GMRC
International Institute For Governance, Management, Risk & Compliance

virtuelle hochschule bayern

CLASSIC VHB KURS:

ESGRC

Environmental, Social, Governance, Risk & Compliance –

Anforderungen an Organisation und Managementsystem

Folge 1:

Was heißt nachhaltige Führung (ESGRC) eigentlich und warum geht das alle etwas an?

Vgl. ISO Harmonized Structure: 2021, Einleitung

Eine Lerneinheit von Prof. Dr. Andreas Grötsch in [illegible] Josef Scherer, 2023©

A	**Allgemeinwissen:** Alles, was nicht mit Level „B“ oder „M“ bezeichnet ist, gehört zu den Basics.
B	**Bachelor:** Die mit Level „B“ gekennzeichneten zusätzlichen Vertiefungsaufgaben ergeben Bachelor-Niveau.
M	**Master:** Die mit Level „M“ gekennzeichneten zusätzlichen Vertiefungsaufgaben ergeben Master-Niveau.

1. Lernziele und „Lernstoff“

1.1 LERNZIELE

Sie sollten wissen, verstehen und mit eigenen Worten erklären können,

- **was nachhaltige Führung (ESGRC) bedeutet,**

und

- **welche Auswirkungen das auf Ihren Arbeitsbereich / Ihre Prozessabläufe in Ihrem Beruf hat.**

M Bitte schreiben Sie bzgl. dieser Lektion ein „reflective paper“ mit Soll-Ist-Abgleich und Handlungsempfehlungen für die Organisation, für die Sie tätig sind.

1.2.1 Einführung: Über uns, über Trends und über unser Integriertes GRC-Managementsystem als Grundlage für „Unternehmensführung 4.0“, Resilienz und Zukunftsfähigkeit[1]

Wer sind wir und was machen wir? „Unternehmenssteckbrief“ mit Finanz-, Ertrags- und Bilanz-Kennzahlen

□ **Unternehmensbeschreibung in Kurzfassung**

GRI 102: ALLGEMEINE ANGABEN 2016

Organisationsprofil

102-1 Name der Organisation
102-2 Aktivitäten, Marken, Produkte, Dienstleistungen
102-3 Hauptsitz der Organisation
102-4 Betriebsstatten
102-5 Eigentumsverhältnisse und Rechtsform
102-6 Belieferte Märkte
102-7 Größe der Organisation
102-8 Informationen zu Angestellten und sonstigen Mitarbeiterinnen und Mitarbeitern
102-9 Lieferkette
102-10 Signifikante Änderungen in der Organisation und ihrer Lieferkette
102-11 Vorsorgeansatz
102-12 Externe Initiativen
102-13 Mitgliedschaften in Verbänden und Interessensgruppen

□ **Finanz-, Ertrags- und Bilanzkennzahlen der N. N. (Firma)**

Beispiel aus der Praxis:

Quelle: STRABAG-Geschäftsbericht 2018, S. 23 ff. (abrufbar im Internet):

Über diesen Bericht

Für das Geschäftsjahr 2018 erstellt die STRABAG SE – wie auch bereits in den Vorjahren – einen kombinierten Geschäftsbericht, der die Lage des Konzerns zum 31.12.2018 wiedergibt.

Finanzielle und nichtfinanzielle Informationen geben Aufschluss über die wesentlichen ökonomischen, ökologischen, gesellschaftlichen und Governance-bezogenen Auswirkungen unserer Geschäftsaktivität.

[1] Scherer/Fruth/Grötsch (Hrsg.), Digitalisierung, Nachhaltigkeit und „Unternehmens-führung 4.0“ (GRC) mit Digitalisiertem Integrierten GRC-Managementsystem, 2021, mit e-Book, Einleitung

So wie unsere Strategie auf verantwortungsvolles, nachhaltiges Handeln ausgerichtet ist**, spiegelt sich dies auch in unserer Berichterstattung wider: **Dieser Geschäftsbericht zeigt, wie alle Nachhaltigkeitsaspekte ganzheitlich in unserer Strategie aufgehen: Die Inhalte unserer strategischen Felder – Ökonomische, Ökologische und Gesellschaftliche Verantwortung, Menschen & Arbeitsplatz, Business Compliance sowie Corporate Governance – behandeln wir umfassend in unterschiedlichen Kapiteln.

*(...) Der **möglichst schonende Umgang mit Ressourcen ist einer von vielen Grundwerten**, die sich durch unsere Arbeit ziehen und der als „**Nachhaltigkeit“ auch in unseren Konzernwerten** verankert ist.*

Beispiel aus der Praxis: Organisationsprofil

Quelle: STRABAG-Geschäftsbericht 2018, S. 2 (abrufbar im Internet):

STRABAG ist ein europäischer Technologiekonzern für Baudienstleistungen, führend in Innovation und Kapitalstärke. Unser Angebot umfasst sämtliche Bereiche der Bauindustrie und deckt die gesamte Bauwertschöpfungskette ab. Wir bringen Menschen, Baumaterialien und Geräte zur richtigen Zeit an den richtigen Ort und realisieren dadurch auch komplexe Bauvorhaben – termin- und qualitätsgerecht und zum besten Preis.

Beispiel aus der Praxis: Finanz-, Ertrags- und Bilanz-Kennzahlen im Überblick

Quelle: STRABAG-Geschäftsbericht 2018, S. 3 ff. (abrufbar im Internet):

FINANZKENNZAHLEN

	2014	*2015*	*2016*	*2017*	*Δ %*	*2018*
Leistung (€ Mio.)	*13.566,00*	*14.289,76*	*13.491,03*	*14.620,89*	*12*	*16.322,88*
Umsatzerlöse (€ Mio.)	*12.475,67*	*13.123,48*	*12.400,46*	*13.508,72*	*13*	*15.221,83*
Auftragsbestand (€ Mio.)	*14.403,44*	*13.134,58*	*14.815,79*	*16.591,87*	*2*	*16.899,71*
Mitarbeiteranzahl (FTE)	*72.906*	*73.315*	*71.839*	*72.904*	*4*	*75.460*

ERTRAGSKENNZAHLEN

Ein **strategisches überlebensnotwendiges Ziel**, das derzeit nahezu alle Unternehmen / Organisationen mehr oder weniger effektiv verfolgen, **ist die Digitale Transformation**.

Dadurch ergibt sich in vielen Unternehmen **ein z. T. geändertes Geschäftsmodell** oder eben auch eine verstärkt „**geistige Leistung“** (intellectual property / digital assets), die aus Wissen in Form von Prozessen mit zugehörigen Komponenten (Rollen, Ziele, Ressourcen), IT-Systemen und IT-Tools, Algorithmen, Robotern und an verbleibenden Stellen Menschen mit angemessenen Kompetenzen und Einstellungen besteht.

Beispiel aus der Praxis: Aktivitäten eines Konzerns im Bereich Innovation

Quelle: STRABAG-Geschäftsbericht 2018, S. 176 (abrufbar im Internet):

(…) Um diesen Wandel aktiv mitzugestalten und ihn gewinnbringend für sich zu nutzen, gibt sich der STRABAG-Konzern eine technologische Ausrichtung, (…)

Ein besonderer Fokus lag dabei 2018 auf der Digitalisierung (…)

*(…) Daher gilt es, den Umfang und idealerweise die Tragweite der Veränderungen zu erkennen. Denn **in Zukunft wird der unternehmerische Erfolg von der Fähigkeit abhängen, Trends zeitig zu erkennen und auf diese neue Komplexität vorbereitet zu sein.** Unser Handeln mit Bezug auf die Innovationsaktivität ist daher entsprechend strategisch zu steuern.*

*(…) Denn Innovation steht für einen Prozess, der Neues bringt. **Dazu müssen eingeführte Routinen abgeändert, Widerstände überwunden, Teilorganisationen angepasst werden**.*

*Damit Innovationen erfolgreich werden, sind diese entsprechend umsichtig **in das Wirkungsgefüge der Organisation einzuführen**, um den vielschichtigen Interessen der unterschiedlichen Anspruchsgruppen – u. a. Eigentümer- und Auftraggeberseite sowie Mitarbeiterinnen und Mitarbeiter – Rechnung zu tragen.*

***Die Digitalisierung ist aktuell eine der wichtigsten Fragen im Themenkomplex „Innovation“ bei STRABAG.** Sie ist **ein Megatrend**, der auch die traditionellen Bauprozesse verändern wird, indem sie eine schnelle und weltweite Vernetzung von Dingen, Maschinen („Internet der Dinge“) und Menschen gestattet. (…)*

Für STRABAG bedeutet der Trend zur Digitalisierung, dass alle wesentlichen Geschäftsprozesse – Planung, Ausführung, Produktion, Betrieb und Administration – an diese neue Art der Informationsverarbeitung schrittweise angepasst werden müssen.

1.2.2 Erste Definitionen

Was heißt Governance, Risk, Compliance, GRC, Managementsystem und Integriertes GRC-Managementsystem?

Corporate Governance heißt in etwa „Angemessene Interaktion zwischen den Organen [Gesellschafter, Leitung (Vorstand / Geschäftsführer) und Aufsichtsgremium (Aufsichtsrat / Beirat)] sowie ordnungsgemäße Unternehmensführung und -überwachung“.

Governance ist mehr als Management:
Governance soll auch gesellschaftliche Verantwortung (Corporate Social Responsibility (CSR) mit ökonomischer, sozialer und ökologischer Nachhaltigkeit) und Integrität / Ethik umfassen.

Risikomanagement beschäftigt sich mit Unsicherheiten bei Entscheidungen und Zielerreichung. Es hilft, Gefahren (und Chancen) zu identifizieren, zu bewerten und zu steuern.

Compliance bedeutet pflichtgemäßes Verhalten in Hinblick auf allgemein verbindliche Regeln (Gesetze, Rechtsprechung), aber auch in Hinblick auf für verbindlich erklärte (interne) Vorgaben [z.B. Regelungen aus dem „Code of Conduct“ (unternehmensspezifische Verhaltensregelungen) oder Anstellungsvertrag].

Governance, Risk und Compliance „zusammen“, also **„GRC“** ist u.U. etwas anderes als die Summe dieser drei Komponenten. Eine Legal-Definition gibt es hier nicht. GRC könnte (leider etwas komplex) mit „Integre, nachhaltige, complianceorientierte und risikobasierte Interaktion der Organe und Unternehmensführung und -überwachung“ übersetzt werden.

Die Begründung, weshalb Governance compliance-orientiert sein muss: Compliance bildet generell den rechtlichen, zwingenden Rahmen für unternehmerisches Handeln.

Risikobasiert muss Unternehmensführung sein, weil andernfalls nicht wie ein „gewissenhafter“ Unternehmer, Vorstand, Geschäftsführer agiert werden würde: Gefahren (und Chancen) zu identifizieren, bewerten und steuern, ist Voraussetzung für die Erreichung der Ziele.

Nachhaltigkeit könnte mit „*bei Fortschritt bewahrend ausgerichtetes Entscheiden und Handeln*“ beschrieben werden.

Ein **Managementsystem** besteht aus Komponenten, wie Aufbau- und Ablauforganisation mit dem Zweck, eine Organisation bei Entscheidungen, Zielsetzung und Planung, Umsetzung sowie Steuerung und Überwachung zur Erreichung zwingender und fakultativ gesetzter Ziele zu unterstützen.

In diesem Bericht wird das Managementsystem der N. N. (Firma), das mehrere Unternehmensfunktionen (z.B. Risiko-, Qualitäts-, Umwelt-, Arbeitssicherheits- und Compliancemanagement) digitalisiert und integriert, **„Digitalisiertes Integriertes GRC-Managementsystem** genannt.

Wie viele Managementsysteme gibt es im Unternehmen?

In der Praxis herrscht z. T. der Irrglaube vor, es gäbe im Unternehmen Raum für eine beliebige Vielzahl von Managementsystemen. Auch in diversen ISO-Standards wird bei der Definition von „Managementsystem“ festgestellt, dass es sich auf alle oder einzelne Themenbereiche (z.B. Compliance, QM, Umwelt, etc.) beziehen kann.

Genährt wird dieser alle Manager und Mitarbeiter abschreckende oder frustrierende Gedanke durch die „Erfindung“ ständig neuer „Managementsysteme“.

Positiv ist die großzügige Überschneidung dieser Standards, so dass beispielsweise die Implementierung der Anforderungen an QM, Umwelt- und Arbeitssicherheitsmanagement bereits einem Großteil des Integrierten Risiko-Managementsystems abdecken mag.

Die bereits vorhandenen, aber in diversen „Ablagen“ verstreuten Komponenten müssten zunächst gesucht, identifiziert und strukturiert vernetzt in die Prozesse / (Ablauf-) Organisation eingebaut werden.

Die Rolle der IT-Lösungen für Managementsysteme

Die IT spielt hier zunächst nur eine sekundäre Rolle, wenngleich die Bedeutung der IT aufgrund der Digitalisierung als „zentrales Nervensystem“ überproportional wächst. Insofern ist zunächst ein Gesamtkonzept für die unternehmensweite IT-Infrastruktur zu schaffen, das diverse Systeme oder Insellösungen verbindet. Für große Unternehmen eignet sich beispielsweise SAP mit Schnittstellen für zahlreiche Spezial-Systeme, für kleine nicht unbedingt[2]: Wichtigste Voraussetzung für Mehrwert ist die konsequente „Fütterung“ und Pflege des Systems und die einfache Handhabbarkeit für alle Mitarbeiter.

Das Unternehmensflugschiff

Die diversen zu digitalisierenden und mit GRC-Komponenten anzureichernden (Prozess-) Themenfelder einer Organisation (Führungs-, Kern- und Unterstützungsprozessthemenfelder) lassen sich bildhaft mit einem „Unternehmensflugschiff“ darstellen:

[2] Hier gibt es diverse Anbieter, bzw. Produkte (auch internetbasierte, mit und ohne Cloud-Lösung und z.T. frei verfügbar), z.B. „ADO GRC“„Pro Alpha“, „AMS“, „Navision“, etc.

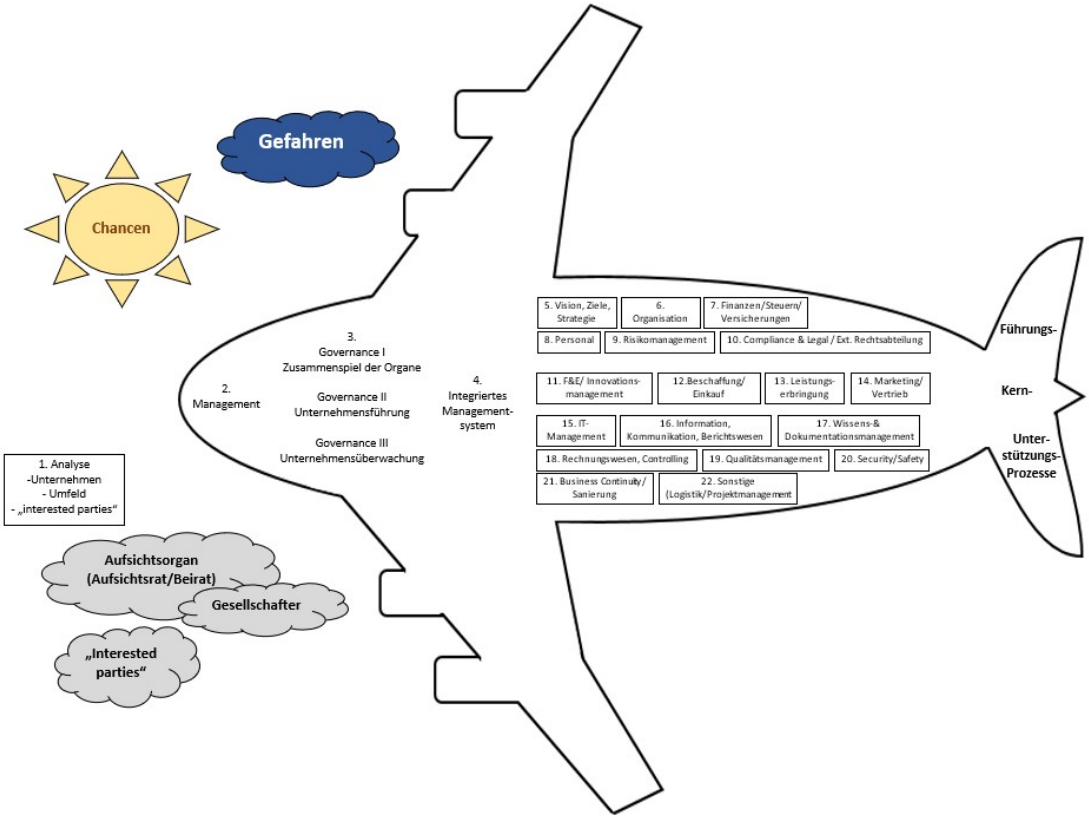


Abbildung 1: Das Unternehmensflugschiff und die vom hier dargestellten digitalisierten Integrierten GRC-Managementsystem behandelten Felder: Alle! Vgl. hierzu auch ÖNORM 4901 ff.:2020 (Risiko-Managementsystem), Anhang: Dort ist das „Unternehmensflugschiff" abgebildet und kommentiert.

Das **„Unternehmensflugschiff"** des „Ordentlichen Kaufmanns 4.0" fliegt mithilfe von **Governance (Ziele setzen, planen, umsetzen, steuern, überwachen)** durch die raue Welt des Wirtschaftslebens.

Das **„Compliance-Cockpit"** zeigt Pilot und Crew die **rechtlichen Grenzen / Rahmenbedingungen** und (kreative) Möglichkeiten zur Erfüllung der vielfältigen Anforderungen auf: In bestimmten Hoheitsgebieten / Korridoren darf das Flugschiff sich nicht bewegen!

Der **„Risikomanagement-Radar"** zeigt **Chancen** (günstige Luftströmungen und Kurse [Trends]) **und Gefahren** (nahende Stürme oder Wettbewerber auf Kollisionskurs) auf und hilft, **durch (kreative) Lösungen** zur Steuerung der (Compliance-) Risiken **die Zielerreichung sicherzustellen.**

GRC ist „Ziel-führend"!

1.2.3 Tempora mutantur: Trends

„Tempora mutantur, nos et debemur mutare in illis": Die Zeiten ändern sich und wir müssen uns mit ihnen ändern.

Die aktuellen (Mega-) Trends bringen viele neue Anforderungen, Gefahren, aber auch Chancen: Mit „business as usual“ ist das Ziel „nachhaltige Existenzsicherung“ kaum zu erreichen.

Governance, Risk und Compliance soll zum einen helfen, durch Prophylaxe den Eintritt von Zielabweichungen oder Pflichtverletzungen, Schadens- und Haftungsfällen zu vermeiden. Zum anderen sollen eingetretene Zielabweichungen oder Pflichtverstöße frühzeitig erkannt und bewertet und es muss angemessen darauf reagiert werden.

1.2.4 Motivatoren für Digitalisierung, Nachhaltigkeit und Einführung eines digitalisierten Integrierten GRC-Managementsystems

- □ Intrinsische Motivation der Leitung und/oder Aufsichtsgremium, um die Existenz nachhaltig zu sichern (strategische Bedeutung) und die Zielerreichung zu fördern
- □ „Wunsch“ nach Struktur, Transparenz, Effektivität und Effizienz
- □ Sonstiges?

Unser „klassisches und neues Geschäftsmodell“

Fast jede Organisation hat ein individuelles Geschäftsmodell, also auch individuelle Geschäftsprozess-Abläufe („Kernprozesse“).

Die nachfolgende Abbildung zeigt als Modell (!), wie ein standardisierter Kernprozess (nach ISO 9001:2015) in Anlehnung an BPMN 2.0 modelliert werden könnte. Der Abschnitt ganz unten (Swimlane „IT-Systeme“) soll zeigen, dass bei Durchführung der einzelnen Prozessschritte diverse IT-Systeme zum Einsatz kommen.

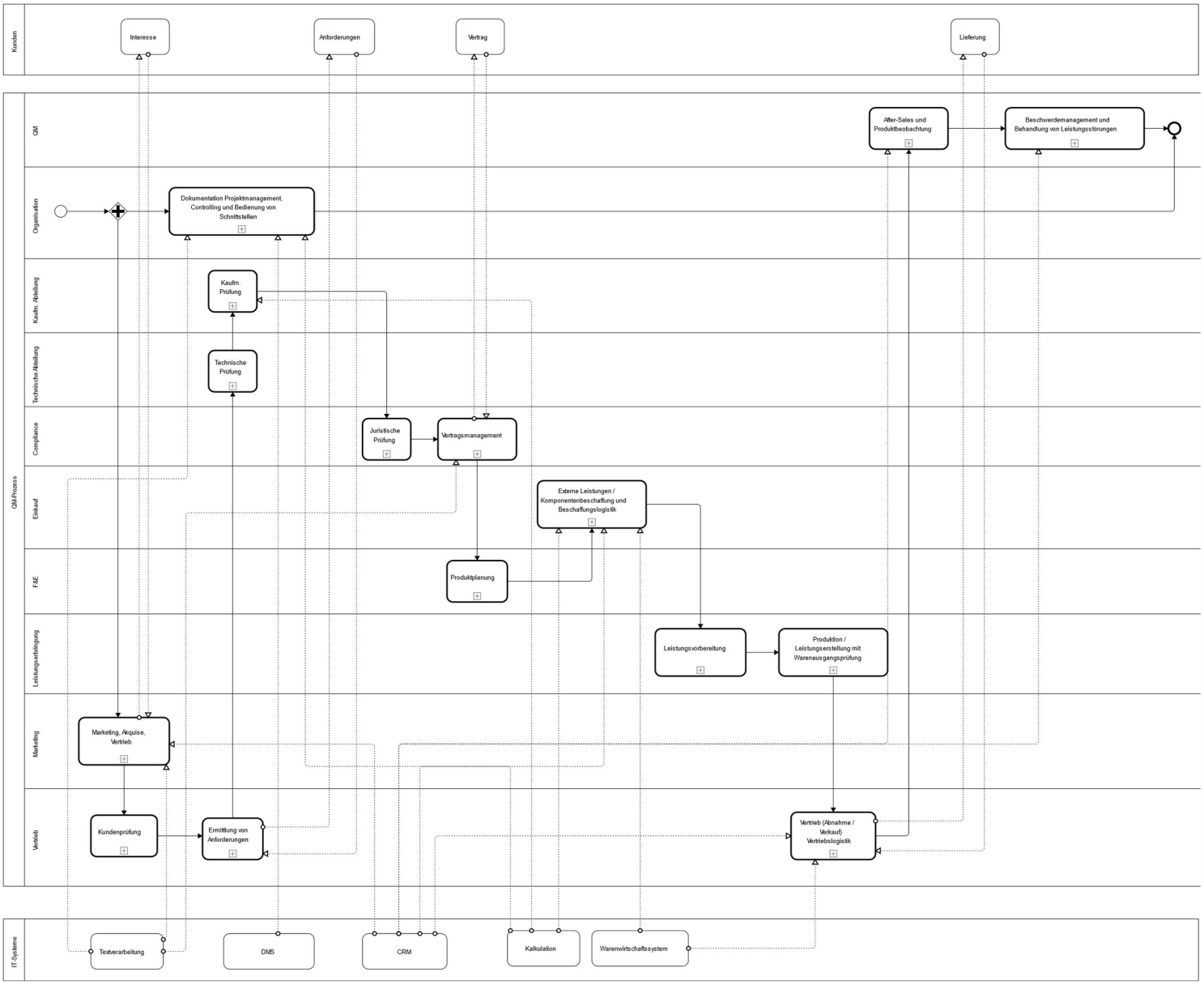


Abbildung 2: „Was machen wir?“ Schematische Darstellung eines standardisierten Hauptprozess-Stranges: Vernetzung von Aktivitäten und Komponenten

In den modellierten, teil-automatisierten (Einkaufs-, Leistungserstellungs-, Vertriebs-, Personal-, etc.-) Prozessen sorgen integrierte Kontrollen **(Internes Kontrollsystem-IKS**), Risiko- und Compliance-„Steckbriefe“ für Prozesstreue.

Die Prozesstreue kann dadurch künftig überwiegend in Echtzeit per Knopfdruck („remote“) überprüft werden und **erspart viel Zeit, Nerven und Geld** durch Reduzierung der Überwachungsaktivitäten durch Menschen.

Über ein **GRC-Tool**, das die **modellierten Prozesse mit den diversen Komponenten**, Rollen, Verantwortlichkeiten, Ressourcen, Dokumenten, etc. **in einem „Repository“ (Datenraum) verknüpft** und **via „Human Workflows“ die prozessverant-**

wortlichen Mitarbeiter zur Prozesstreue anhält, lässt sich das „digitalisierte Integrierte GRC-Managementsystem“, das all diese Anforderungen erfüllt und die Zielerreichung steuert, darstellen.

In softwaregestützten Systemen ist hier vor allem auf den integrierten und auf Basis eines wiederverwendbaren Grundkatalogs (Repository) durchführbaren Betrieb der folgenden Themen zu achten:

- ☐ Prozessdokumentation und -management (QM)
- ☐ Prozessausführung (Workflows)
- ☐ Risiko-, Kontroll- und Compliancemanagement (GRC)
- ☐ Verwaltung der damit einhergehenden zentralen Ressourcen wie Rollen, IT-Systeme und Dokumente

Die **meisten unternehmerischen Aktivitäten laufen als Prozesse ab**.

Diese werden auch künftig zum (wesentlichen) Teil noch von Menschen ausgeführt.

Auch, um **auf der „Prozessebene“** das „Richtige richtig zu tun“, ist für Management und Mitarbeiter die angemessene Einstellung auf der kognitiven und emotionalen Ebene enorm wichtig (vgl. Punkt 7.2):

Tone from the top, Kultur, Awareness, Kompetenzen, Motivation u.v.m…

Erst dann kann eine Ablauforganisation „wirksam“ („gelebt“) werden.

Anforderungen an Governance-Strukturen des „Ordentlichen Kaufmanns“ und seine Organisation

Werke wie „Der Kaufmann von Venedig“ von William Shakespeare oder „Die Buddenbrooks“ von Thomas Mann beschreiben den im Mittelalter zunächst in Italien und später auch in Nordeuropa (z.B. bei der Hanse) geprägten Unternehmer-Typen:

Er vereinte stets theoretische und praktische Fähigkeiten bzgl. wirtschaftlicher und betrieblicher Prozesse, um Anforderungen und Ziele diverser Interessensgruppen zu erfüllen, mit (Charakter-) Eigenschaften wie Vertrauenswürdigkeit, Organisationstalent, Ehrlichkeit, Zuverlässigkeit, Gewissenhaftigkeit, Fleiß, Mut und Integrität.

Die derzeitigen Megatrends „Digitalisierung, Nachhaltigkeit, Regulierung (Governance-, Risiko- und Compliancemanagement („GRC“)) und Fachkräftemangel“ stellen hohe neue Anforderungen.

Unter anderem muss der „Ordentliche Kaufmann 4.0“ über eine angemessene strategische **digitale Kompetenz** verfügen, Trends frühzeitig erkennen und angemessen darauf reagieren-

Trends: Compliancemanagement: „Eine neue Ära bricht an“

Aufgrund einiger prominenter Fälle spricht sich mittlerweile sehr schnell herum, dass vieles, was früher noch toleriert oder nicht konsequent verfolgt wurde, nun jedoch empfindlich geahndet wird.

Relevante Standards:

Auf internationaler Ebene (ISO) und auf deutscher Ebene über die DIN werden derzeit die Standards ISO 37000 Governance of Organizations, ISO 37001 Anti-Korruptions-Managementsystem, ISO 37002 Whistleblowing-Managementsystem, ISO 37301 Compliance-Managementsystem, ISO 37003 Anti-Fraud Controls neu entstehen bzw. überarbeitet.

Vgl. auch U.S. Department of Justice 6 / 2020: Evaluation of Compliance Programs

Trends: Risikomanagement: „High risk, no fun!“

Bereits Anfang der 2000er-Jahre tauchten die ersten Gerichtsentscheidungen gegen Geschäftsleitungen mit dem Vorwurf der unterlassenen Einrichtung eines Risiko-Managementsystems auf:

Fall: „Haftung wegen unterlassener Einrichtung eines Risiko-Managementsystems“

Am 08.07.2004 urteilte das Verwaltungsgericht Frankfurt am Main, die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) habe rechtmäßigerweise vom Aufsichtsrat verlangt, er müsse den Vorstand eines Versicherungsunternehmens abberufen, was auch befolgt wurde. Das Verwaltungsgericht berief sich u. a. darauf, dass der Vorstand es unterlassen hatte, ein Risiko-Managementsystem einzurichten.

Relevante Standards:

Derzeit erarbeitet die Austrian Standards International eine auf der ISO 31000:2018 beruhende zertifizierbare ÖNORM 4901 ff. zum Risiko-Managementsystem.

Der IDW PS 340 (Risikofrüherkennungssystem) wurde 2020 neu gefasst und wird künftig von Wirtschaftsprüfern bei Abschlussprüfungen herangezogen: Unter anderem verlangt der Standard jetzt die Quantifizierung und Aggregation von Risiken.

Trends: Haftung von Führungskräften und Reputationsschäden

Die „gefühlte“ **Verschärfung von Haftungs- und Sanktionsgefahren** für Vorstände, Geschäftsführer, Aufsichtsräte, Führungskräfte und sogar Gesellschafter mit dem Vorwurf, pflichtwidrig gehandelt zu haben, **ist objektiv messbar:**

Im 10-Jahreszeitraum 1986-1995 gab es genauso viele Urteile zur Haftung von Führungskräften, wie in den letzten 100 Jahren zuvor.
Für die nachfolgenden 10-Jahreszeiträume 1996-2005 und 2006-2015 wurde eine nochmalige Verdoppelung gemessen bzw. geschätzt!

Sogar der im Großen und Ganzen pflichtbewusst Agierende sieht sich nicht nur mit zivilrechtlichen Risiken, sondern auch der Gefahr der Strafbarkeit immer häufiger bedroht.

Kennen Sie Zeitfresser?

Studie: Unternehmer beschäftigen sich im Schnitt zu 80% ihrer Zeit mit der Lösung (unnötiger) Probleme.

Nur der Rest (20%) bleibt für Themen wie Strategie, Planung und Innovation.

„Verkehrtes Pareto-Prinzip“

Unternehmen, Manager und Mitarbeiter stoßen auf neue Herausforderungen bei ihrer täglichen Arbeit

Daraus erwächst auch das gemeinsame **Bedürfnis** der Betroffenen **nach passenden Tools**, die Management und Mitarbeiter zugleich unterstützen, ihre Aufgaben rechtssicher zu erfüllen: **Prozesse, die auch die Wirksamkeit (das „Gelebt werden“) von Compliance und Qualität sicherstellen.**

Ein „Hemmschuh“: Geringer Reifegrad bei Digitalisierung von Prozessen

Häufig wird der **Unternehmensalltag** noch durch E-Mails, Excel-Tabellen und mit MS-Office bestritten. Die Prozesse sind oft nicht dokumentiert oder nicht aktuell, beziehungsweise nicht nachverfolgbar.

Bei **Prozessanpassungen** müssen teure IT-Spezialisten erst mal die Zeit finden, um die Unternehmen zu unterstützen. E-Mails werden nach Gießkannenprinzip an alle verteilt, so dass jeder in einer E-Mail-Flut versinkt. Sofern Prozesse existieren, sind diese nicht ausreichend mit Governance-, Risk-, oder Compliance-Komponenten angereichert.

Mit (teil-) automatisierten Prozessen dagegen wird der Mensch und Mitarbeiter durch den Prozess geführt und damit zur Zeit-, Rechts- und Systemtreue angehalten. Dadurch könnten auch viele Probleme vermieden werden, die durch die **Fehleranfälligkeit menschlichen Denkens, Entscheidens und Handelns** entsteht:

Wirtschaftsnobelpreis für Richard Thaler: Abschied vom homo oeconomicus: Der Nachweis der Unvernunft

Richard Thaler bewies, dass der Mensch sowohl im Privat-, wie auch im Berufsleben eher unvernünftig agiert.

Dies zeigt sich auch daran, dass lediglich der Erlass immer neuer Regelungen nicht mehr (Rechts-) Sicherheit bringt. Regelungen (und sonstige – ausufernde – Bürokratie) gibt es meist schon ausreichend.

„Je verdorbener der Staat, desto mehr Gesetze hat er."

(Tacitus, 58 - 120, römischer Historiker und Senator, Annalen III, 27)

Technischer Fortschritt in Kombination mit menschlichen Fehleranfälligkeiten: Compliance-Verstöße und Risiken / Problemfälle haben meist mit Menschen zu tun!

Die (wahren) Probleme entstehen, weil Regeln häufig eben nicht gekannt und / oder befolgt werden.

Begriffe wie „Datenschutz“ oder „(technische oder Informations-) Sicherheit“ sind aus diesem Grunde nur relativ.

Die **Kunst** bestünde daher **für die Geschäftsleitung** in der Fähigkeit, die **Menschen** (sich selbst und das Personal) **ausreichend zu vernünftigem Handeln zu motivieren.** Dafür seien nach oben genannter Theorie aber „nudges“ – kleine Stupse – nötig, um den inneren Schweinehund zu überwinden, der uns das vernünftige Handeln stets ausreden will.

„Homo rationalis“ durch Human Workflow Management

Der Mensch und Mitarbeiter, der gerade eben wegen menschlicher Schwächen auch nicht stets alles weiß und fehleranfällig ist, würde bei standardisierten, (teil-) automatisierten und workflow-geführten Abläufen **Fehler nur noch** machen können, **wenn er bewusst die Prozessvorgaben technisch überwindet** und auch Kontrollen in arglistiger Weise ausschaltet.

Zusammenhang zwischen Governance und Vernunft: Idealerweise deckt sich pflichtgemäßes und risikobewusstes Verhalten mit „vernünftigem Verhalten“

So, wie ein Bauarbeiter heutzutage von selbst und freiwillig Schutzkleidung (Helm / Sicherheitsschuhe / etc.) trägt und auf Alkohol auf der Baustelle verzichtet.

Oder ein Autofahrer sich angurtet.

Oder vor der Vergabe von Aufträgen die Vertragspartner (Lieferanten) „gecheckt“ werden in Hinblick auf Compliance, Qualität, Risiko, Nachhaltigkeit, etc. ….

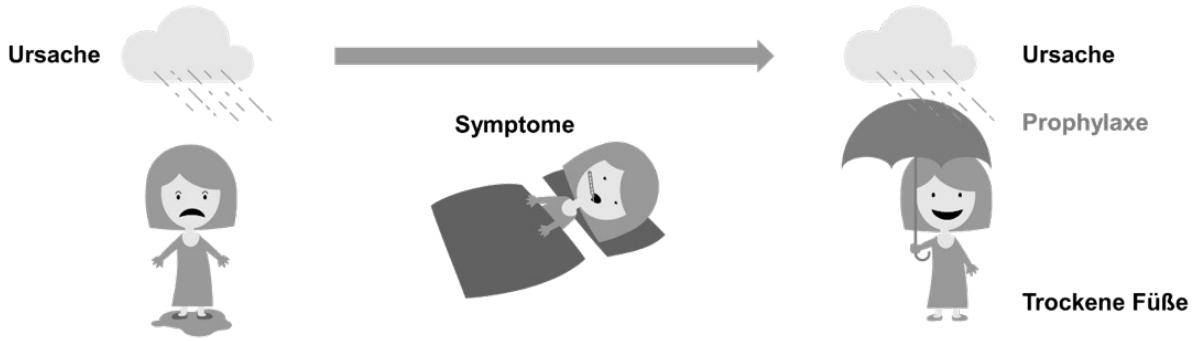
Oder vor dem Start größerer Projekte deren Risiken fachmännisch und systematisch bewertet werden und erst dann auf Basis dieser Informationen über die Durchführung entschieden wird.

Das war – zum Teil – früher anders!

Die letzten Jahre hat sich da viel verändert! Fallen Ihnen weitere (positive?) Beispiele ein?

Systemische Probleme erkennen und beheben!

In vielen Unternehmen werden enorme **Ressourcen (Zeit / Geld / Nerven) verschwendet, um lediglich Symptome (Problemfälle) zu kurieren**. **Es ist sinnvoller, rechtzeitig in Prophylaxe zu investieren.**



Das „Neue" an Governance, Risiko- und Compliancemanagement (GRC) ist, dass nicht – wie früher üblich – nur gelöscht wird, wenn es brennt und dann (reaktiv!) gewartet wird, bis es wieder brennt.

GRC kümmert sich gleich nach dem Brand um Brandschutz, damit es nicht nochmal brennt. Oder noch viel besser: Gleich, bevor es überhaupt brennt, sorgt es prophylaktisch für Brandschutz. Und:

Ein funktionierendes „Brandschutzsystem" (der Nachweis, dass gesetzliche, behördliche und interested-parties (z. B. Kunden, Aufsichtsfunktionen, etc.) -Anforderungen erfüllt werden) **ist schließlich Voraussetzung für die Erlaubnis und die Fähigkeit, das Unternehmen zu betreiben!**

Digitalisierung, Nachhaltigkeit, Governance, Risk und Compliance heißt, den **Zugang zu Markt und Kunden und unternehmerische Tätigkeit an sich zu ermöglichen,** also resilient und zukunftsfähig zu sein**.**

2. BREAKING NEWS

„Gute Firma? Schlechte Firma?

Jetzt plant Brüssel das nächste Nachhaltigkeits-Label“

„Die sogenannte soziale Taxonomie soll analog zur grünen Variante Anlegern signalisieren, welche Unternehmen dem Gemeinwesen dienen und sich deshalb für die immer wichtiger werdenden Anlagen nach sozialen Standards eignen.“ […][3]

„Österreich klagt vor Europäischem Gerichtshof gegen Taxonomie

„Österreich hat eine Klage gegen Teile der sogenannten Taxonomie-Verordnung eingereicht. […]

Im Zuge der Verordnung hat die EU-Kommission Erdgas und Kernkraft als nachhaltige Wirtschaftstätigkeiten eingestuft.“[4]

B Erarbeiten Sie sich bitte diese Fälle über Internetrecherche.

3. TESTFRAGEN

[3] Vgl. WELT, Gute Firma? Schlechte Firma? Jetzt plant Brüssel das nächste Nachhaltigkeits-Label, aufrufbar unter: https://www.welt.de/wirtschaft/article236826273/Soziale-Taxonomie-Bruessel-plant-das-naechste-Nachhaltigkeits-Label.html, 11.02.2022 (zuletzt aufgerufen am 19.11.2022).
[4] Vgl. BMK Infothek, Österreich hat Klage gegen umstrittene Teile der EU-Taxonomie eingereicht, abrufbar unter: Österreich hat Klage gegen umstrittene Teile der EU-Taxonomie eingereicht – BMK INFOTHEK (zuletzt aufgerufen am 22.03.2023)

Testfrage 1

Frage: Was hat Nachhaltigkeit mit Bildung und Compliance zu tun?

☐ Relativ wenig. Wichtig ist künftig primär, vieles zu Umweltschutz zu kommunizieren, um zu zeigen, dass wir „gut“ sind.

☐ Compliance steckt den zwingenden Rahmen im ökonomischen, sozialen und ökologischen Bereich ab. Diese Anforderungen zu erfüllen ist Pflicht, der Rest ist „Kür“.

☐ Ohne Bildung aller Mitarbeitenden im Themenfeld ökonomische, soziale und ökologische Entwicklung werden Vorgaben/Prozesse zur Erfüllung von Nachhaltigkeitsanforderungen nicht gelebt werden / wirksam werden.

Testfrage 2

Frage: Was heißt ESGRC?

□ Enterprise Society’s German Risk Convention.

□ Ökonomische, soziale und ökologische risikobasierte und compliance-orientierte Unternehmensführung.

4. Was heißt nachhaltige Führung von Organisationen (ESGRC)?

Ökologische (Enviromental),

soziale (Social),

ökonomische (Governance)

risikobasierte (Risk),

compliancebasierte (Compliance)

Führung (Governance)

5. **Relevante Begriffe, die wir künftig kennen sollten:**

Taxonomie: Organisationen müssen transparent über ihre Geschäftsaktivitäten im Bereich ESG berichten.

Dekarbonisierung: Auch über den CO2-Fußabdruck der wirtschaftlichen Aktivitäten müssen Unternehmen berichten.

6. **Was bedeutet „Nachhaltigkeits- (ESGRC-) Compliance“?**

Beachtung der zwingenden Anforderungen in Bezug auf Nachhaltigkeit (ESGRC)

7. **ESGRC-Managementsystem**

Vgl. Scherer Compliance-Managementsystem nach DIN ISO 37301:2021 – erfolg-reich implementieren, integrieren, auditieren, zertifizieren / 2022,

Herausgeber: DIN, Verlag: Beuth

Regulatorische Aktivitäten zu Nachhaltigkeit gibt es auf globaler, europäischer und nationaler Ebene:

8. **Global: 17 Sustainable Development Goals der UN**

9. Europäische Nachhaltigkeitsregulierung:

Europa: **Accounting Directive**	**Corporate Sustainability Reporting Directive** **(CSRD)**	Erweiterung des Adressatenkreises und der Berichtsinhalte, verpflichtende Prüfung, maschinenlesbares Format, Verknüpfung mit Berichtsstandards	Unternehmen, Banken, Versicherungen ab 250 Mitarbeiter für Geschäftsjahr 2024?
	EU Sustainability Reporting Standards	Europäische Standards für die nichtfinanzielle Berichterstattung mit doppelter Materialität (Wesentlichkeit) als Grundlage	Unternehmen, Banken, Versicherungen ab 250 Mitarbeiter für Geschäftsjahr 2024?

10. Deutschland:

Alle verpflichtenden Anforderungen im Bereich Nachhaltigkeit (ESGRC):

z.B.: Deutsche Gesetze, Rechtsprechung, Standards usw.

z.B. Umweltstandards, Arbeitsrecht, Antikorruptionsgesetze, Lieferkettensorgfalts-pflichtengesetz (LKSG), u.v.m.

11. Jedes Thema aus Nachhaltigkeit (ESGRC) hat rechtliche (Compliance-) Anforderungen §§

Was ist **Pflicht** und was ist **Kür**?

Was ***muss*** ich in meinem Arbeitsumfeld beachten?

12. Auswirkungen auf meinen Arbeitsbereich?

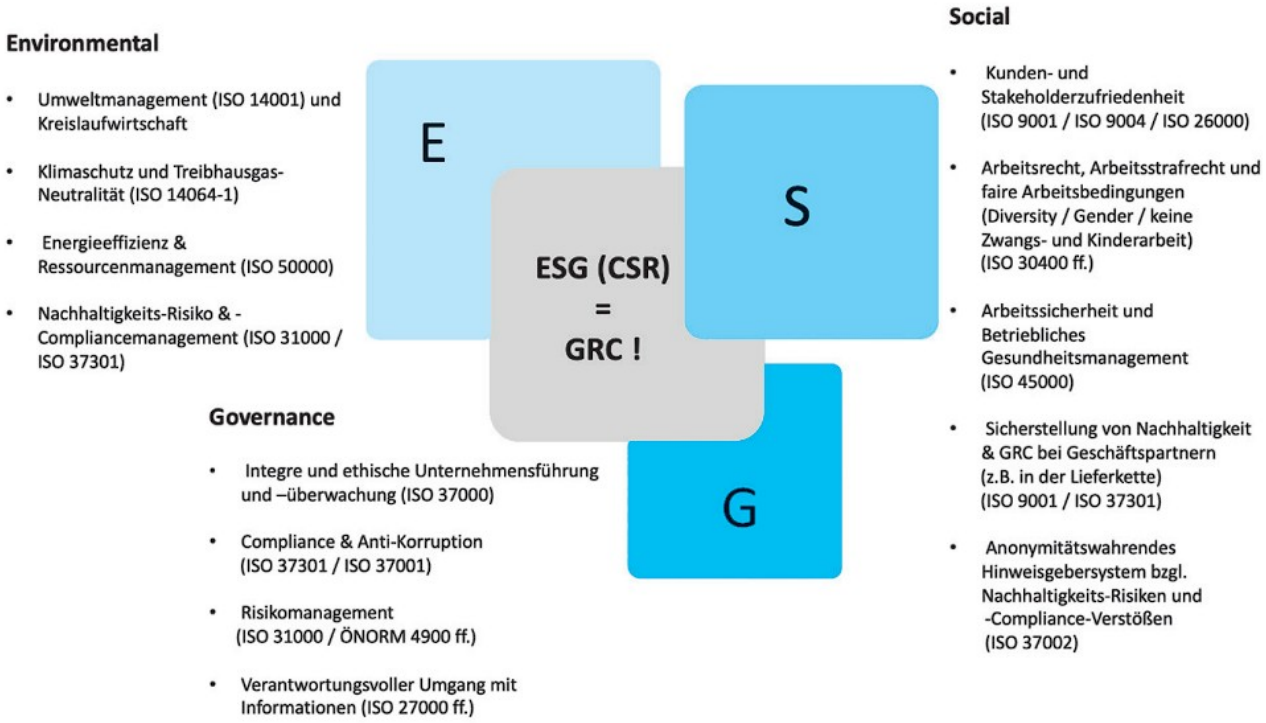
Beispiel: Berichtspflicht aus ESRS S1: “Arbeitsbedingungen der eigenen Mitarbeitenden”

13. Das Richtige richtig machen? - Spaghetti im Kopf?

Wir brauchen:

- Angemessene, smarte Ziele,
- Wissen
- Verstehen
- Können
- Wollen
- führende Prozesse
- und Steuerung.

14. Wir sollten zunächst die vielen Redundanzen auflösen…



15. ESGRC-Compliance

Zwingende Nachhaltigkeits-Compliance-Ziele erreichen wir nur mit Risikokompetenz und Bildung!

16. Diskussion

B

Können Sie die vielen Begriffe aus dem Bereich nachhaltige Führung von Organisationen (ESGRC) verstehen und erklären?

Ist (ESGRC) Pflicht?

Hat das Auswirkung auf Ihren Arbeitsbereich?

17. TESTANTWORTEN

Antwort zu Testfrage 1

Antwort: Was hat Nachhaltigkeit mit Bildung und Compliance zu tun?

☐ Relativ wenig. Wichtig ist künftig primär, vieles zu Umweltschutz zu kommunizieren, um zu zeigen, dass wir „gut“ sind.

☑ Compliance steckt den zwingenden Rahmen im ökonomischen, sozialen und ökologischen Bereich ab. Diese Anforderungen zu erfüllen ist Pflicht, der Rest ist „Kür“.

☑ Ohne Bildung aller Mitarbeitenden im Themenfeld ökonomische, soziale und ökologische Entwicklung werden Vorgaben/Prozesse zur Erfüllung von Nachhaltigkeitsanforderungen nicht gelebt werden / wirksam werden.

Antwort zu Testfrage 2

Antwort: Was heißt ESGRC?

□ Enterprise Society’s German Risk Convention.

☑ Ökonomische, soziale und ökologische risikobasierte und compliance-orientierte Unternehmensführung.

18. Hausaufgabe

Lesen Sie bitte einen Nachhaltigkeitsbericht Ihrer oder einer branchengleichen Organisation und suchen Sie dort nach dem gerade behandelten Thema.

Beispiel: Auszug aus Nachhaltigkeitsbericht

Strabag SE 2022, zum Download auf https://www.strabag.com/databases/internet/_public/files.nsf/SearchView/EAF44042C93D77E8C12589C600465FCD/$File/STRABAG%20SE_Geschaeftsbericht_2022_DE.pdf

*„Das **Sustainability Management** ist im Zentralbereich STRABAG Innovation & Digitalisation (SID) im Verantwortungsbereich von CEO Klemens Haselsteiner angesiedelt und verantwortet das **konzernweite Nachhaltigkeitsmanagement**. Die Aufgaben reichen von der Erarbeitung und Weiterentwicklung der **Nachhaltigkeitsstrategie** über die **Steuerung (Governance) von Nachhaltigkeit** bis hin zur **nichtfinanziellen Berichterstattung** im Einklang mit den **gesetzlichen Erfordernissen**. Eine der Kernaufgaben ist die **Datenerhebung und -berichterstattung** sowie deren **Analyse**. Der Bereich zeichnet verantwortlich für die Initiierung und Durchführung von konzernweiten Nachhaltigkeitsprojekten, z. B. in den Themenfeldern Kreislaufwirtschaft, Dekarbonisierung von Baustoffen oder Nachhaltigkeit in der Lieferkette. Das Nachhaltigkeitsmanagement der STRABAG SE richtet sich nach **weltweit anerkannten Regel- und Rahmenwerken** wie der **Global Reporting Initiative**, den **Sustainable Development Goals** (SDG) und den Prinzipien des **UN Global Compact**. Es beruht auf einem **Drei-Säulen-Modell** aus **Ökonomie, Ökologie und Sozialem**. Im Zentrum des Nachhaltigkeitsmanagements steht die **Wesentlichkeitsanalyse**, wobei die Anforderungen von GRI an die Wesentlichkeitsanalyse gegenüber dem Vorjahresberichtszeitraum deutlich zunahmen. Die neue Methodik beinhaltet nun zusätzlich Angaben über das **Ausmaß**, die **Tragweite** und **die Behebbarkeit** der **Auswirkungen** eines Themas auf die **Umwelt**, auf **Menschen** und auf die **Wirtschaft**."*

(Strabag SE Geschäftsbericht 2022, S. 69)

E.ON 2022, zum Download auf https://www.eon.com/de/investor-relations/finanz-publikationen/geschaeftsbericht.html

*„Gute **Corporate Governance** ist im E.ON-Konzern die zentrale Grundlage für eine **verantwortungsvolle** und **wertorientierte Unternehmensführung**, die effiziente*

*Zusammenarbeit von Vorstand und Aufsichtsrat, Transparenz in der Berichterstattung sowie ein **angemessenes Risikomanagement**. (…)*

*Das **Ziel** von Compliance bei E.ON ist es, **Unternehmenskriminalität** zu **verhindern** oder jedenfalls **aufzudecken** und **abzustellen**. Kunden, Geschäftspartner und andere Stakeholder sollen niemals getäuscht, betrogen oder anderweitig geschädigt werden. Die strikte **Einhaltung von Gesetzen und Unternehmensrichtlinien** wird folglich als unerlässliche Grundlage einer guten Corporate Governance verstanden. Der E.ON-Konzern hat hierfür ein **Compliance-Management-System** (CMS) implementiert. Das CMS basiert auf einer Reihe von allgemein anerkannten Praktiken, darunter der Förderung einer Compliance-Kultur. Diese umfasst ein aktives **Bekenntnis zu Compliance-Zielen**, die **Identifizierung und Analyse von Compliance-Risiken**, die Gestaltung eines **risikoadäquaten Compliance-Programms** sowie einer **Compliance-Organisation**. (…)*

***Nachhaltigkeit** ist einer der Grundpfeiler der in 2021 überarbeiteten E.ON Strategie. E.ONs Geschäftstätigkeit richtet sich nach dem Grundsatz, dass unternehmerischer Erfolg nur durch eine konsequente Ausrichtung auf **verantwortungsvolles**, **nachhaltiges Wirtschaften** und **langfristigen Mehrwert** für alle Beteiligten erreichbar ist: für Kunden, Mitarbeiter, Aktionäre, Geschäftspartner - und auch die Umwelt. E.ON **verpflichtet sich zu nachhaltigem Handeln** und der Berücksichtigung von kurz- und langfristigen Auswirkungen auf materielle und immaterielle Ressourcen und Interessensgruppen in allen Geschäftsentscheidungen."*

(E.ON Integrierter Geschäftsbericht 2022, S.146 f.)

Technische Universität Darmstadt 2022, online verfügbar unter https://www.tu-darmstadt.de/nachhaltigkeit/nachhaltigkeits_kompass/index.de.jsp:

*„Durch die Implementierung von **Standards und Prozessen** sowie durch Maßnahmen zur **Vermeidung** von **rechtswidrigem Verhalten** und **Korruption**, wird ein **gesetzes- und richtlinienkonformes Verhalten** gefördert und ein verantwortungsvoller Umgang mit hochschulrelevanten Themen gewährleistet."*

(TU Darmstadt 2022 digitaler Nachhaltigkeits-Kompass)

*„Die Benennung von **Regeln und Prozessen** innerhalb der Organisation fördert die Entwicklung einer **Organisationskultur und -struktur**, sowie **Handlungsroutinen** im Sinne des Nachhaltigkeitsleitbildes. Außerdem tragen sie zu einer **transparenten Vorgehensweise** bei und ermöglichen so Partizipation. Räume für einen kontinuierlichen Lern- und Entwicklungsprozess innerhalb der Universität sind wesentlich, um die **Regeln und Prozesse** stetig **weiterzuentwickeln** und **anzupassen.**"*

(TU Darmstadt 2022, digitaler Nachhaltigkeits-Kompass)

19. BULLETPOINTS

1. Es gibt zahlreiche regulatorische Aktivitäten bzgl. Nachhaltigkeit und ESGRC auf Globaler, Europäischer und Nationaler Ebene.

---

2. Dabei gibt es viele Überschneidungen...
   Und viele offene Fragen…

---

3. Er ist unverzichtbar, Mitarbeiter*Innen zunächst in den Basics zu Nachhaltigkeits-Schlüsselqualifikationen zu bilden, um ein „Gelebt-werden“ zu ermöglichen.

---

4. Nachhaltigkeit (ESGRC) hat Auswirkungen auf **jeden** Arbeitsbereich.

Bitte erarbeiten Sie sich folgende Quellen und weiterführende Literatur:

20. QUELLEN

WELT, Gute Firma? Schlechte Firma? Jetzt plant Brüssel das nächste Nachhaltigkeits-Label, aufrufbar unter: https://www.welt.de/wirtschaft/article236826273/Soziale-Taxonomie-Bruessel-plant-das-naechste-Nachhaltigkeits-Label.html, 11.02.2022 (zuletzt aufgerufen am 19.11.2022).

BMK Infothek, Österreich hat Klage gegen umstrittene Teile der EU-Taxonomie eingereicht, abrufbar unter: Österreich hat Klage gegen umstrittene Teile der EU-Taxonomie eingereicht – BMK INFOTHEK (zuletzt aufgerufen am 19.11.2022)

CSR-Berichtspflicht, Nachhaltigkeit betrifft alle - auf unterschiedliche Weise, abrufbar unter: https://www.csr-berichtspflicht.de/eu-roadmap (zuletzt abgerufen: 19.11.2022)

17 Sustainable Development Goals“ (deutsch). Entnommen aus: *https://www.bundesregierung.de/bregde/themen/nachhaltigkeitspolitik/nachhaltigkeitszieleverstaendlich-erklaert-232174 (zuletzt abgerufen: 19.11.2022)*

21. WEITERFÜHRENDE LITERATUR

Scherer, Compliance-Managementsystem nach DIN ISO 37301:2021 erfolgreich implementieren, integrieren, auditieren, zertifizieren, Herausgeber: DIN Beuth – Verlag 2022, Kapitel Einleitung

Scherer/Fruth/Grötsch (Hrsg.), Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0“ (GRC) mit Digitalisiertem Integrierten GRC-Managementsystem, 2021, mit e-Book, Einleitung

Scherer / Grötsch, Nimby: Frieden und Klimaschutz: Unverzichtbare Voraussetzungen für Nachhaltigkeit (ESG) und Überleben, Zum kostenlosen Download auf Scherer-GRC.net/Publikationen

Scherer / Grötsch / Romeike, Forschungsbedarf bei Nachhaltigkeit (CSR / ESG), Governance und Digitalisierung / KI, Zum kostenlosen Download auf Scherer-GRC.net/Publikationen