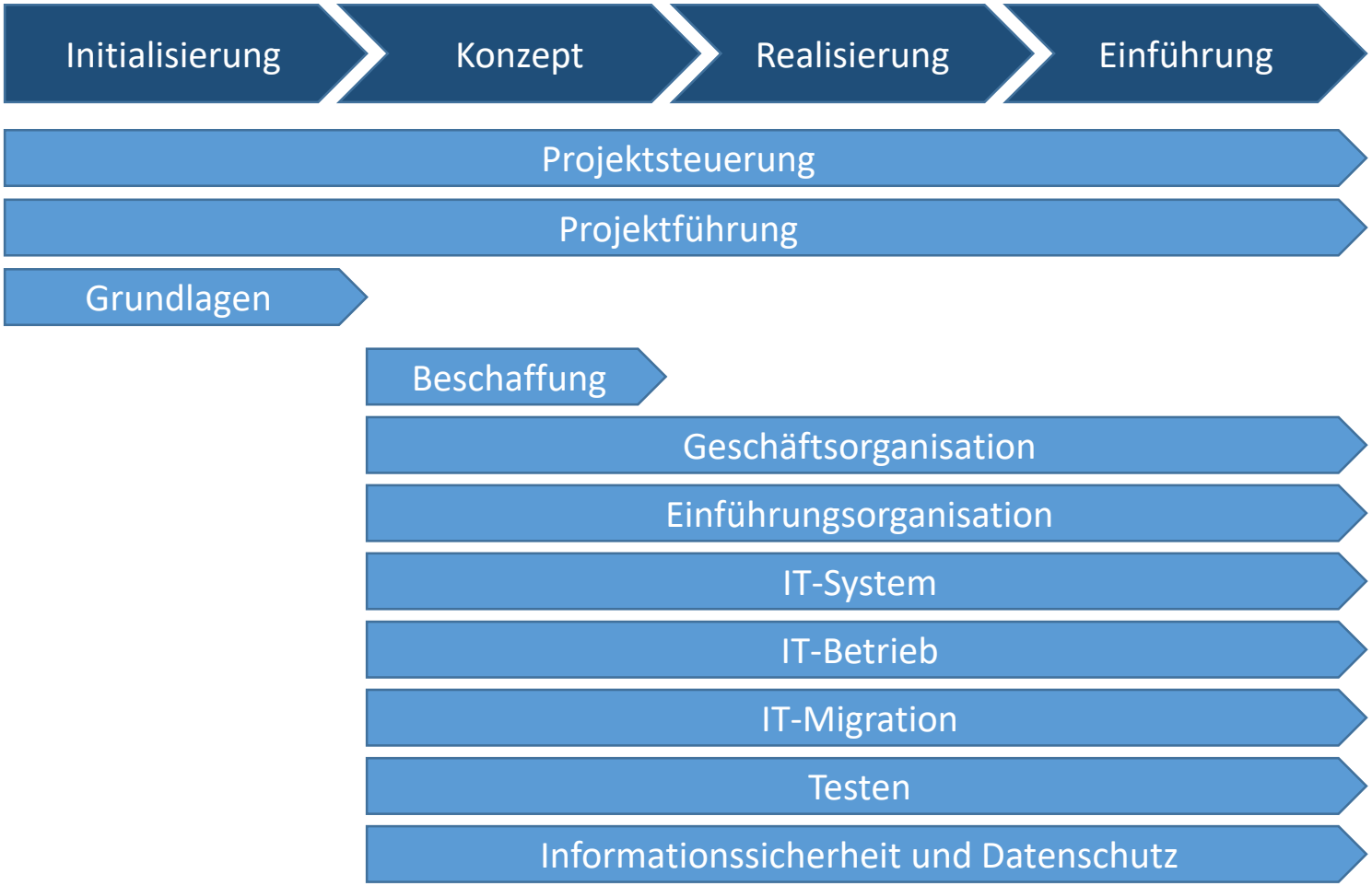
EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Schutz digitalisierter Assets in Projekten

Netzwerk Risikomanagement, Jahrestagung 23.06.2022

Bernhard Hamberger,
Leiter Fachbereich Informatikprüfungen, Eidg. Finanzkontrolle

Sichere Assets durch - oder trotz - Projekte?

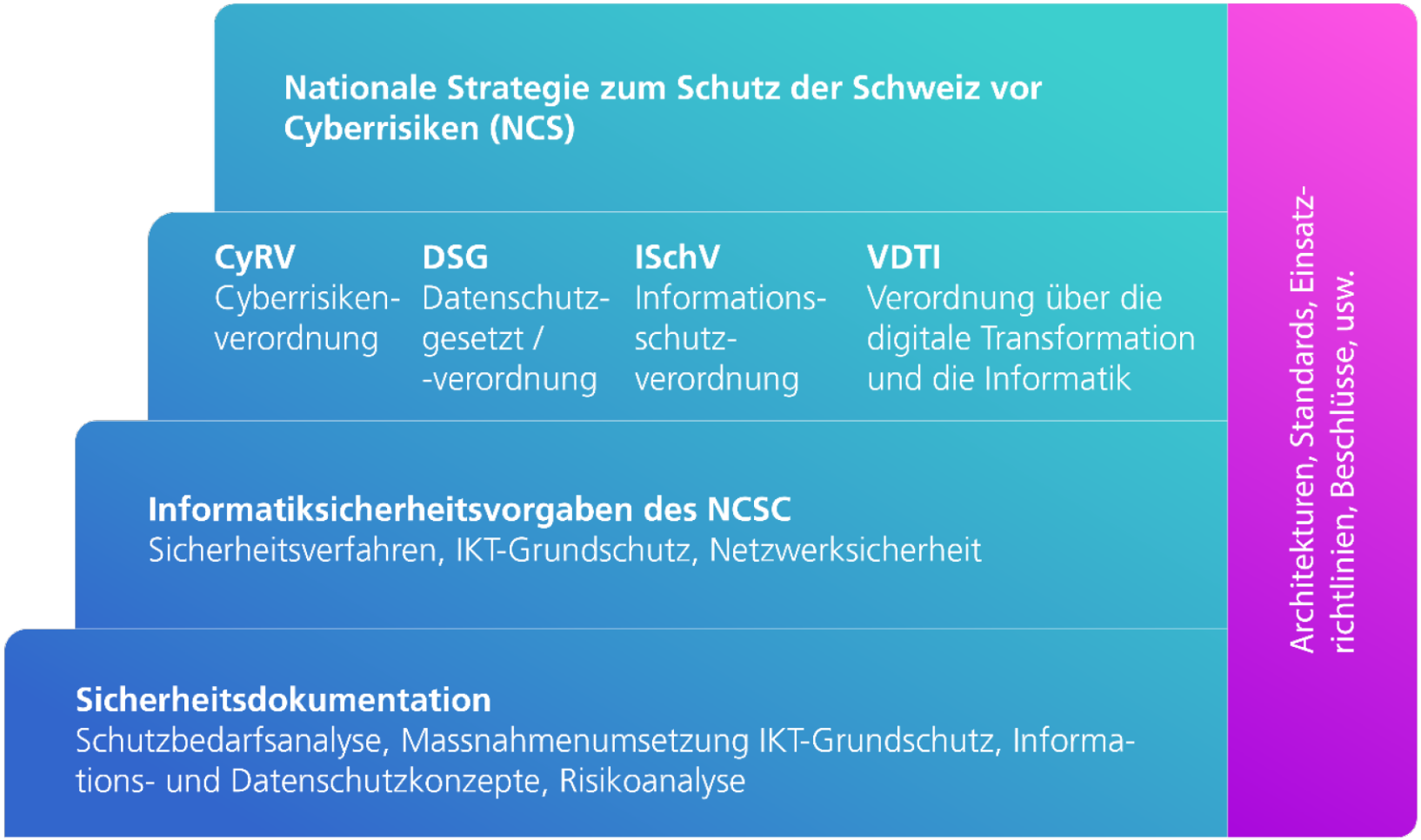


https://www.hermes.admin.ch/

Agenda

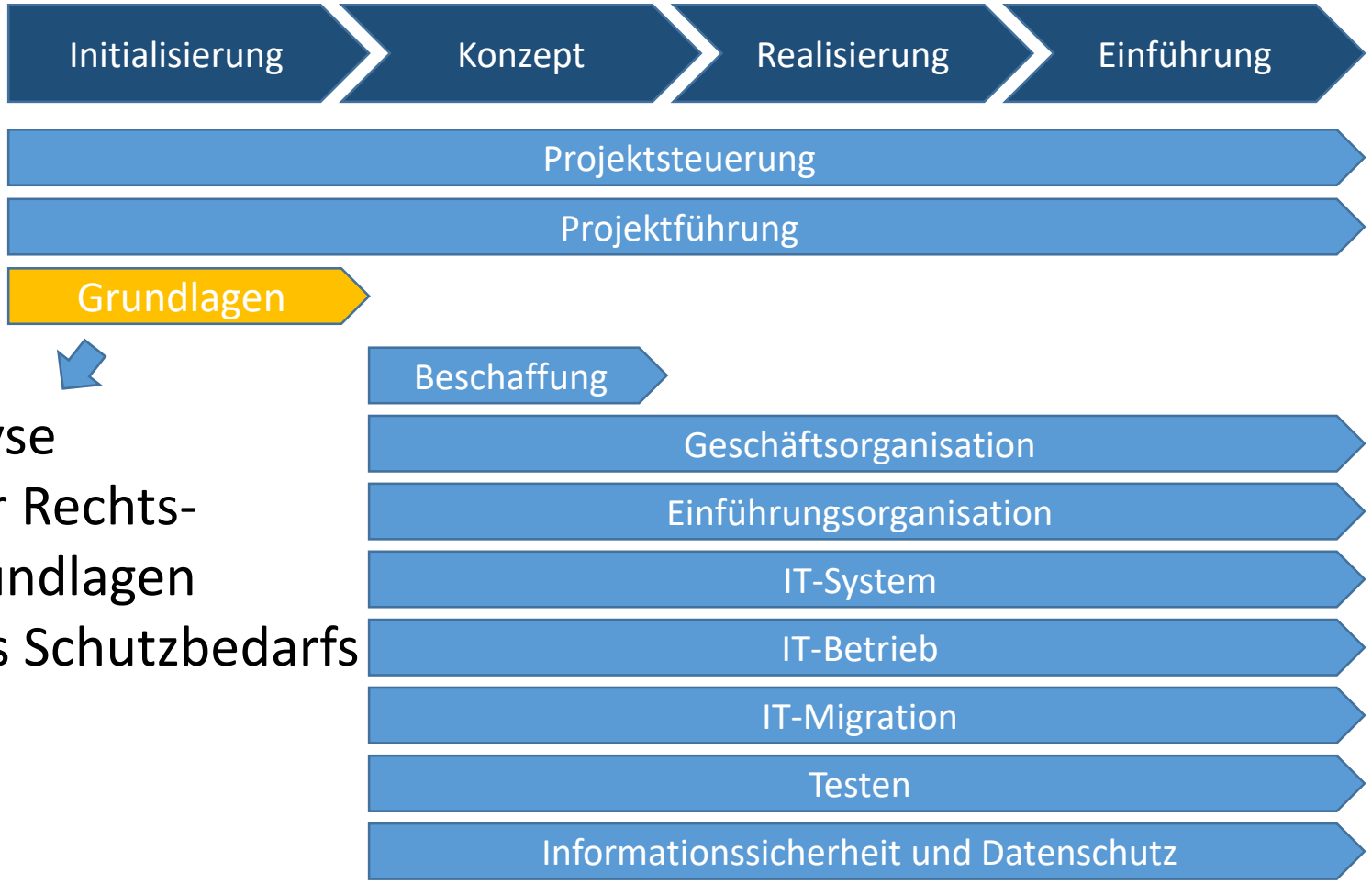
- Informationssicherheitsverfahren der Bundesverwaltung
- Herausforderungen moderner Software-Entwicklung
- Risiken bei der Digitalisierung
- Systematisches IT Risk Management

Informatiksicherheitsgrundlagen Bund



https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund.html

Schutzbedarf erkennen…



Analyse

- der Rechts-grundlagen
- des Schutzbedarfs

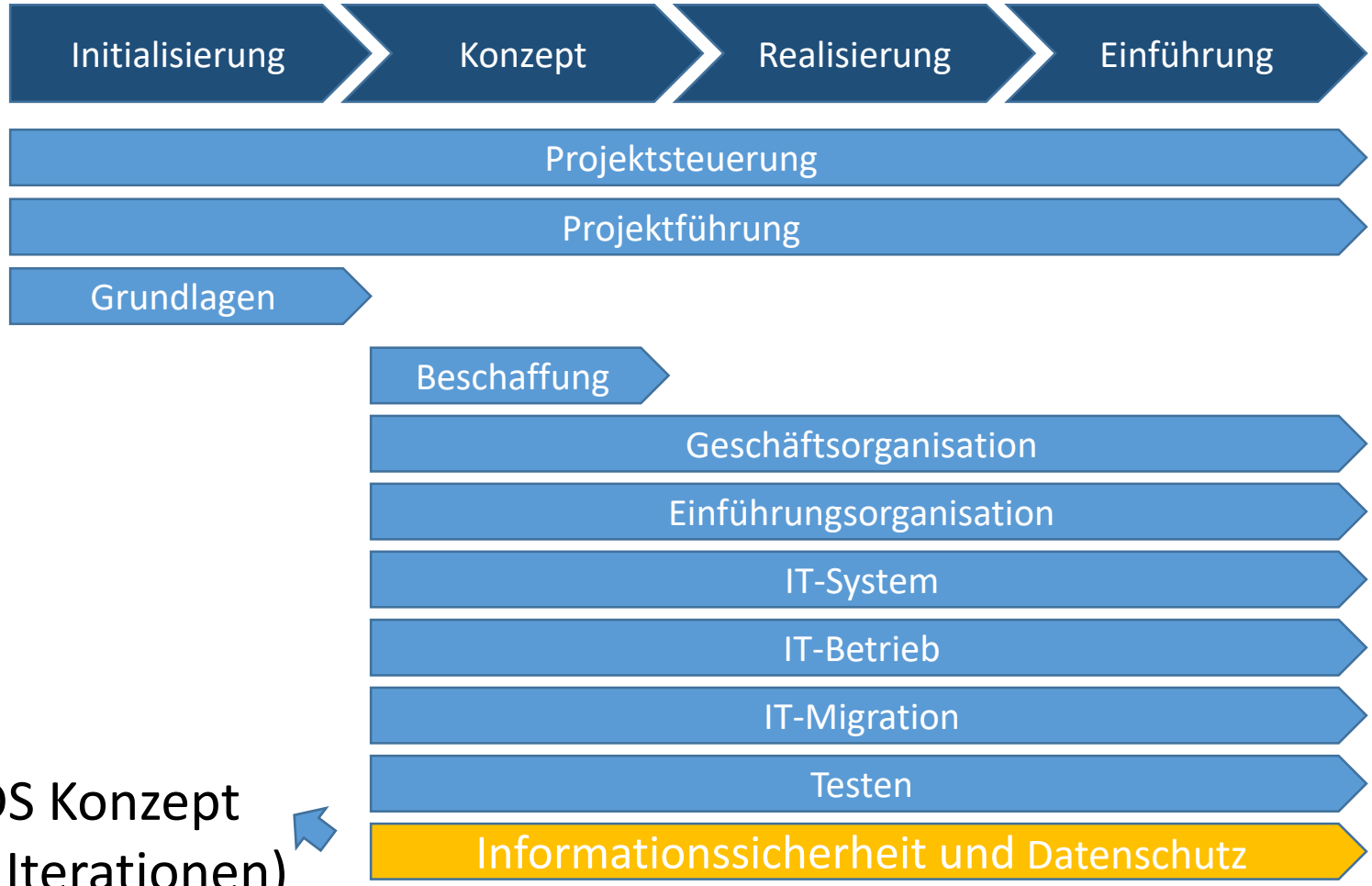
Am Anfang war die «SCHUBAN»…

Ergebnis der Einstufung	
Vertraulichkeit:	*Keine Personendaten*
	Nicht klassifiziert
	Keine erhöhten Anforderungen an die Vertraulichkeit
Verfügbarkeit:	*Ausfalldauer grösser 12 Std.*
	Servicezeiten Standard (11/5)
	ITSCM / BCM nicht notwendig
Integrität:	*Keine speziellen Anforderungen*
Nachvollziehbarkeit:	*Keine speziellen Anforderungen*
RINA-Relevanz:	*Nein - Nicht RINA-relevant*

- Schutzbedarfsanalyse
  - Anforderungen an die Sicherheit der Informatikschutzobjekte
  - durch Informatiksicherheitsbeauftragten zu prüfen
  - Genehmigung Auftraggeber(in) und Geschäftsprozessverantwortliche(r)
- Zu beurteilen:
  - Vertraulichkeit, Verfügbarkeit, Integrität, Nachvollziehbarkeit, Nachrichtendienstliche Relevanz
- Resultat: Grundschutz oder erhöhte Anforderungen

Gretchenfrage: Daten als Digitalisierungstreiber versus Datensparsamkeit?

…konkretisieren und umsetzen



ISDS Konzept
(in Iterationen)

https://pixabay.com/

Grundschutz

- Erlassen durch den Delegierten für Cybersicherheit
- Legt die minimalen organisatorischen, personellen und technischen Anforderungen an die Informatiksicherheit der Bundesverwaltung bzw. deren Informatikschutzobjekte (Schutzobjekte) fest.
- Genehmigung durch
  - Schutzobjektverantwortliche(r)
  - Informatiksicherheitsbeauftragte(r) der verantwortlichen Verwaltungseinheit
  - Auftraggeber(in)
  - Geschäftsprozessverantwortlichen
- 64 konkrete Anforderungen zu Organisation, Personal, Technik, Informationen (Daten), Systeme, Entwicklung und Wartung, Netzwerkzonen
- Die Umsetzung muss dokumentiert und überprüft werden

ISDS Konzept – erhöhter Schutz

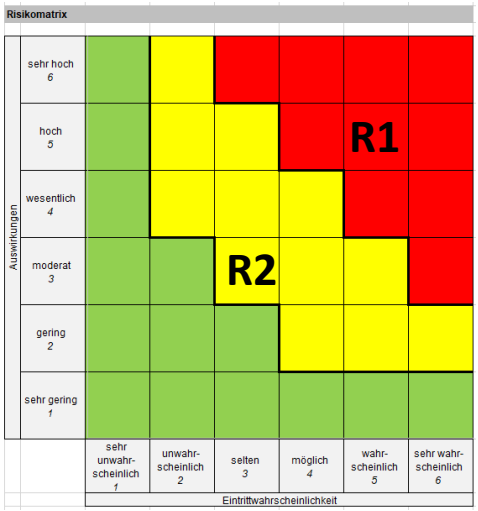
- Bei ausgewiesenem, erhöhtem Schutzbedarf ist ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) zu erarbeiten.
- Umsetzung der Sicherheitsvorgaben für den Grundschutz
- Weitere Sicherheitsmassnahmen, basierend auf einer Risikoanalyse, spezifisch für das *Projekt* oder *Informatikschutzobjekt*

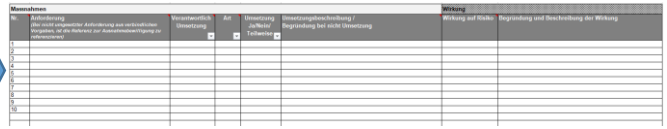
- Gretchenfrage:
  Wieviel Grundschutz wollen wir uns leiste
  Oder eher Fokus auf die Kronjuwelen.

https://pixabay.com/

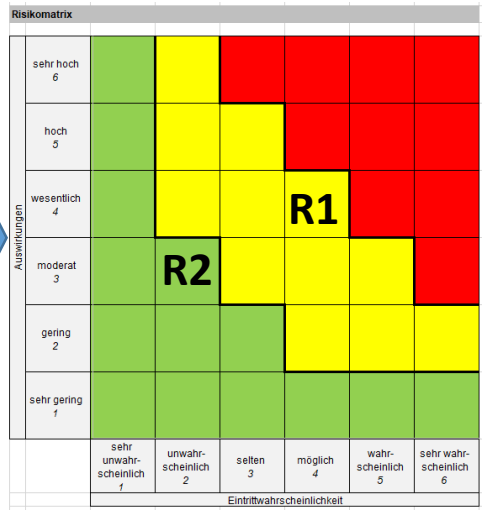
Risikoanalyse

	Risiko	Szenario	Eintrittswahrscheinlichkeit 1- 6	Vertraulichkeit (Vt)		Verfügbarkeit (Vf)		Integrität (I)		Nachvollziehbarkeit (N)		Risikobewertung max(Vt, Vf, I, N)
				Auswirkungen 1 - 6	Risikobewertung R=E*A	Auswirkungen 1 - 6	Risikobewertung R=E*A	Auswirkungen 1 - 6	Risikobewertung R=E*A	Auswirkungen 1 - 6	Risikobewertung R=E*A	
R1	Feuer, Wasser, Naturkatastrophen, Verschmutzung, Staub, Korrosion				0		0		0		0	0
R2	Ausfall oder Störung der Stromversorgung oder von Kommunikationsnetzen				0		0		0		0	0
R3	Ausfall oder Störung von Dienstleistern				0		0		0		0	0
R4	Ausspähen von Informationen, Spionage, Abhören				0		0		0		0	0
R5	Diebstahl oder Verlust von Geräten, Datenträgern oder Dokumenten				0		0		0		0	0
R6	Fehlplanung oder fehlende Anpassung, Ressourcenmangel				0		0		0		0	0
R7	Manipulation von Informationen, Hard- oder Software				0		0		0		0	0
R8	Zerstörung, Ausfall oder Fehlfunktion von Geräten oder Systemen				0		0		0		0	0
R9	Softwareschwachstelle oder -Fehler				0		0		0		0	0
R10	Verstoss gegen Vorschriften oder Regelungen				0		0		0		0	0
R11	Unberechtigte oder fehlerhafte Nutzung oder Administration von Geräten und Systemen, Missbrauch von Berechtigungen				0		0		0		0	0
R12	Personalausfall				0		0		0		0	0
R13	Missbrauch personenbezogener Daten				0		0		0		0	0
R14	Verhinderung von Diensten (Denial of Service), Sabotage				0		0		0		0	0
R15	Unbefugtes Eindringen in Räumlichkeiten				0		0		0		0	0
R16	Datenverlust				0		0		0		0	0





Massnahmen



Bruttorisiko

Risikoakzeptanz

Nettorisiko

Gretchenfrage: Risikoappetit

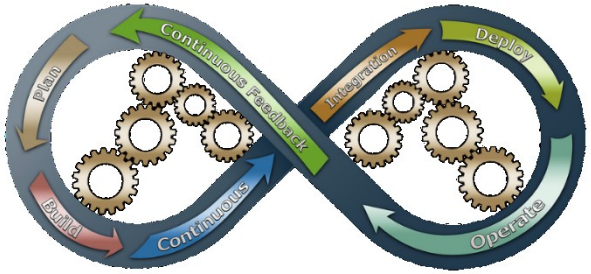
EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Aber was muss ich eigentlich schützen?

- Informatikschutzobjekte: Anwendungen, Services, Systeme, Netzwerke, Datensammlungen, Infrastrukturen und Produkte der Informatik; mehrere gleiche oder zusammenhängende Objekte können zu einem Informatikschutzobjekt zusammengefasst werden;
- Projekte, Systeme oder doch eher Daten?
- Trend: Orientierung an den Datensammlungen
- IT Dienste sind modular aufgebaut: Basisinfrastruktur, Standardisierte Leistungen, Fachspezifische Anwendungen….

- Gretchenfrage: Wer kennt alle (akzeptierten) Restrisiken?

Herausforderungen moderner SW Entwicklung



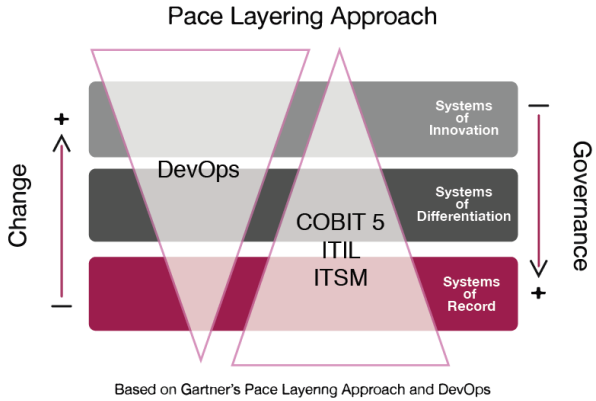
- Klassische Projekte verlagern sich in den Unterhalt
- Kontinuierliche Releases (z.B. monatlich)
- Management von Abhängigkeiten (SW-Libraries)
- «Vernetzte» Entwickler (Intellectual Property, Secu
- Entwicklung und Betrieb rücken zusammen
- Resultate gehen schnell in den Betrieb
- Systeme müssen sich rasch anpassen können
- Risikomanagement muss den konstanten Wandel meistern
- Der Fokus der Risiko-Verantwortlichen muss auf die Veränderungs-prozesse gerichtet werden und nicht auf den aktuellen Status
- Nicht perfekt, sondern brauchbar ist das Ziel
- Grosse Risiken bei der Umstellung vom Wasserfall auf DevOps

DevOps vs. DevOps

Praxiserfahrungen in der Bundesverwaltung und Lösungsansätze

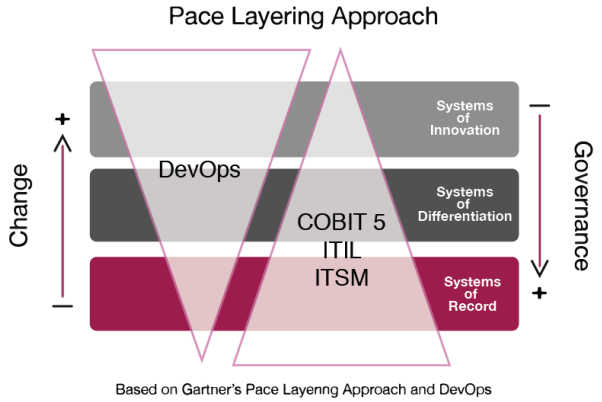
- Agile Entwicklung trifft heute noch auf “Wasserfall” basierte Compliance Systeme
- Systeme verändern sich rasch – die Kontrollen damit potentiell auch
- Go-Live mit MVP’s (minimum viable product)
- Querschnittsthemen wie Architektur, Sicherheit, IKS, BCM werden vernachlässigt
- SW-Abhängigkeitsmanagement als grosse Herausforderung (log4j)

Lösungsansätze
Compliance by Design I



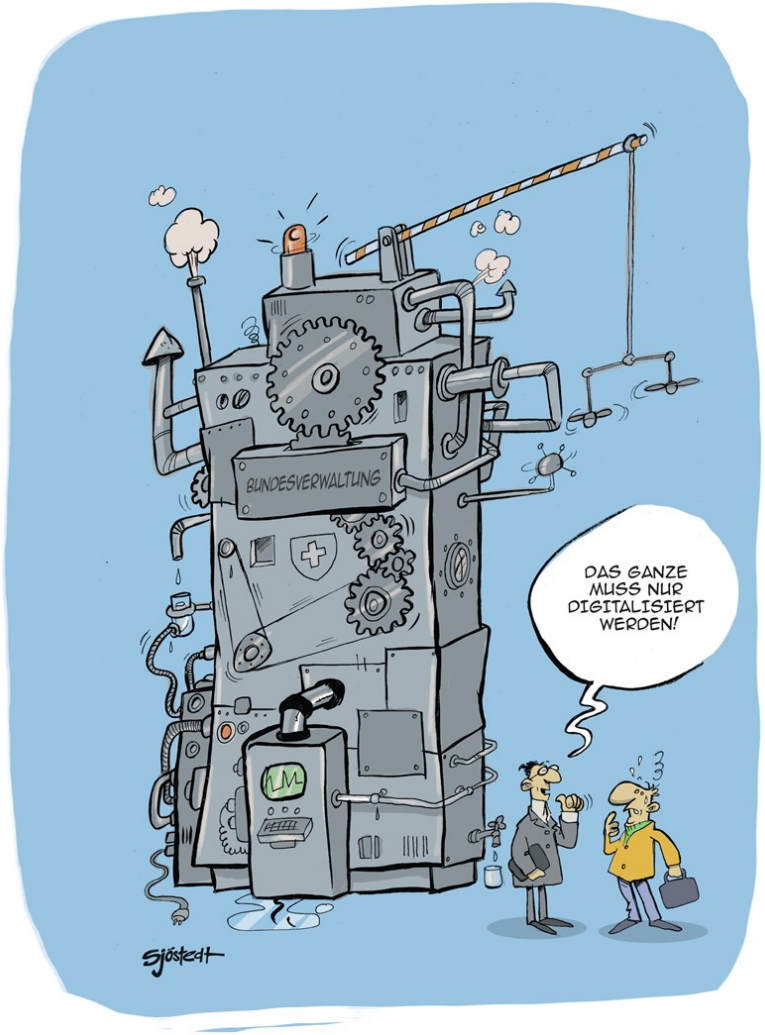
- Die Kontrollen müssen im Lösungs-Ansatz integriert sein
- Auch “selbstverständliche Anforderungen” müssen ausformuliert werden (explizit gemacht)
- Was nicht ins “Backlog” gelangt wird nie realisiert – alles was der Verantwortliche später sehen will, muss er als Anforderung einbringen
- Autotesting verhindert «Erosion» von Kontrollfunktionalität
- Verstärkte Präsenz von Vertretern von Querschnittsthemen

Lösungsansätze
Compliance by Design II



- Verwenden von (zertifizierten) architectural building blocks bringt Stabilität
- Software Bill-of-Materials
- Kontrollen dort, wo sie die längste Lebensdauer haben – Backbone vs. App
- Monitoring und Datenanalyse als Frühwarnsystem und für Nachvollziehbarkeit (nahe an den Daten bleiben, schafft Unabhängigkeit von Entwicklungen)

Wenn wir jetzt einen Schritt zurückgehen…



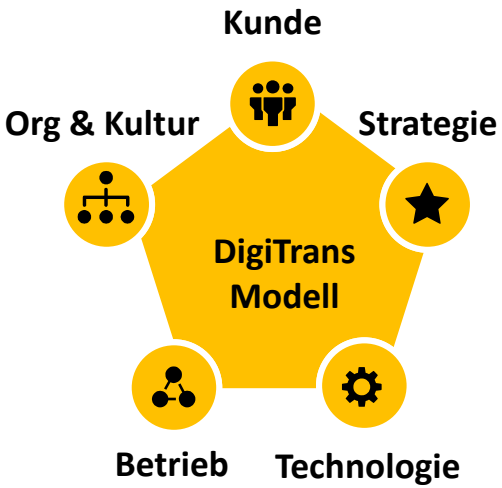
…dann sprechen wir von den Chancen und Risiken der Digitalen Transformation

Eine digitale Transformation bezeichnet einen fortlaufenden, durch digitale Technologien oder darauf beruhenden Kundenerwartungen ausgelösten Veränderungsprozess in Organisationen, Verwaltungseinheiten oder Unternehmen, der mittels Digitalisierungsvorhaben unterstützt wird.

«DigiTrans» Prüfungen der EFK - Prüffragen

1. Wird das Effizienzsteigerungspotenzial der Digitalen Transformation ausgeschöpft?
2. Werden neue potentielle Kunden, Partner, Produkte und Dienstleistungen adäquat berücksichtigt?
3. Wird die Digitale Transformation adäquat in eine Gesamtarchitektur eingebettet, gesteuert und geführt?
4. Ermöglichen die bestehenden Rahmenbedingungen (z. B. Gesetze, Technologie) die zeitgerechte und flexible Umsetzung und eine durchgängige Digitalisierung?

Grundlage zur Beantwortung der Prüffragen ist das DigiTrans Modell EFK mit fünf Dimensionen



Kunde

Betrachtung der Kunden- und Stakeholder Bedürfnisse sowie der existierenden Druckpunkte.

Strategie

Betrachtung der Art und Weise, wie die Organisation transformiert werden soll, um Wirkung und Effizienz zu erhöhen.

Technologie

Betrachtung der Art und Weise, wie Daten generiert, verarbeitet, gesichert und ausgetauscht werden, um die Bedürfnisse der Kunden zu geringen variablen und fixen Kosten zu adressieren.

Betrieb

Betrachtung von Prozessen und Governance im Hinblick auf den Einsatz digitaler Technologien, um die Effizienz und Effektivität zu verbessern.

Org & Kultur

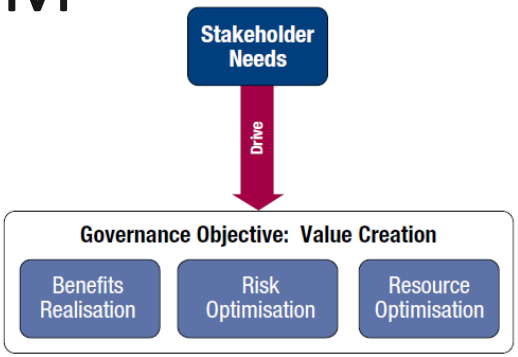
Betrachtung der Organisation und Kultur im Hinblick auf Governance- und Talentprozesse zur Unterstützung des Fortschritts.

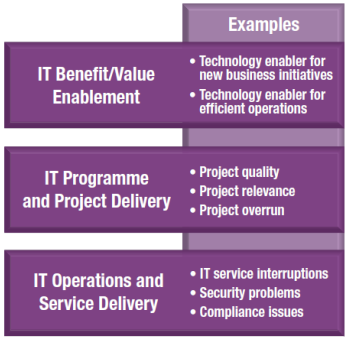
Die Hauptrisiken in 19 Kriterien

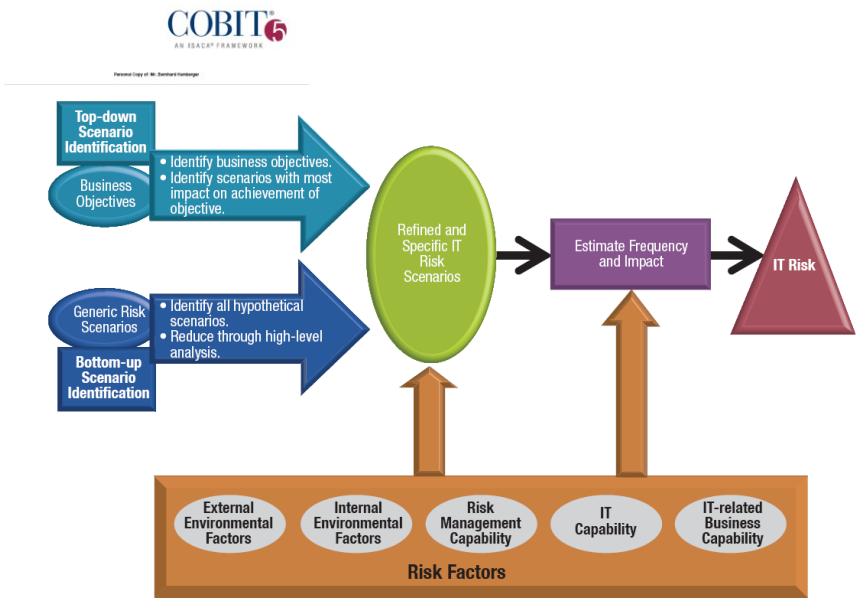
*Kunden umfassen sowohl interne als auch externe Partner und Stakeholder

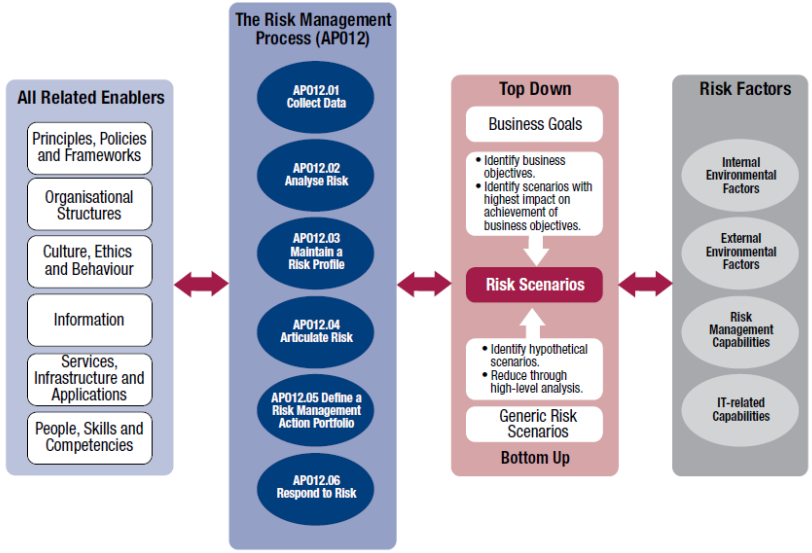
Quelle: https://www.efk.admin.ch/de/publikationen/allgemeine-kommunikation/fachtexte/4377-digitale-transformation-digitalisierungsvorhaben-und-pruefziel.html

CobiT 5 for Risk schliesst die Lücke zwischen ISMS und ERM



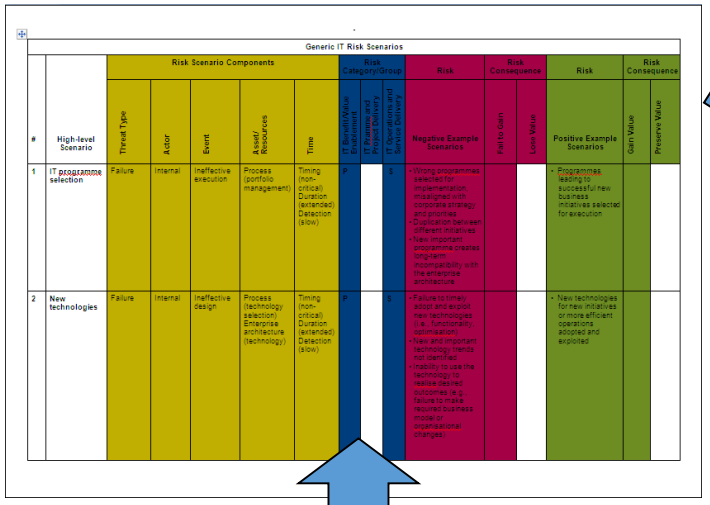






Anwendungsbeispiel

Risk Scenarios



Generic IT Risk Scenarios

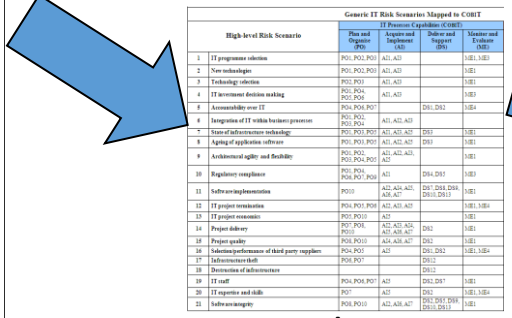
#	High-level Scenario	Risk Scenario Components: Threat Type	Actor	Event	Asset/ Resources	Time	Risk Category/Group: IT Benefit/Value Enablement	IT Programmes and Projects Delivery	IT Operations and Service Delivery	Risk: Negative Example Scenarios	Risk Consequence: Fail to Gain	Loss Value	Risk: Positive Example Scenarios	Risk Consequence: Gain Value	Preserve Value
1	IT programme selection	Failure	Internal	Ineffective execution	Process (portfolio management)	Timing (non-critical) Duration (extended) Detection (slow)	P		S	• Wrong programmes selected for implementation, misaligned with corporate strategy and priorities • Duplication between different initiatives • New important programme creates long-term incompatibility with the enterprise architecture			• Programmes leading to successful new business initiatives selected for execution		
2	New technologies	Failure	Internal	Ineffective design	Process (technology selection) Enterprise architecture (technology)	Timing (non-critical) Duration (extended) Detection (slow)	P		S	• Failure to timely adopt and exploit new technologies (i.e., functionality, optimization) • New and important technology trends not identified • Inability to use the technology to realise desired outcomes (e.g., failure to make required business model or organisational changes)			• New technologies for new initiatives or more efficient operations adopted and exploited		

Environmental Risk Factors

- Market
- Rate of Change
- Geopolitical Situation
- Regulatory Environment
- Technology Status and Evolution

Internal Risk Factors

- Strategic Importance of IT
- Complexity of IT
- Complexity of the entity
- Degree of change
- Risk Management Philosophy
- Risk Appetite
- Operating Model



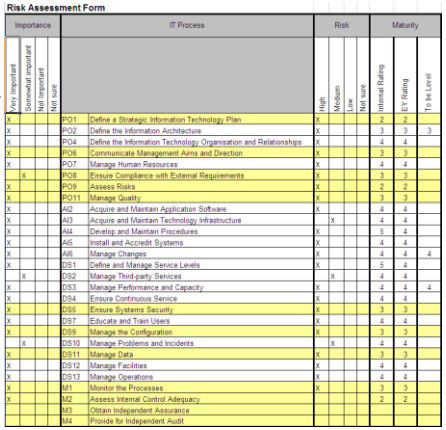
Generic IT Risk Scenarios Mapped to COBIT

	High-level Risk Scenario	IT Process Capabilities (COBIT): Plan and Organize (PO)	Acquire and Implement (AI)	Deliver and Support (DS)	Monitor and Evaluate (ME)
1	IT programme selection	PO1, PO2, PO3	AI1, AI3		ME1, ME3
2	New technologies	PO1, PO2, PO3	AI1, AI3		ME1
3	Technology selection	PO2, PO3	AI1, AI3		ME1
4	IT investment decision making	PO2, PO4, PO5, PO8	AI1, AI3		ME1
5	Accountability over IT	PO4, PO8, PO7		DS1, DS2	ME4
6	Integration of IT within business processes	PO1, PO3, PO4	AI1, AI2, AI3		
7	State of infrastructure technology	PO3, PO7, PO7	AI1, AI3, AI7	DS3	ME1
8	Ageing of application software	PO3, PO3, PO7	AI1, AI2, AI7	DS3	ME1
9	Architectural agility and flexibility	PO3, PO2, PO3, PO4, PO5	AI1, AI2, AI3, AI5		ME1
10	Regulatory compliance	PO1, PO4, PO8, PO7, PO9	AI1	DS4, DS5	ME3
11	Software implementation	PO10	AI2, AI4, AI5, AI6, AI7	DS7, DS8, DS9, DS10, DS13	ME1
12	IT project termination	PO4, PO5, PO8	AI2, AI3, AI5		ME1, ME4
13	IT project economics	PO5, PO10	AI5		ME1
14	Project delivery	PO5, PO8, PO10	AI2, AI3, AI5, AI6, AI7	DS2	ME1
15	Project quality	PO8, PO10	AI4, AI6, AI7	DS2	ME1
16	Selection/performance of third-party suppliers	PO4, PO5	AI5	DS1, DS2	ME1, ME4
17	Infrastructure theft	PO5, PO7		DS12	
18	Destruction of infrastructure			DS12	
19	IT staff	PO4, PO5, PO7	AI5	DS2, DS7	ME1
20	IT expertise and skills	PO7	AI5	DS2	ME1, ME4
21	Software integrity	PO5, PO10	AI2, AI6, AI7	DS2, DS5, DS8, DS10, DS13	ME1

Mapping Risk vs. Maturity

relevant risk scenarios vs. maturity level of mitigating controls

Heat map



Risk Assessment Form

Importance: Very important	Somewhat important	Not important	IT Process	Risk: High	Medium	Low	Not sure	Maturity: Internal Rating	EY Rating	To be Level
X			PO1 Define a Strategic Information Technology Plan	X				2	2	
X			PO2 Define the Information Architecture	X				3	3	3
X			PO4 Define the Information Technology Organisation and Relationships	X				4	4	
X			PO6 Communicate Management Aims and Direction	X				3	3	
X			PO7 Manage Human Resources	X				4	4	
	X		PO8 Ensure Compliance with External Requirements	X				3	3	
X			PO9 Assess Risks	X				2	2	
X			PO11 Manage Quality	X				3	3	
X			AI2 Acquire and Maintain Application Software	X				4	4	
X			AI3 Acquire and Maintain Technology Infrastructure		X			4	4	
X			AI4 Develop and Maintain Procedures	X				5	4	
X			AI5 Install and Accredit Systems	X				4	4	
X			AI6 Manage Changes	X				4	4	4
X			DS1 Define and Manage Service Levels	X				5	4	
	X		DS2 Manage Third-party Services		X			4	4	
X			DS3 Manage Performance and Capacity	X				4	4	4
X			DS4 Ensure Continuous Service	X				4	4	
X			DS5 Ensure Systems Security	X				3	3	
X			DS7 Educate and Train Users	X				4	4	
X			DS9 Manage the Configuration	X				3	3	
	X		DS10 Manage Problems and Incidents		X			4	4	
X			DS11 Manage Data	X				3	3	
X			DS12 Manage Facilities	X				4	4	
X			DS13 Manage Operations	X				4	4	
X			M1 Monitor the Processes	X				3	3	
X			M2 Assess Internal Control Adequacy					2	2	
			M3 Obtain Independent Assurance							
			M4 Provide for Independent Audit							

Maturity Level Assessment of IT Processes

Gretchenfrage: Welche IT Fähigkeiten benötigt mein Geschäftsmodell?

EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Fragen?