BearingPoint
RCS Capability Statement

- Security Governance -

Juli 2015

BearingPoint®

Agenda

1. Herausforderungen
2. Unser Angebot
3. Ihr Nutzen

Information Security Governance muss vielen Herausforderungen begegnen

Für **Information Security Governance** ist es essentiell, dass Information Security mit dem dazugehörenden Managementsystem (ISMS) die Behördenziele unterstützt. Information Security Governance liegt in der Verantwortung der Behördenleitung, schafft eine transparente Organisation und steuert vorausschauend die IS-Prozesse.

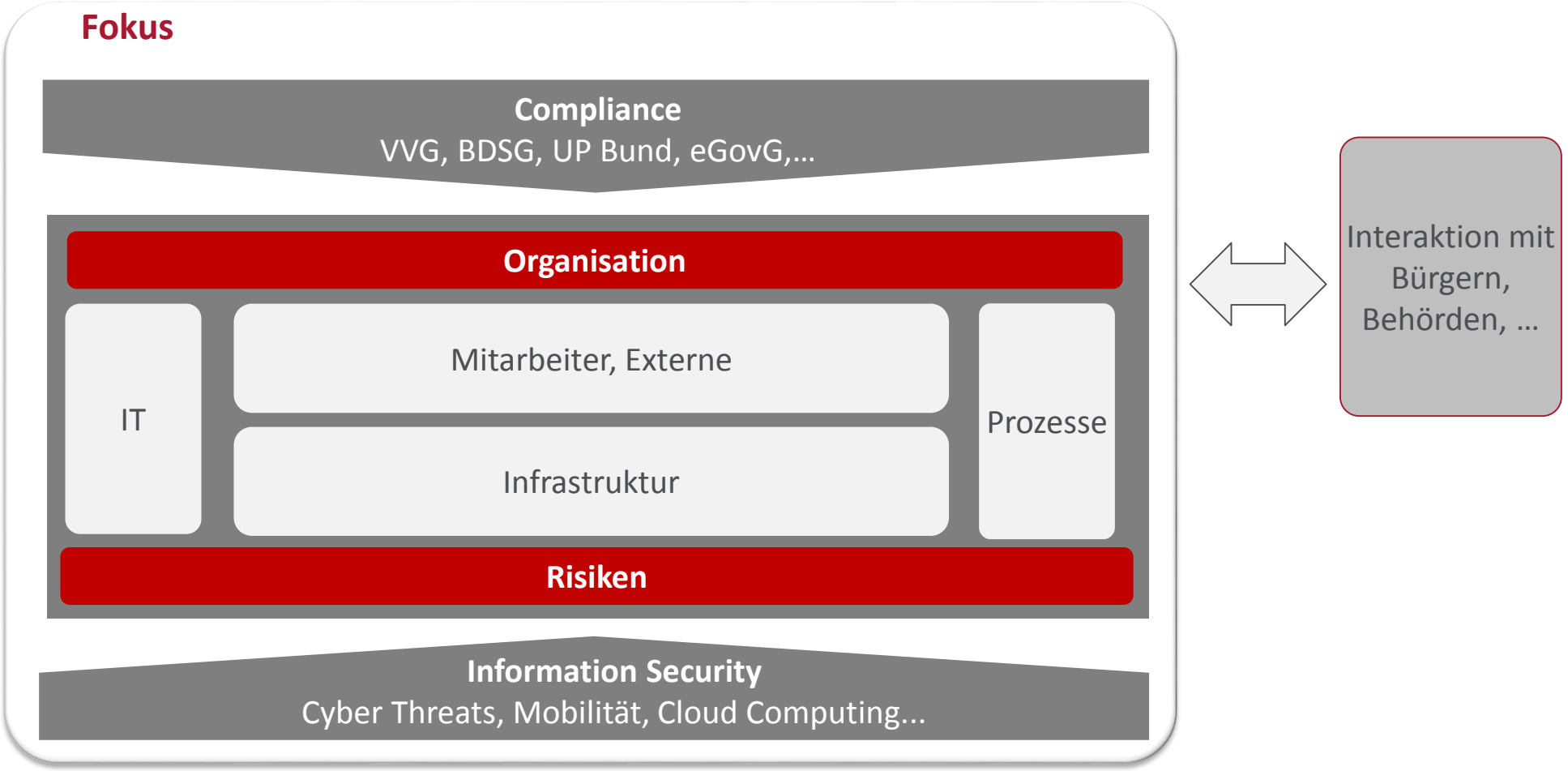
Herausforderungen

- Neue regulatorische Anforderungen
  - Gesetze, Verordnungen (VVG, BDSG, IT-SiG, eGovG, IFG…)
  - Prozess- und Verhaltenskodizes
- Personal-und Changemanagement
  - Personalabbau wegen Umstrukturierung oder IT-Konsolidierung
  - Ausscheiden von Mitarbeitern
  - Kompetenzaufbau, Kompetenzvermittlung
  - Rollen und Verantwortlichkeiten

- Adaptierung der Cybersicherheitsstrategie des Bundes, Abgleich mit eigenem Leitbild
- Information Security
  - Etablieren einer Information Security Policy und Standards (BSI-100)
  - Verifizierung von Risiken
  - Kontrolle und Implementierung von IS-Maßnahmen
  - Test Business Continuity Plan
  - Erreichen von Ende-zu-Ende Information Security
- Pflicht zur Rechenschaft
- Transparente Arbeit

Fokus von Information Security Governance

Die Ziele von Information Security Governance sind die Unterstützung der Behördenstrategie, Nutzengenerierung durch Management von Ressourcen, Wissenserweiterung, Risikomanagement, Krisenmanagement und Optimierung der Information Security.



BearingPoint

Modulare Lösungsansätze zum Erreichen von Information Security Governance

Jedes Thema unterstützt in seiner spezifischen Ausrichtung Information Security Governance.

Organisation & Changemanagement

- Definition von Rollen und Verantwortlichkeiten
- Rollen und Verantwortlichkeiten
- Stakeholderanalyse
- Differenzierte Awarenessmaßnahmen

IS - Strategie

- Entwicklung einer IS-Strategie
- Abgleich mit der Business Strategie und Zielbildern
- Auswahl geeigneter Standards

Risikomanagement

- Aufbau eines Risikomanagements
  - Erfassung relevanter Bedrohungen und Schwachstellen
  - Empfehlen von Risikomanage-mententscheidungen
- Auswahl Informationssicherheits-management und geeigneter IS-Maßnahmen

Personalmanagement

- Altersstrukturanalyse für IS-Stakeholder
- Kompetenzabgleich

IS Governance Fokusthemen

IS Betrieb

- Test BCM
- Test Krisenmanagement
- Test PDCA-Zyklus

Finanzen

- Ressourcenprüfung
- Ressourcensteuerung
- Investitionsplanung

Compliance

- Prüfung relevanter Gesetze, Verordnungen
- Prozess- und Verhaltenskodizes
- Benchmarking

Controlling, Reporting, Transparenz

- Definition von KPIs für alle kritischen Prozesse
- Etablierung von transparenten Reportingstrukturen
- Performance Management

BearingPoint

Unserer Value Proposition – Projektprofil als Beispiel

Bewährte Methode zur Beurteilung und Abgabe von Empfehlungen für Information Security Governance

Information Security Governance Review – Projekt Profil

- Ca. 50 TEUR
- 4 Wochen Dauer
- 2 Mitarbeiter plus ggf Spezialisten für funktionale Domänen
- 1 MA seitens des Kunden als Ressource
- Sponsorship: Behörden – und IT-Leitung

Genutzte Standards und Tools

- BearingPoints Governance Assessment Tool
- Eingesetzte Standards
  - COBIT
  - COSO
  - ISO 2700x
  - ITIL

- Bewertet die Ausrichtung von Business und Technologie-Strategien und beurteilt die Organisationsstruktur der Informationssicherheit
- Bietet eine High-Level-Überprüfung der Information Security Governance anhand funktionaler Domänen wie IT, Prozesse, Infrastruktur, Mitarbeiter
- Identifiziert Schwachstellen, aber auch Chancen
- Priorisiert und empfiehlt Effizienzsteigerungsmöglichkeiten

Für Information Security Governance gibt es entscheidende Vorteile

Nutzen

- **klare Positionierung der IS** im Gesamtspektrum der Leistungskomponenten und Ressourcen,
- **Fokussierung** auf hochpriorisierte Themen und **optimale Ausrichtung** der IT durch abgestimmte Prozeduren für IT-Entscheidungen und Priorisierungen.
- **hohe Transparenz** über alle Aktivitäten und Status im Bereich des Security-, IT Compliance -und OpRisk Managements
- **permanente Information** über alle Veränderungen und Verbesserungen über den PDCA Kreislauf
- **Optimierung der IT-Investitionen** durch Transparenz der geschäftskritischen Prozesse – Möglichkeit zur Konzentration auf Spitzenrisiken
- **Einsparung von ca. 30-50%** der internen und externen Kosten bei ISMS-Einführung / Betrieb sind möglich und ggf. **Reduzierung der Aufwendungen** für Zertifizierung/Rezertifizierung
- **Unternehmens- behördenweite und einheitliche Nachweisbarkeit der Compliance**
- **Imagegewinn** (bei Bürgern, Kunden, Lieferanten und Investoren)

Ihre Ansprechpartnerin:

BearingPoint

Caroline Neufert
Senior Manager
BearingPoint
Kurfürstendamm 207-208
10719 Berlin
Germany

T +49 30 88004 2230
F +49 30 88004 100
M +49 174 33 51 127

www.bearingpoint.com

caroline.neufert@bearingpoint.com

BearingPoint®