit Risiken im Unternehmen betreffen (vgl. ISO/IEC 27014).