Geheimschutz, Grundschutz, ISMS – ein integratives Modell für Information Security

verinice.XP 2017

Alexander Koderman, CISA, PMP
Chief Security Officer
Cassidian Communications GmbH
Secure Land Communications

AIRBUS DEFENCE & SPACE

Prolog

Geheimschutz? Grundschutz? Aller Anfang ist schwer.

Aktivitäten zu sehr auf Geheimschutz ausgerichtet

Rechnungshof: Das BSI soll sich mehr um die DV-User kümmern

31.05.1991

MÜNCHEN (gs) - Das Anfang 1991 gegründete Bundesamt für Sicherheit in der Informationstechnik (BSI) kommt nur schwer von seiner geheimdienstlichen Vergangenheit los. In einer Stellungnahme zur Aufgabenstellung und Planung des BSI rügte der Bundesrechnungshof, daß die Behörde offenbar nicht vorhat, ihren neuen Aufgaben ernsthaft nachzukommen.

Mit der Ausgliederung der ehemaligen "Zentralstelle für Chiffrierwesen" (ZfCh) aus dem Bundesnachrichtendienst und ihrer Aufwertung zum Bundesamt wollte die Bundesregierung (mindestens) drei Fliegen mit einer Klappe schlagen: Das BSI sollte für mehr Sicherheit in der DV der Bundesbehörden sorgen, die öffentliche Forderung nach allgemeinen DV-Sicherheitsstandards erfüllen und schließlich noch Polizei und Geheimdiensten ein kompetenter Partner bei Abhöraktionen sein.

Diese "traditionelle" Ausrichtung des neuen Amtes zeigt auch die Herkunft und die Zuordnung des Personals: Etwa 75 Prozent der Mitarbeiter kommen aus den Nachrichtendiensten, und während für "Beratung und Unterstützung" gerade 18 der 278 Planstellen vorgesehen sind, sollen sich insgesamt 137 mit der Entwicklung von Verschlüsselungssystemen und mit Abstrahlsicherheit beschäftigen.

Laut Gesetz sollte das BSI "durch pragmatische umfassende Beratung und Unterstützung der

AIRBUS DEFENCE & SPACE

Prolog
BSI heute

- 600 Mitarbeiter
- Zertifizierung von Produkten, Managementsystemen & Personen
- Technische Richtlinien
- De-Mail, Elektronische Ausweise, Smart Metering, eHealth…
- Cyber-Sicherheit
- CERT-Bund
- Kryptotechnologie
- IT-Grundschutz

- Und nach wie vor: Materieller und IT-Geheimschutz

AIRBUS DEFENCE & SPACE

Inhalt

- **Vorstellung**
  - **Secure Landline Communications**
- Grundlagen: Geheimschutz
- Geheimschutz und IT
- Vergleich mit ISO 27001, BSI ITGS
- Konsolidiertes Maßnahmenmodell

AIRBUS DEFENCE & SPACE

Secure Land Communications

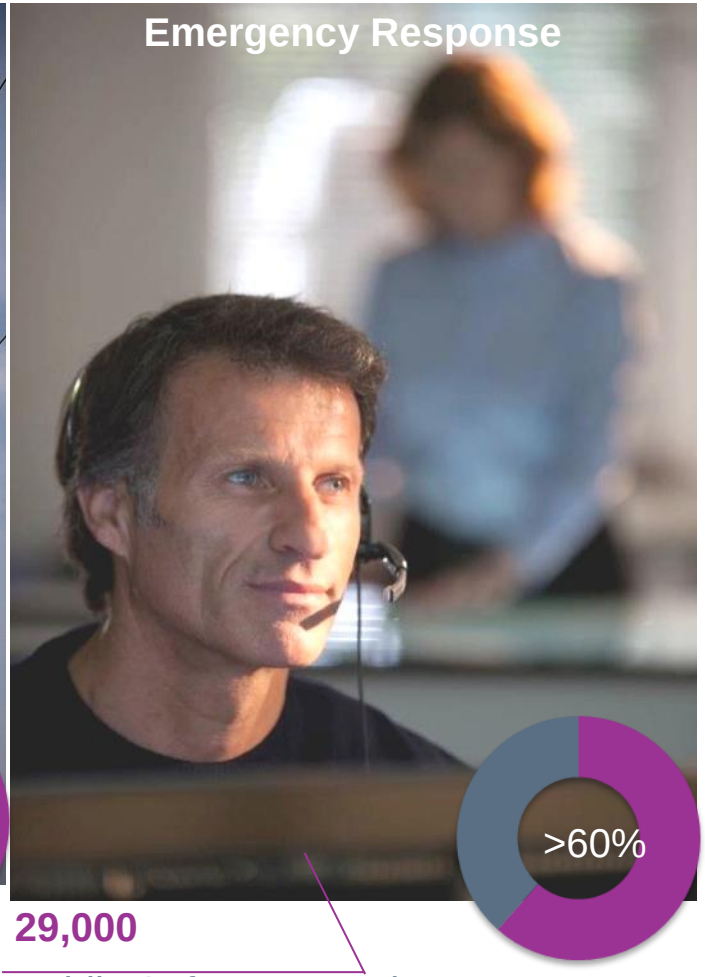
A worldwide leader in mission critical communications

3,000,000

Users in Public Safety/Defence in Europe, Middle East and Asia

>100

Operators for CNI in Europe, Middle East and Asia



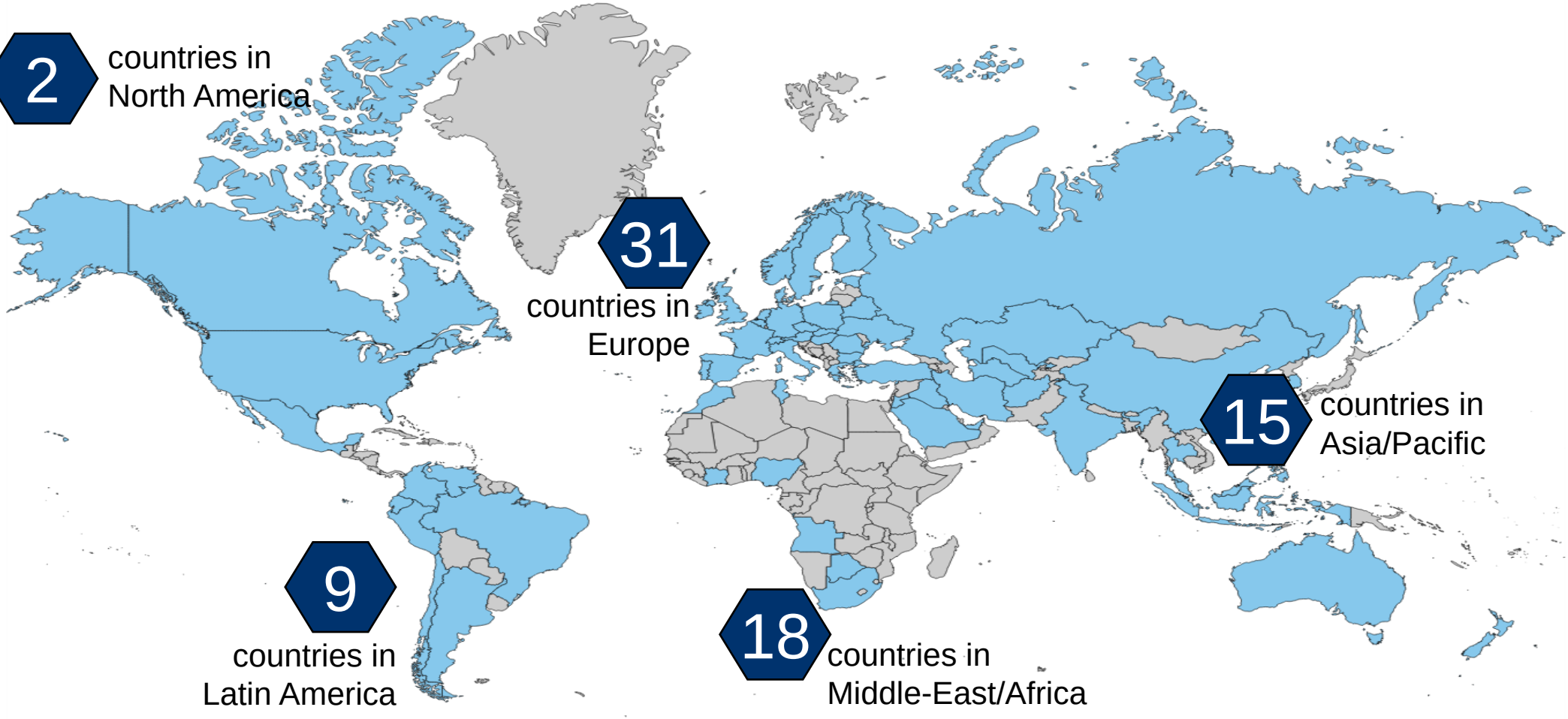
29,000

Public Safety Answering Points in USA

AIRBUS DEFENCE & SPACE

Secure Land Communications

We support our customers in 75 countries



AIRBUS DEFENCE & SPACE

Cassidian Communications GmbH Overview

- Cassidian Communications GmbH is the regional entity of the Airbus Secure Land Communications Communication Business Line (SLC)

- Responsible for business development, sales and operations in the DACH countries (GE, AUT, SUI) plus dedicated export markets

- Three sites with 191 employees overall (31.08.2016)
  - Ulm: HQ, PM, Engineering, Sales, Service
  - Berlin: Sales, Service
  - Sulzbach: Sales, Service, 24/7Service Center

- Annual turnover of 131 Million € in 2015 (HGB)

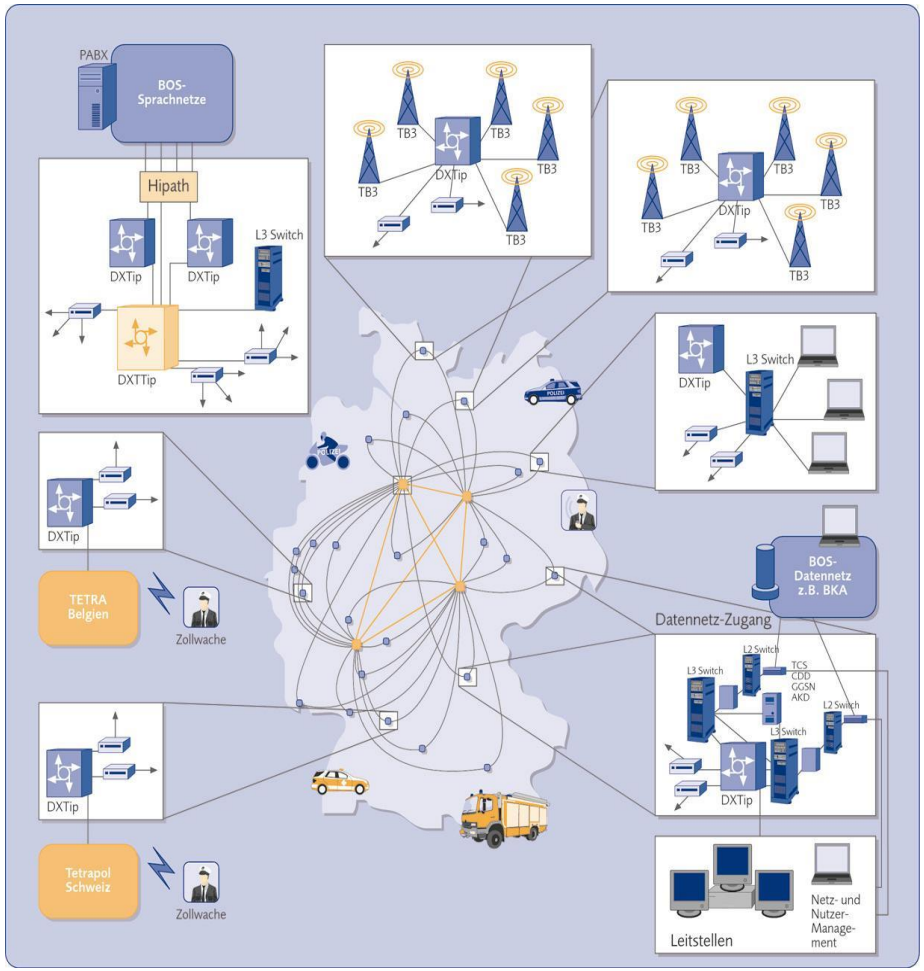
AIRBUS DEFENCE & SPACE

References (1)

BOSNET

- Nationwide coverage (including maritime islands and 12-mile-zone) makes BOSNET worldwide the largest TETRA network
- Designed for up to 500.000 users from police, fire brigade, rescue, customs and intelligence services
- Strong customer focus on security, interoperability and resilience in both design and operations
- Owned and operated by a federal agency (BDBOS) on behalf of the federal republic of Germany and its 16 states
- Key data: BS installations: 4.570* (4.800 planned), Switching Centes: 64*, two georedundant Network Management Centers, users: 520.000 * (>700.000 users planned)
- Cassidian Communications GmbH is the prime contractor for the installation, integration, commissioning and maintenance of the network

Bundesanstalt
für den Digitalfunk der Behörden und
Organisationen mit Sicherheitsaufgaben



* August 2015

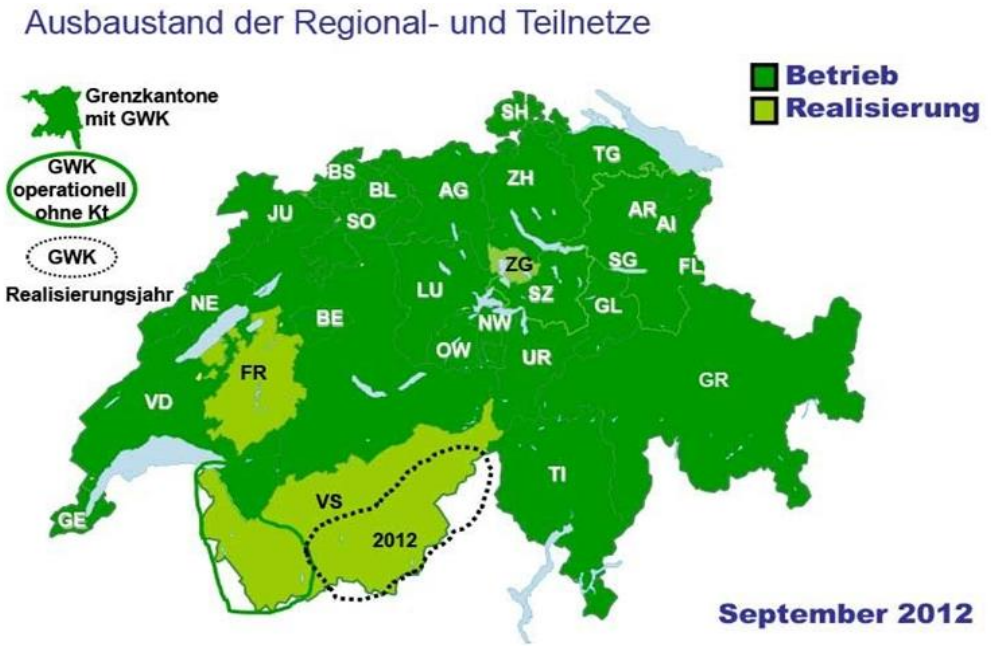
AIRBUS DEFENCE & SPACE

References (2)

POLYCOM

- POLYCOM:
  Nationwide PMR network in CH (TETRAPOL-Technology)
- Roll-Out 1998 to 2014
- partnership with ATOS AG
- Delivery till today app. 190 Mio.€
- Next Campaigns
  - IP Migration
  - Extension with LTE Broadband

	installed
BS	700
User	50.000
Switch	40



References (3)

Landesfunknetz Südtirol (LFN)

- Nationwide Tetra network for civil protection (small copy of BOSNET)
- Contract won after 1 year defending appeals form Motorola, project start 09.2013
- First 62 base stations build up in 6 month in the mountains
- Second batch of 51 base stations awarded end 2014, acceptance planned in 2016
- Further extension in the pipeline
  - Terminals shall be awarded in 2016/17
  - Further network extensions planned for Phase 3 (2016)
  - Customer budget total 20 Mio for 5 years
- Strategic footprint for the renewal of public safety networks in Northern Italy

CASSIDIAN
AN EADS COMPANY

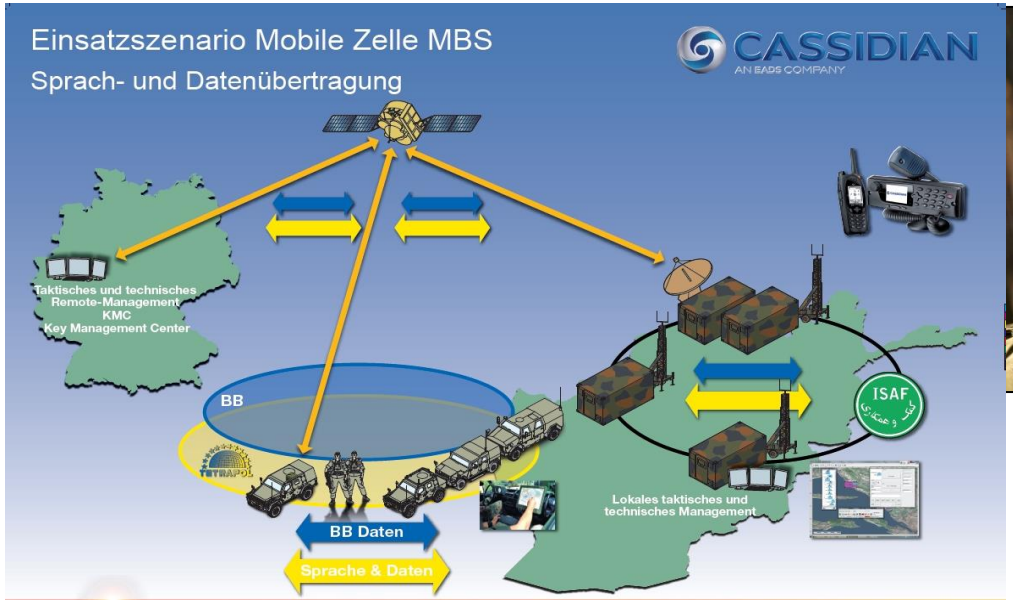
AIRBUS
DEFENCE & SPACE

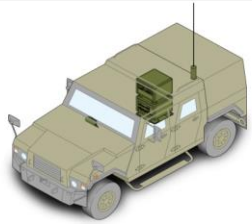
References (4)

German Army

BAAINBw

- Secure, cellular networks for the German Army
  - CRF: 30 deployable shelters delivered 2008-2008, backbone for tactical communications for the German Army in out-of-area missions
  - TetrapolBw: PMR networks based on CRF for Bw installations in Germany
  - Support: in service support for all CRF system with stringent SLAs
- Highly Mobile Cell (HochZeN):
  - 3 mobile networks with NB voice and BB data capability delivered in 2014
  - Field trials to prepare procurement and CRF refurbishment scheduled in 2015





AIRBUS DEFENCE & SPACE

References (5)

Transport and Utilities

- Networks for
  - Utilities (Lechwerke, Evonik, Stadtwerke Munich, Vattenfall, …)
  - Airports (Zürich, Berlin Tegel, …)
  - Public Urban Transport (Hamburg Subway, Berlin Subway, …)
- Voice Network for maintenance staff
- Data network for command and control applications;
- Basic communication infrastructure for future “Smart Grid”
- Service contracts with stringent SLAs

LEW Lechwerke

SWM Stadtwerke München

VATTENFALL

Inhalt

- Vorstellung
  - Secure Landline Communications
- **Grundlagen: Geheimschutz**
- Geheimschutz und IT
- Vergleich mit ISO 27001, BSI ITGS
- Konsolidiertes Maßnahmenmodell

Grundlagen: Geheimschutz (in der Wirtschaft)

- Voraussetzung: VS-Auftrag
- Betreuung und Kontrolle durch BMWi
- §25 SÜG
- Geheimschutzhandbuch: 85 Seiten
- Anlagen: 226 Seiten
- Weitere technische Leitlinien
  - Sind VS-NfD…

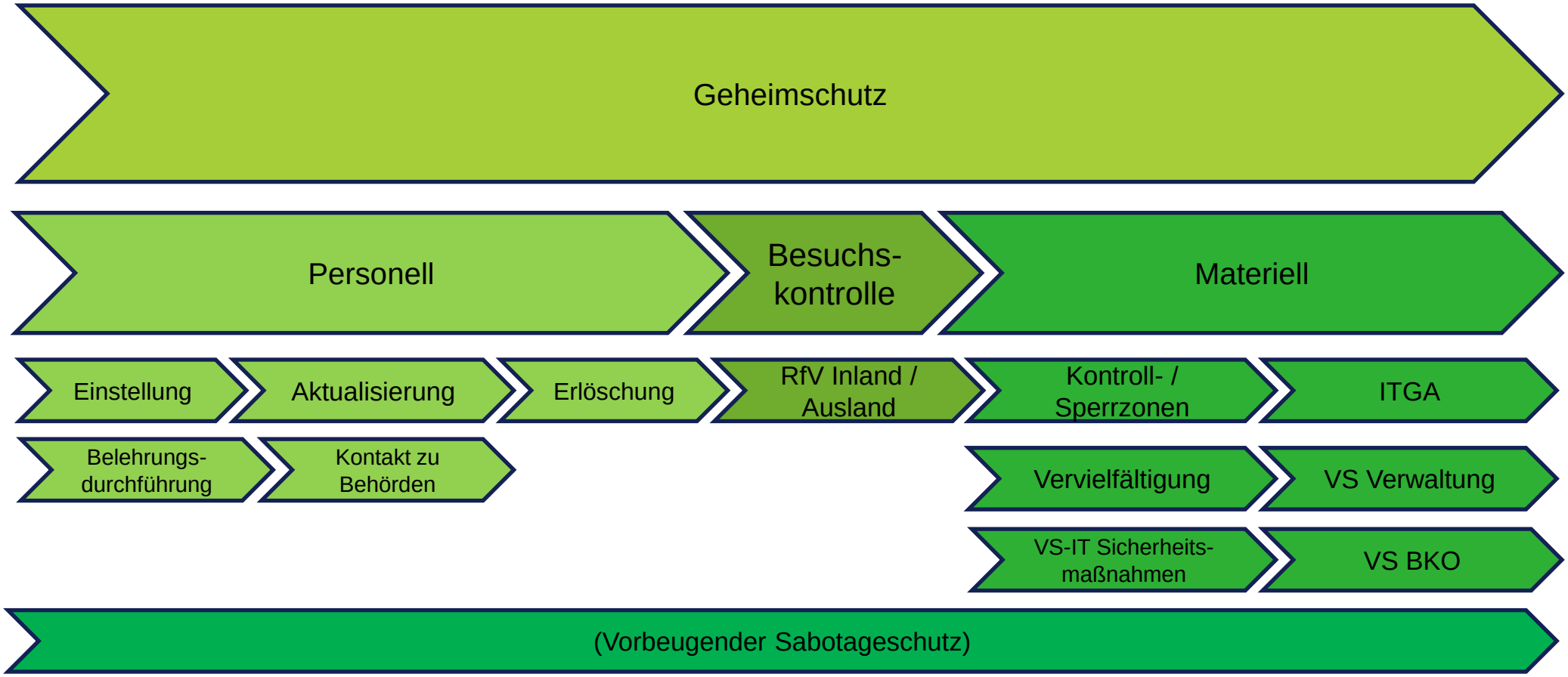
AIRBUS DEFENCE & SPACE

Verschlusssachen

- Information von amtlicher Stelle (oder auf deren Veranlassung) eingestuft
- Klassifikation:
  - VS-Nur für Dienstgebrauch (NfD)
  - VS-Vertraulich
  - VS-Geheim
  - VS-Streng Geheim
- Organisatorische, personelle, materielle, technische Maßnahmen

AIRBUS DEFENCE & SPACE

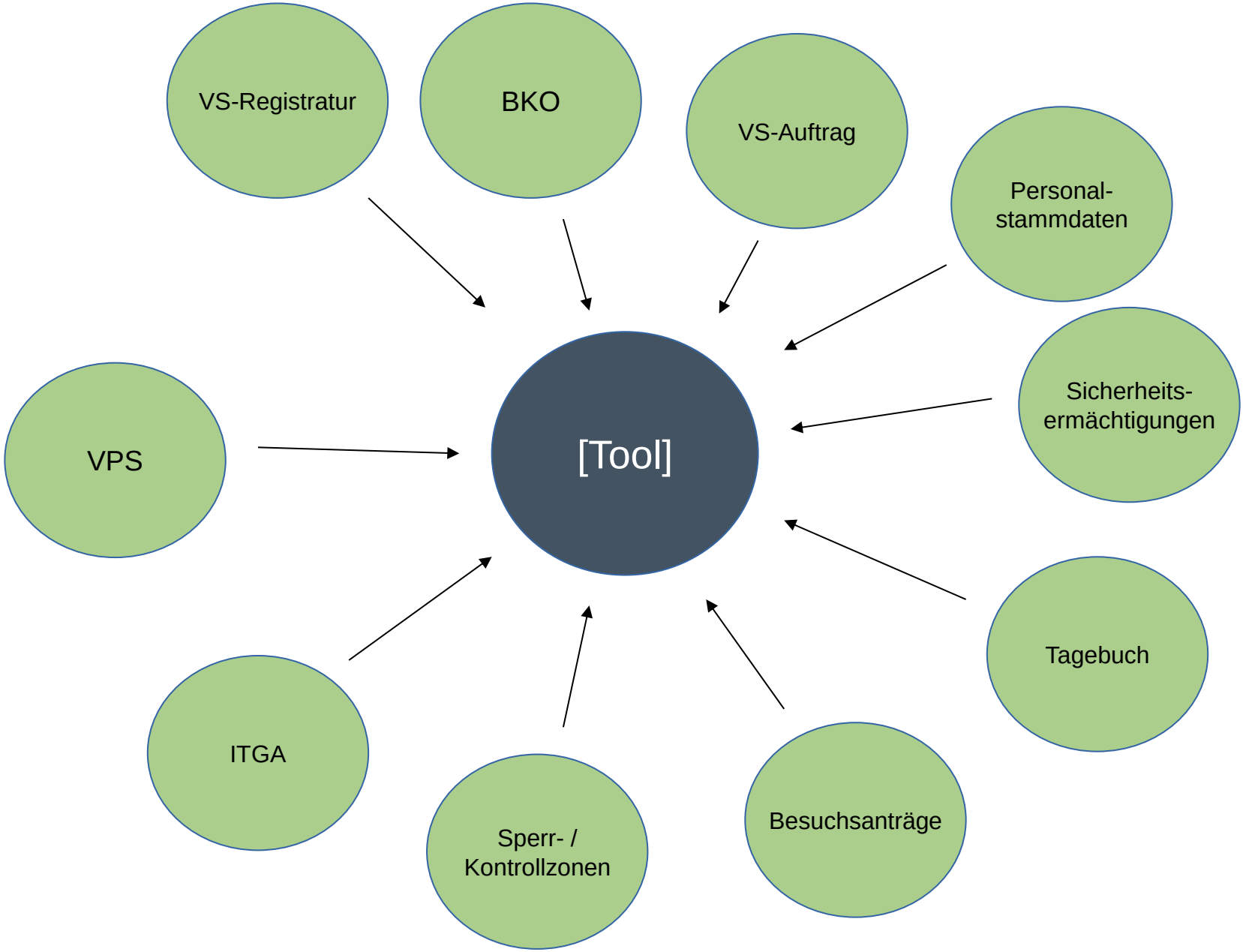
Geheimschutz-Prozesse



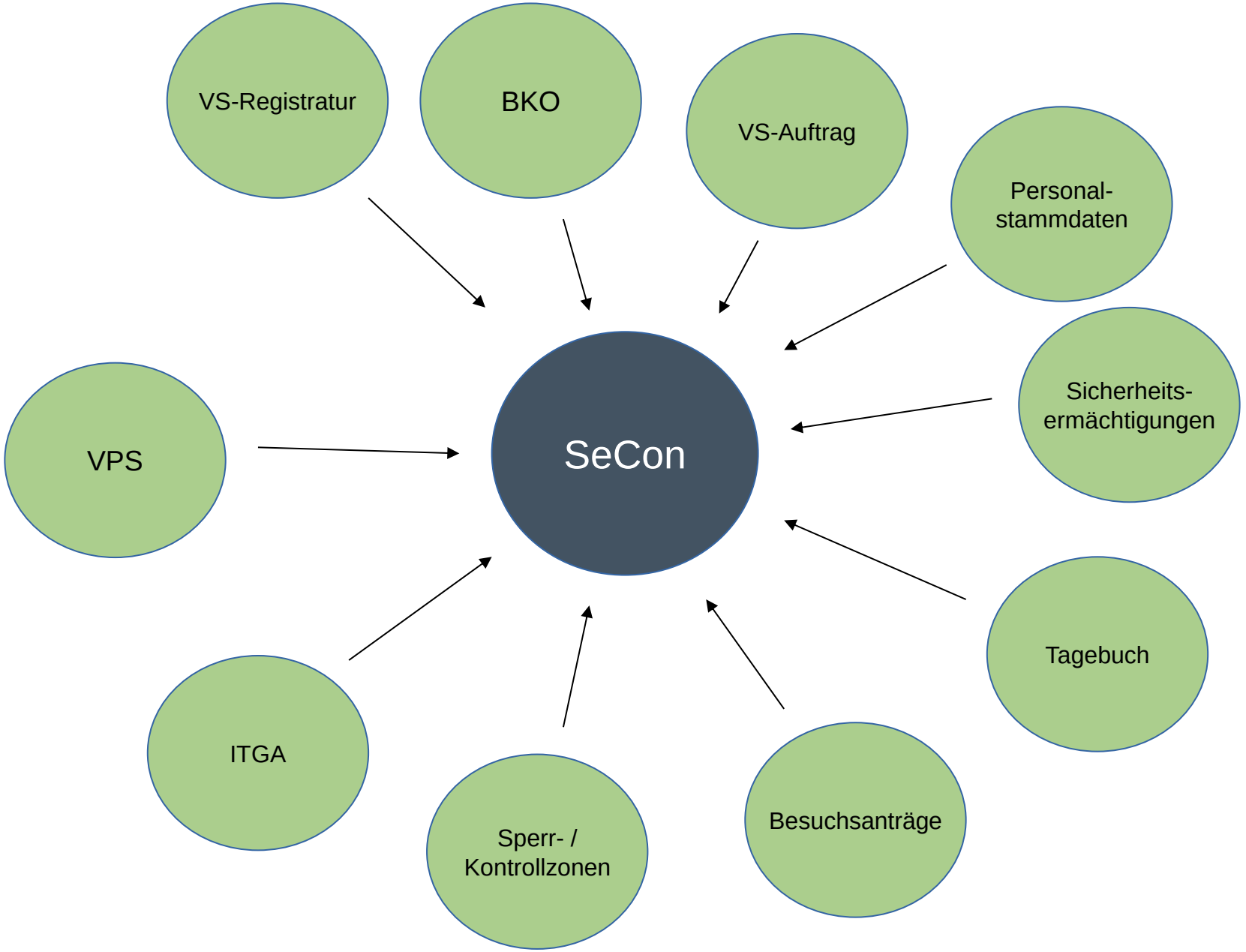
AIRBUS DEFENCE & SPACE

Geheimschutzprozesse: Dokumente, Ressourcen

Prozess: Geheimschutz gewährleisten		
Input	***Ressourcen***	***Output***
• VS-Auftrag • Meldung: neuer Kollege/in • Meldung: Beendigung Arbeitsverhältnis • Besuchsanmeldung • Meldung: Geplante IT-Bearbeitung von VS	Personal: • Sicherheitsbevollmächtigte/r • SiBE-Vertreter/in • VS-Verwalter/in • VS-IT Sicherheitsbeauftragte/r Infrastruktur: • VS-Lager • VS-Registratur • Kontrollzone / Sperrzone	• Sicherheitsbescheid (CCG) • Ermächtigungsurkunde (Kollege) • Sicherheitsbescheinigung (Besucher) • Genehmigte Sperrzone • Genehmigte IT-Verarbeitung von VS
	Dokumente: • Verschlusssachen (Dokumente, Datenträger…) • VS-Material (Geräte) • VS-Zwischenmaterial • VS-Einstufungsliste • VS-Bereichsverzeichnis • VS-Personalverzeichnis • VS-Auftragsverzeichnis • VS-Auftragsmeldung (halbjährlich) • Auftragsbezogene Rollenliste • VS-NfD-Merkblatt • Sicherheitsakte • Antrag auf VS-Ermächtigung • VS-Ermächtigungsurkunde • VS-Ermächtigungsbestätigung • VS-Empfangsschein • Zusatzvereinbarung bei Abstellungsvereinbarung • Sicherheitserklärung • Beiblatt zur Sicherheitserklärung • Wiederholungsprüfung • Aktualisierung der Prüfung • Erlöschungsantrag • Beiblatt zum Austritt • Veränderungsmeldung • IT-Geheimschutzanweisung • Einwilligung zur VS-IT-Bearbeitung • ITGA-Checkliste (Neuanmeldung) • VS-Auftragsmeldung • Security Aspects Letter (projektbezogen) • Geheimschutzplan • Jahresbericht für die Geschäftsleitung • Kommunikationskonzept • IT-Sicherheitskonzept • Bestätigung der Erstbelehrung • Merkblatt „Anleitung für Geheimhaltung in der Wirtschaft"	



AIRBUS
DEFENCE & SPACE



AIRBUS
DEFENCE & SPACE

6.6.2 Nachweise

(1) VS-Vervielfältigungsauftrag (Anlage 46), VS-Tagebuch (Anlage 47), VS-Quittungsbuch (Anlage 50), VS-Empfangsschein (Anlage 51), VS-Übergabeprotokoll (Anlage 52), VS-Vernichtungsverhandlung (Anlage 53), VS-Ausfertigungs-/Vervielfältigungsnachweis (Anlage 48), Quittungsbuch für VS-Zwischenmaterial (Anlage 54) und Berichtigungsnachweis (Anlage 55) sind grundsätzlich nach den von BMWi verfügten Vorgaben zu führen. VS-Tagebücher und VS-Ausfertigungs-/-Vervielfältigungsnachweise sind grundsätzlich in Buchform zu führen. Abweichungen hiervon und eine IT-gestützte VS-Tagebuchführung bedürfen der Einwilligung des BMWi.

(2) VS-Tagebücher und VS-Ausfertigungs-/Vervielfältigungsnachweise sind entsprechend dem Geheimhaltungsgrad der höchsten in ihnen nachgewiesenen VS zu verwahren.

(3) VS-Tage- und VS-Quittungsbücher, VS-Empfangsscheine,

AIRBUS DEFENCE & SPACE

Die Briefhüllen sind mit Scotch-Siegelband 820 und dem Scotch-Schnellsiegler TSZ 2240 mit Anwenderlogo zu versiegeln. Die dafür erforderliche Ausstattung kann im Bürofachhandel bezogen werden:

- Scotch-Siegelband 820 von 3M
- Scotch-Handabroller H 315 von 3M
- Scotch-Schnellsiegler TSZ 2240 von 3M

Der spezielle Siegelaufsatz, der das Anwenderlogo trägt, gehört nicht zum Lieferumfang des Schnellsieglers und kann durch örtliche Klischeehersteller hergestellt werden.

Alternativ können die Briefhüllen mit Sicherheitsetiketten versiegelt werden. Vom BSI sind folgende Etiketten zugelassen:

- Advantage Transfer der Firma Schreiner
- Sico Tra-Klebesiegel der Firma Trautwein Security

Als innere Briefhülle können auch DEBASAFE-Taschen aus PE-Folie der Firma Anton Debatin verwendet werden. Für den Versand von GEHEIM eingestuften VS werden die DEBASAFE-Taschen wegen ihrer höheren Sicherheit empfohlen.

AIRBUS DEFENCE & SPACE

Inhalt

- Vorstellung
  - Secure Landline Communications
- Grundlagen: Geheimschutz
- **Geheimschutz und IT**
- Vergleich mit ISO 27001, BSI ITGS
- Konsolidiertes Maßnahmenmodell

AIRBUS DEFENCE & SPACE

Geheimschutz und IT

- Maßnahmen bereits ab VS-NfD
  - Verschlüsselung
  - Organisatorische Maßnahmen
- Ab VS-V:
  - Sperrzone
  - ITGA
  - Spezialhardware
- BSI Technische Leitlinien
  - VS-NfD

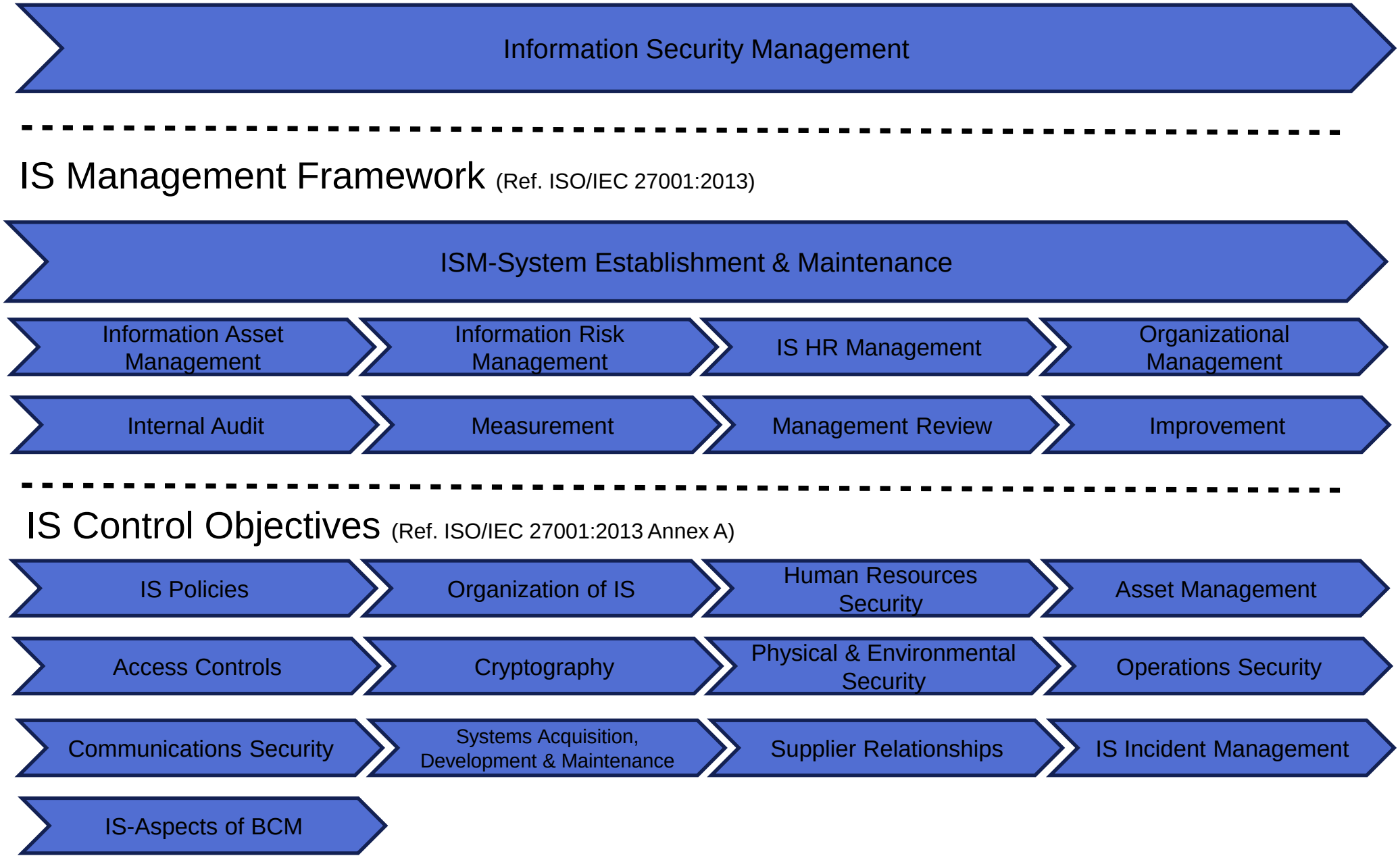
Inhalt

- Vorstellung
  - Secure Landline Communications
- Grundlagen: Geheimschutz
- Geheimschutz und IT
- **Vergleich mit ISO 27001, BSI ITGS**
- Konsolidiertes Maßnahmenmodell

AIRBUS DEFENCE & SPACE

- GHB 6.11.1 – „Grundsatz“:
  - Vertraulichkeit, Verfügbarkeit, Integrität
- VSITR/U Maßnahmen:
  - Zuständigkeiten
  - IT-Planung & Beschaffung
  - Zugangs-, Zugriffskontrolle
  - Schutz von IT-Betriebsräumen
  - Löschen und Vernichten von Datenträgern
  - Systemwartung
  - Abstrahlsicherheit
  - Krypto-Richtlinien
  - Kennzeichnung von Datenträgern
  - Not- / Katastrophenfall
  - […]

AIRBUS DEFENCE & SPACE

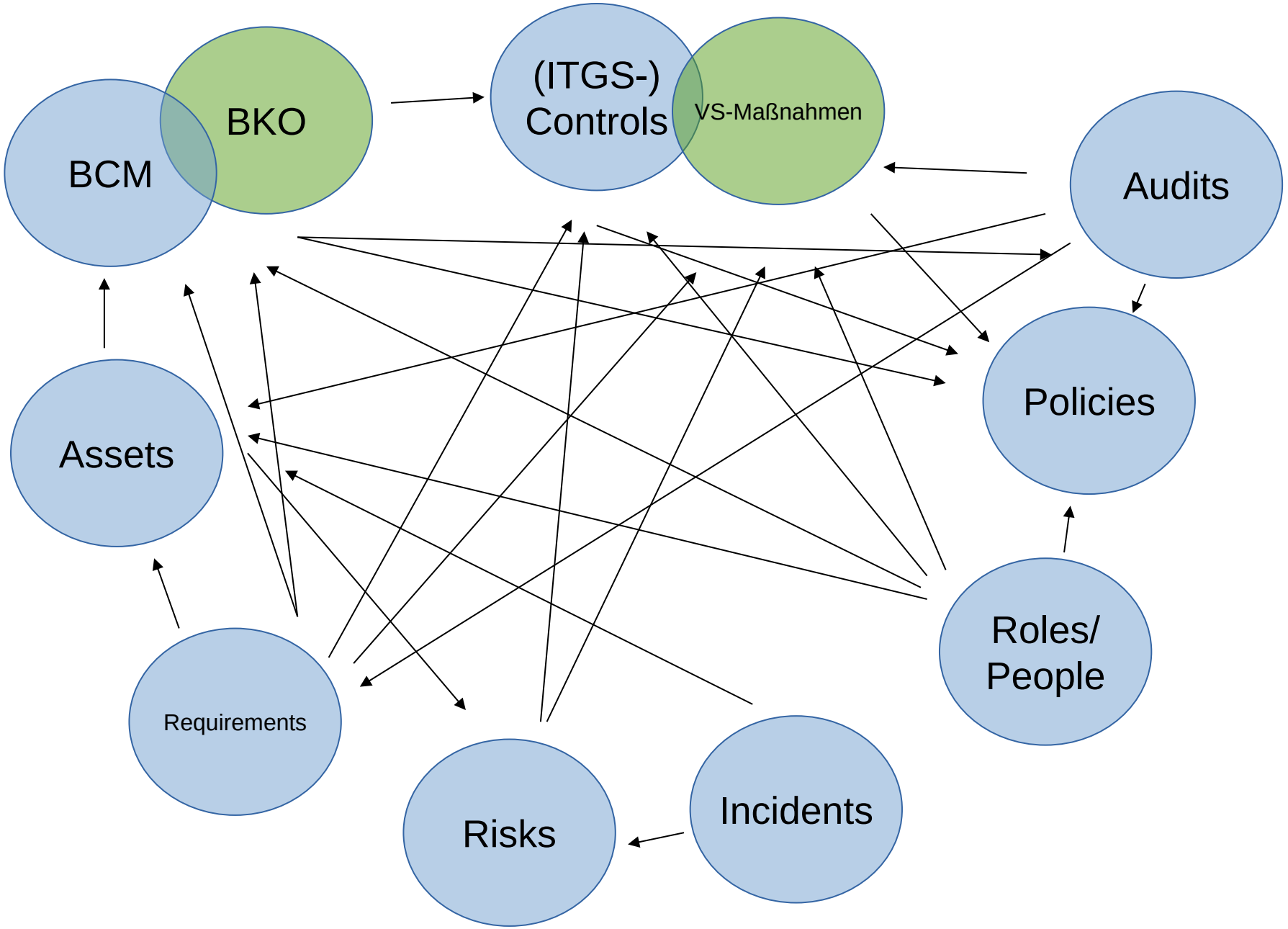


AIRBUS DEFENCE & SPACE

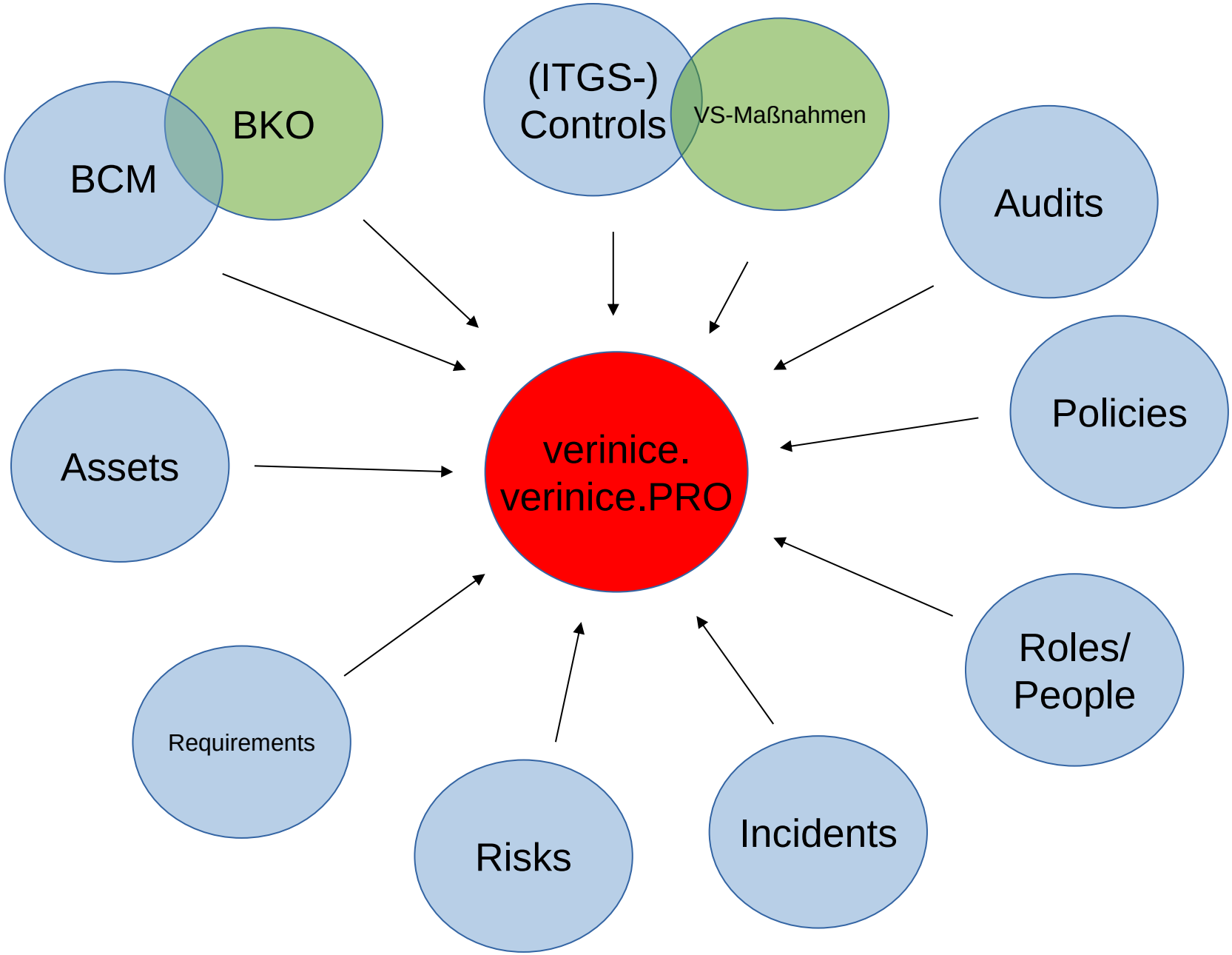
Inhalt

- Vorstellung
  - Secure Landline Communications
- Grundlagen: Geheimschutz
- Geheimschutz und IT
- Vergleich mit ISO 27001, BSI ITGS
- **Konsolidiertes Maßnahmenmodell**

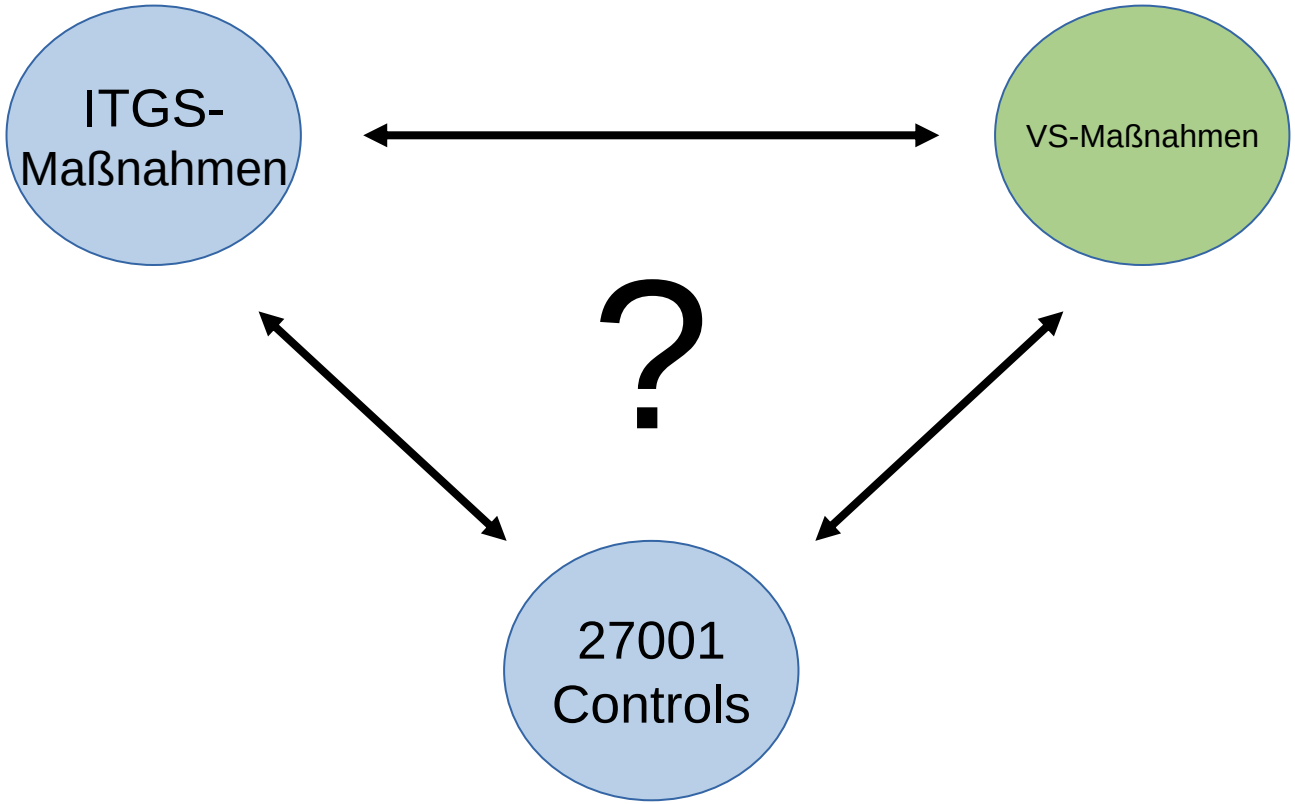
AIRBUS DEFENCE & SPACE



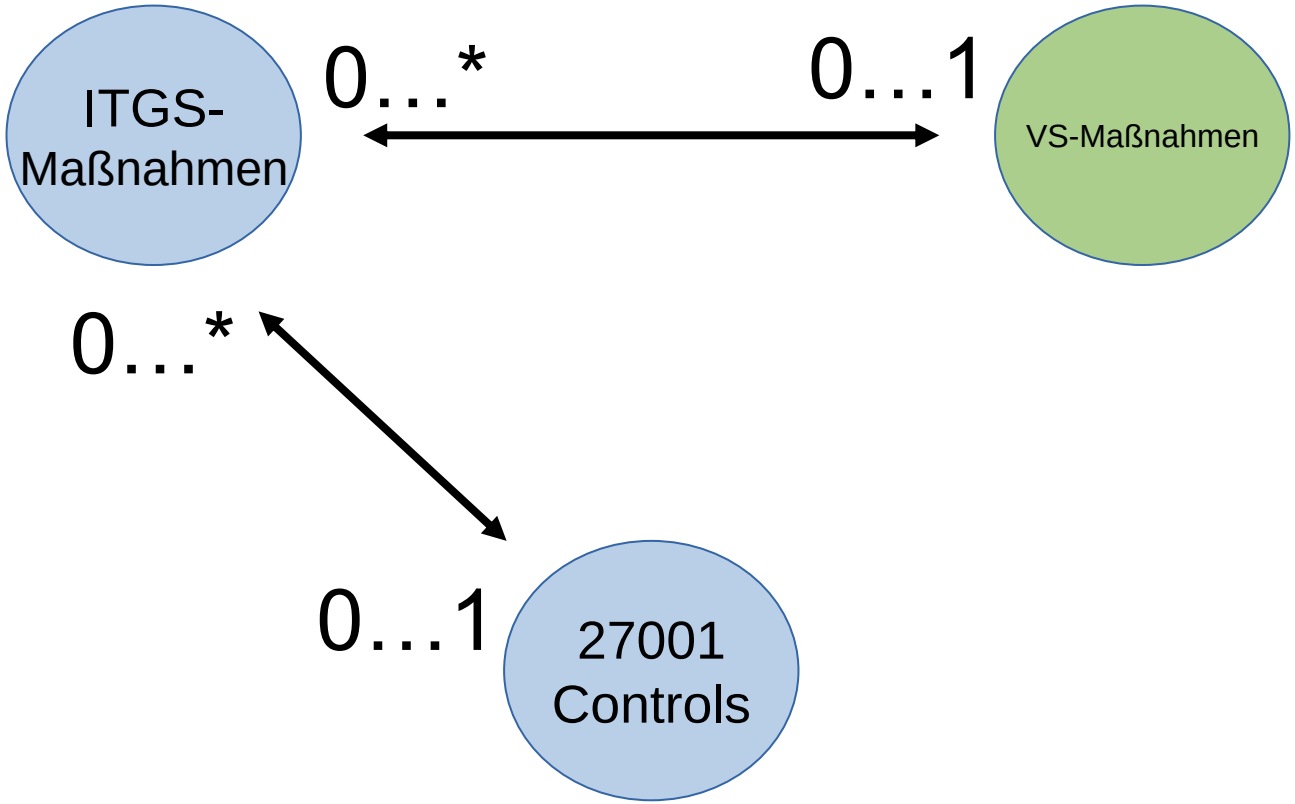
AIRBUS
DEFENCE & SPACE



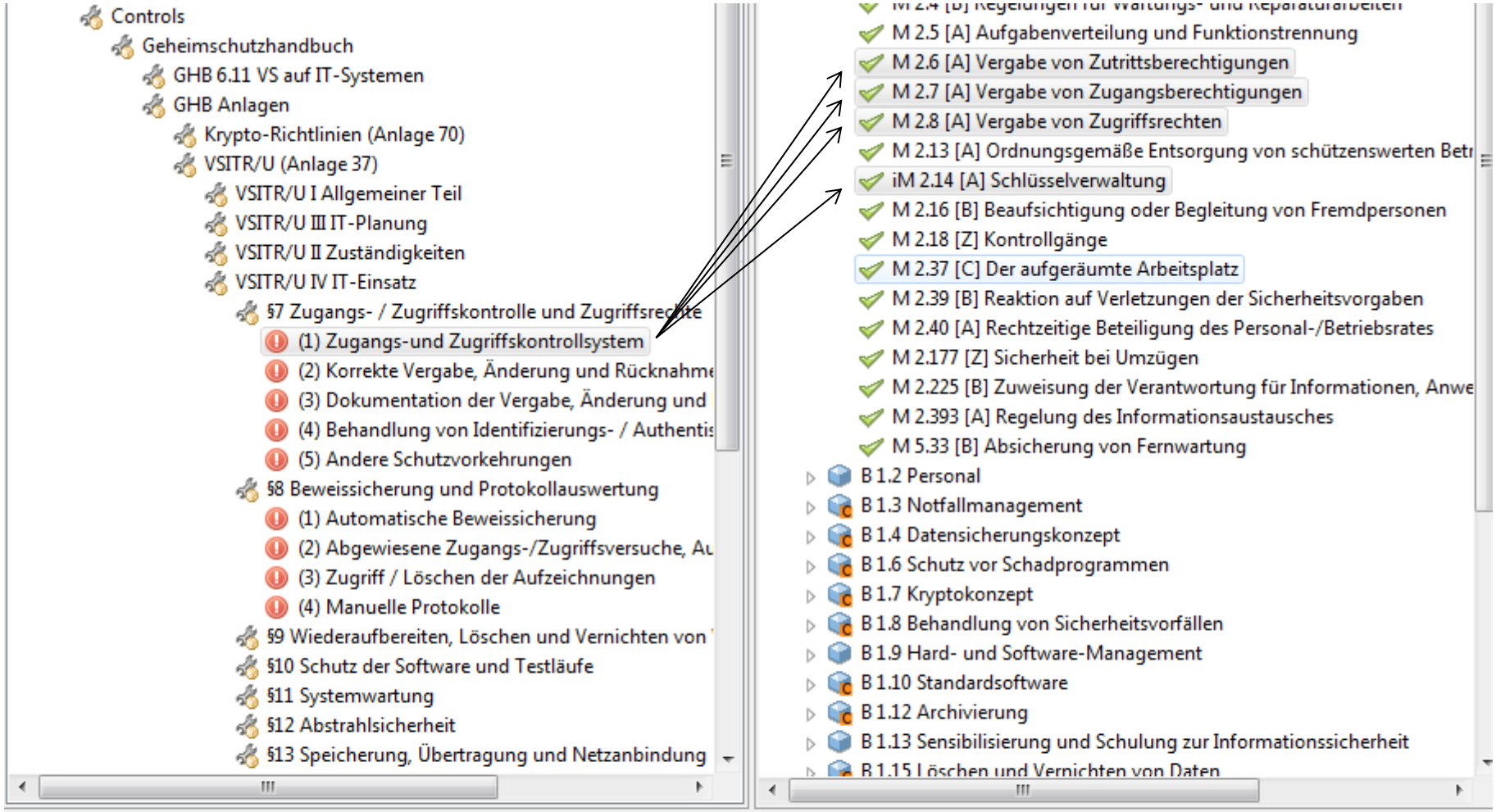
AIRBUS
DEFENCE & SPACE



AIRBUS
DEFENCE & SPACE



AIRBUS DEFENCE & SPACE



Verknüpfungen

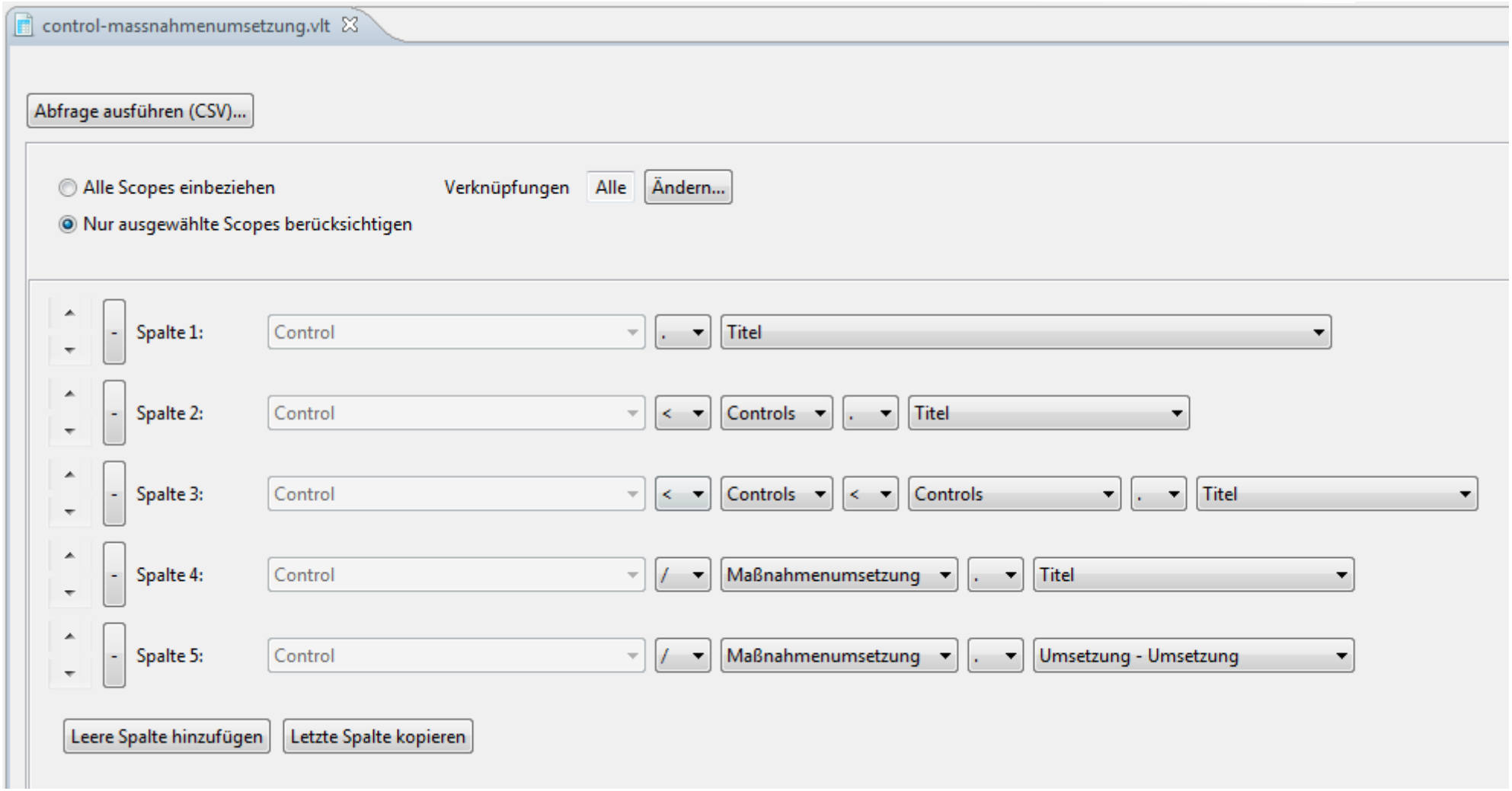
Verknüpfung für: (1) Zugangs-und Zugriffskontrollsystem

Verknüpfung	Titel	Scope	Beschreibung
implementiert durch	M 2.6 [A] Vergabe von Z...	RECPLAST	
implementiert durch	M 2.7 [A] Vergabe von Z...	RECPLAST	
implementiert durch	M 2.8 [A] Vergabe von Z...	RECPLAST	
implementiert durch	iM 2.14 [A] Schlüsselver...	RECPLAST	

Custom Relation-Type

AIRBUS DEFENCE & SPACE

Abfrage über Relation zu Maßnahmen



AIRBUS DEFENCE & SPACE

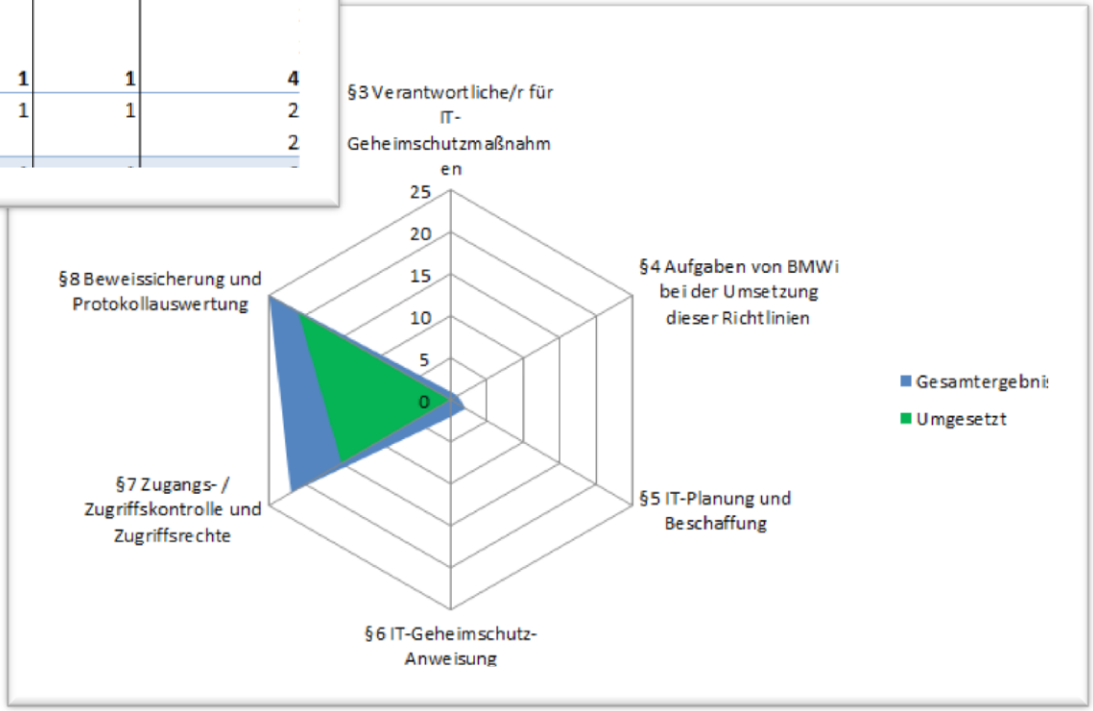
Ausgabetabelle

	A	B	C	D	E
1	Titel_(Control)	Titel_(Controls)	Titel_(Controls)	Titel_(Maßnahmenumsetzung)	Umsetzung_-
2	(1) Automatische Beweissicherung	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	Audit und Protokollierung der Aktivitäten im Netz	Ja
3	(1) Automatische Beweissicherung	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	Datenschutzaspekte bei der Protokollierung	Ja
4	(1) Automatische Beweissicherung	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	Planung der Systemüberwachung unter Windows Server 2003	Ja
5	(1) Automatische Beweissicherung	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	Planung der Systemüberwachung unter Windows Server 2003	Ja
6	(1) Automatische Beweissicherung	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	Planung der Systemüberwachung unter Windows Server 2003	Ja
7	(1) Automatische Beweissicherung	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	Planung der Systemüberwachung unter Windows Server 2003	Ja
8	(1) Automatische Beweissicherung	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	Planung der Systemüberwachung unter Windows Server 2003	Ja
9	(1) Automatische Beweissicherung	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	Planung der Systemüberwachung unter Windows Server 2003	Ja
10	(1) Automatische Beweissicherung	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	Protokollierung am Server	Ja
11	(1) Automatische Beweissicherung	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	Protokollierung bei Routern und Switches	Ja
12	(1) Automatische Beweissicherung	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	Protokollierung bei TK-Anlagen	Ja
13	(1) Automatische Beweissicherung	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	Protokollierung der Archivzugriffe	Ja
14	(1) Automatische Beweissicherung	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	Protokollierung der Sicherheitsgateway-Aktivitäten	Ja
15	(1) Automatische Beweissicherung	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	[leer]	[leer]
16	(1) Beteiligung des SiBe bei Planungsbeginn, bei komplexen IT-Systemen BMWi	§5 IT-Planung und Beschaffung	VSITR/U III IT-Planung	[leer]	[leer]
17	(1) ITGA / Sicherheitskonzept für eingesetzte IT	§6 IT-Geheimschutz-Anweisung	VSITR/U III IT-Planung	[leer]	[leer]
18	(1) Zugangs-und Zugriffskontrollsystem	§7 Zugangs- / Zugriffskontrolle und Zugriffsrechte	VSITR/U IV IT-Einsatz	Schlüsselverwaltung	Ja
19	(1) Zugangs-und Zugriffskontrollsystem	§7 Zugangs- / Zugriffskontrolle und Zugriffsrechte	VSITR/U IV IT-Einsatz	Vergabe von Zugangsberechtigungen	Ja
20	(1) Zugangs-und Zugriffskontrollsystem	§7 Zugangs- / Zugriffskontrolle und Zugriffsrechte	VSITR/U IV IT-Einsatz	Vergabe von Zugriffsrechten	Ja
21	(1) Zugangs-und Zugriffskontrollsystem	§7 Zugangs- / Zugriffskontrolle und Zugriffsrechte	VSITR/U IV IT-Einsatz	Vergabe von Zutrittsberechtigungen	Ja
22	(1) Zugangs-und Zugriffskontrollsystem	§7 Zugangs- / Zugriffskontrolle und Zugriffsrechte	VSITR/U IV IT-Einsatz	Zutrittsregelung und -kontrolle	Ja
23	(1) Zugangs-und Zugriffskontrollsystem	§7 Zugangs- / Zugriffskontrolle und Zugriffsrechte	VSITR/U IV IT-Einsatz	[leer]	[leer]
24	(2) Abgewiesene Zugangs-/Zugriffsversuche, Ausgaben und Übermittlungen	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	Kontrolle der Protokolldateien	Ja
25	(2) Abgewiesene Zugangs-/Zugriffsversuche, Ausgaben und Übermittlungen	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	Kontrolle der Protokolldateien eines Datenbanksystems	Ja
26	(2) Abgewiesene Zugangs-/Zugriffsversuche, Ausgaben und Übermittlungen	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System	Ja
27	(2) Abgewiesene Zugangs-/Zugriffsversuche, Ausgaben und Übermittlungen	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen	Ja
28	(2) Abgewiesene Zugangs-/Zugriffsversuche, Ausgaben und Übermittlungen	§8 Beweissicherung und Protokollauswertung	VSITR/U IV IT-Einsatz	[leer]	[leer]
29	(2) Berücksichtigung der Hinweise des BMWi	§4 Aufgaben von BMWi bei der Umsetzung dieser Richtlinien	VSITR/U II Zuständigkeiten	[leer]	[leer]
30	(2) Festlegung der IT-Sicherheitsfunktionen vor der Beschaffung	§5 IT-Planung und Beschaffung	VSITR/U III IT-Planung	[leer]	[leer]
31	(2) Genehmigung der ITGA durch BMWi	§6 IT-Geheimschutz-Anweisung	VSITR/U III IT-Planung	[leer]	[leer]
32	(2) Korrekte Vergabe, Änderung und Rücknahme von Zugriffsrechten	§7 Zugangs- / Zugriffskontrolle und Zugriffsrechte	VSITR/U IV IT-Einsatz	Schlüsselverwaltung	Ja

AIRBUS DEFENCE & SPACE

Anzahl von Umsetzung_-_Umsetzung_(Maßnahmenumsetzung)	Spalte					
Zeilenbeschriftungen	[leer]	Entbehrlich	Ja	Nein	Teilweise	Gesamtergebnis
B Kryptomittel BSI	**2**					
§ 1 Anwendbarkeit	1					
§ 3 Begriffsbestimmungen	1					
GHB 6.11 VS auf IT-Systemen	**11**					**1**
GHB 6.11.2 Verarbeitung	4					
GHB 6.11.3 Beförderung, Mitnahme, Übertragung	5					
GHB 6.11.4 Weiterführende Richtlinien	2					
Krypto-Richtlinien (Anlage 70)	**1**					
A Kryptomittel BW NDA Germany	1					
VSITR/U (Anlage 37)	**1**					
VSITR/U I Allgemeiner Teil	1					
VSITR/U II Zuständigkeiten	**2**					
§3 Verantwortliche/r für IT-Geheimschutzmaßnahmen	1					
§4 Aufgaben von BMWi bei der Umsetzung dieser Richtlinien	1					
VSITR/U III IT-Planung	**4**					
§5 IT-Planung und Beschaffung	2					
§6 IT-Geheimschutz-Anweisung	2					
VSITR/U IV IT-Einsatz	**9**	**1**	**35**	**1**	**1**	**4**
§7 Zugangs- / Zugriffskontrolle und Zugriffsrechte	5	1	14	1	1	2
§8 Beweissicherung und Protokollauswertung	4		21			2

- Darstellung:
  - Pivot-Tabelle
  - Radar-Chart



AIRBUS DEFENCE & SPACE

Thank you for listening!

Questions?

AIRBUS
DEFENCE & SPACE