



AUTOMOTIVE

INFOKOM

**VERKEHR &
UMWELT**

LUFTFAHRT

RAUMFAHRT

**VERTEIDIGUNG &
SICHERHEIT**

Perspektive über das Spannungsfeld öffentliche Sicherheit und Informationssicherheit

Security Forum 2010 der Fachhochschule Brandenburg

Christian Köhler

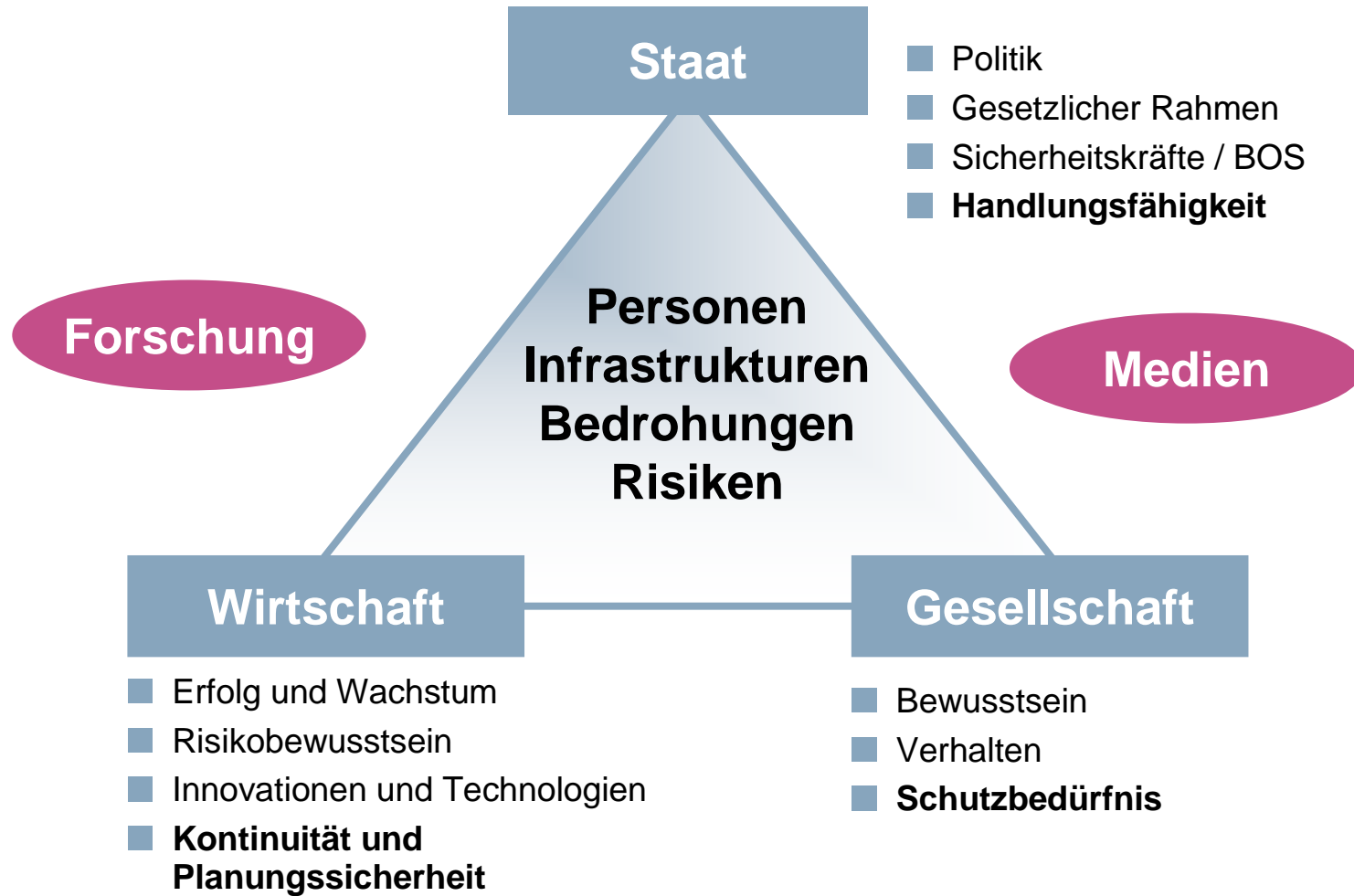
Brandenburg, 21.01.2010

Öffentliche Sicherheit und Informationssicherheit



- Ø **Öffentliche Sicherheit** (auch Innere Sicherheit oder Public Security) befaßt sich mit Fragen des effizienten Einsatzes und der Harmonisierung von Informations- und Kommunikationstechnologien, Netzwerken sowie Infrastrukturen der beteiligten Behörden und Organisationen.
- Ø Als **Informationssicherheit** bezeichnet man Eigenschaften von informationsverarbeitenden Systemen, welche Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen.

Die „Security Key Player“ und ihre Sichtweisen



∅ umfassende Sicherheit kann nur gewährleistet werden, wenn alle Partner ihre Verantwortung wahrnehmen.

Spannungsfeld Öffentliche Sicherheit vs. Informationssicherheit

- Ø **Öffentliche Sicherheit** sollte die Balance halten zwischen Bürgerrechten und Freiheiten (Datenschutz, Informationssicherheit, etc.) auf der einen Seite und Eingriffsrechten und Präventivmaßnahmen des Staates (Telefonüberwachung, Hausdurchsuchung usw.) auf der anderen Seite.
- Ø Angesichts der vielfältigen und wachsenden Gefährdungspotentiale und der steigenden Abhängigkeit stellen sich hinsichtlich der **Informationssicherheit und des Datenschutzes** die Fragen, wie, wo und mit welchen Mitteln mehr Sicherheit erreicht werden kann.
- Ø Die Projekte und Aktivitäten in diesen Themenfeldern beinhalten auch ein riesiges **Spannungsfeld von Budgets und technischen Leistungsfähigkeiten!**

...nur einige Trends im Bereich öffentliche Sicherheit



- Polizeiliche Informations- und Kommunikationssysteme werden mit umfangreichen Budgets ausgestattet.
- Schutz kritischer Infrastrukturen wird in EU- und nationalen Programmen geplant und gewährleistet.
- Deutsche Polizeikräfte sind verstärkt in Friedensmissionen und bilateralen Projekten eingesetzt.
- Bevölkerungsschutz und Katastrophenhilfe wird gestärkt.
- Sichere IT-Infrastrukturen und –Produkte sind ein Kernbestandteil nationaler IT-Strategien.
- Im Bereich Sichere Identitäten bietet Deutschland Spitzentechnologien.

...nur einige Trends der IT-Sicherheit



Steigende Quantität der Bedrohungslage:

- Die Anzahl neuer Schadprogramme (Malware) stieg zwischen 2007 und 2008 um 570 %.
- Eine kontinuierliche Zunahme der Anzahl erkannter Schwachstellen in IT-Produkten ist festzustellen (kurze Entwicklungszyklen, Heterogenität)
- Komplexität der (IKT-)Infrastrukturen und deren Abhängigkeiten nehmen zu

Veränderte Täterstrukturen:

- Trend zu arbeitsteiliger Kriminalität mit regelmäßiger Veränderung der Serverstandorte
- Das Opfer als Mittäter (z. B. durch Bot-Netze; Zombie-PCs)

In Zukunft Sicherheit bei beschleunigtem Innovationsmanagement?!



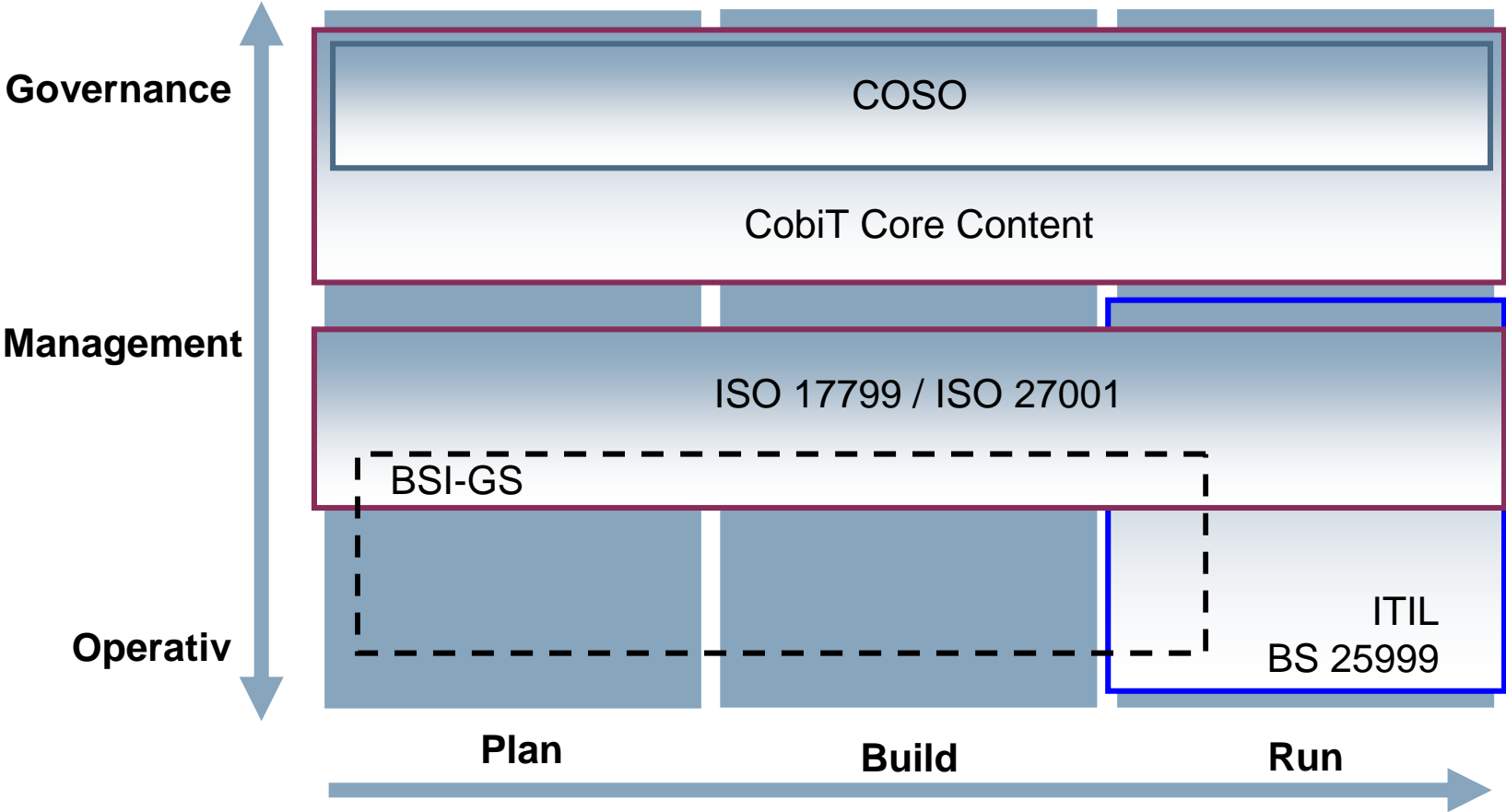
Herausforderungen im Bereich IKT

- Geschäftsprozesse und Infrastrukturen für ‚lebensnotwendige Bereiche‘ sind von Informations- und Kommunikationstechnik (IKT) kritisch abhängig. Eine Verstärkung dieser Abhängigkeiten durch Vernetzung von Marktteilnehmern ist mit singulären Risiko- und Sicherheitsmanagementsystemen nur eingegrenzt beherrschbar.
- Energie und Telekommunikation sowie Mobilität wachsen zusammen und..
- .. die fortschreitende Allgegenwärtigkeit von IKT, Wirtschaftsspionage und Krisenherde sowie die Miniaturisierung von Consumer Produkten verstärken den Trend.
- Die Informationen und Dienste der digitalen Welt sind bereits hochmobil an jedem beliebigen Ort abrufbar, Anwender sind nur wenig im Umgang damit sensibilisiert.
- Die permanent aufrechtzuhaltende Informationssicherheit ist den Innovationszyklen der IKT vorausseilend, in immer kürzeren Zeitabständen zu planen und sicherzustellen (Security Convergence Roadmap).
- Intelligente Systeme und Gegenstände beherrschen den Alltag. Die Funktionalität ist unüberschaubar und die Herkunft aus aller Welt.

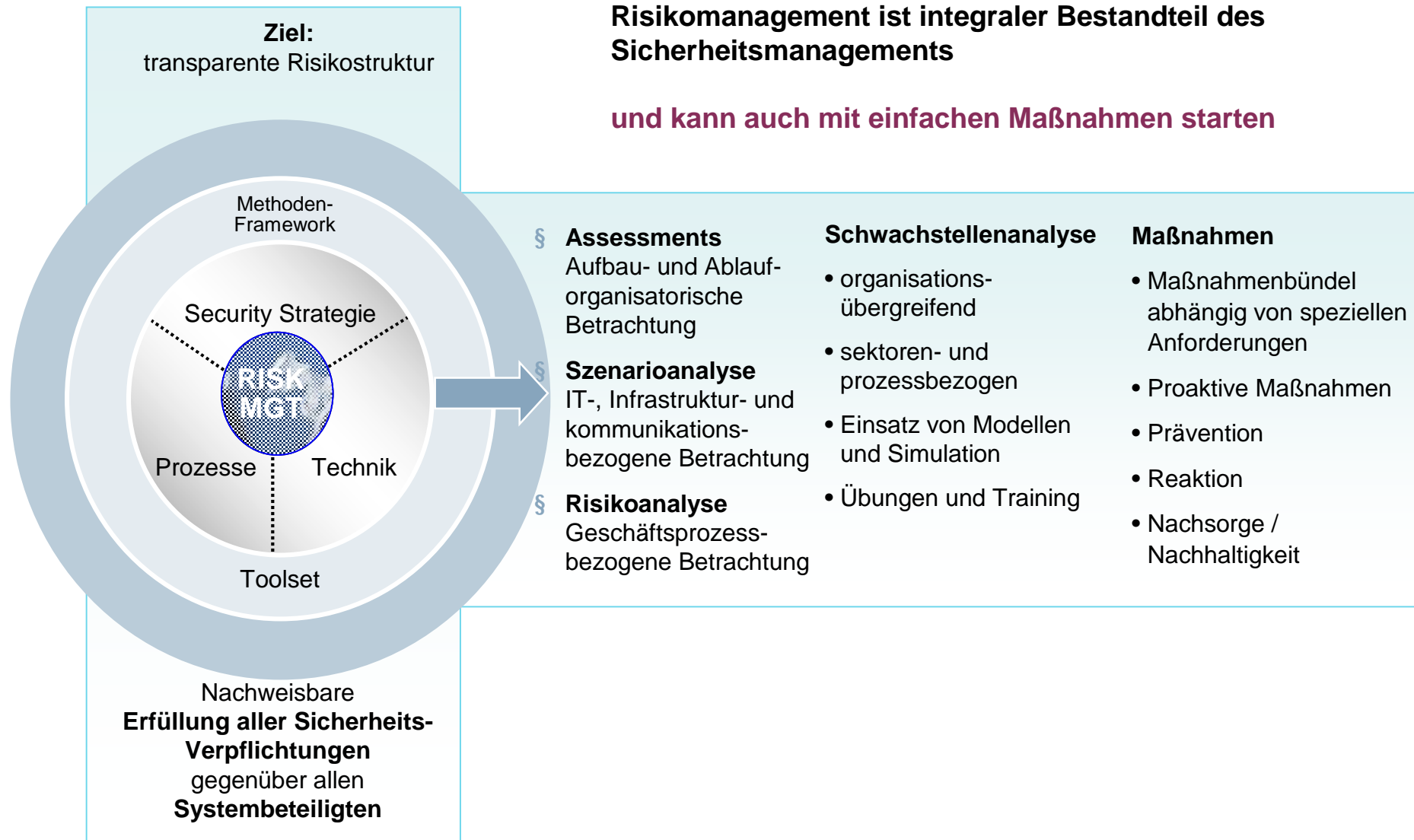
Umfassende Sicherheitsvorsorge ist einfach..



Verbesserung der Sicherheit und Wirtschaftlichkeit der IKT durch Transparenz, Aktualität und Messbarkeit.



Risikomanagement als Ansatz für effiziente Prävention



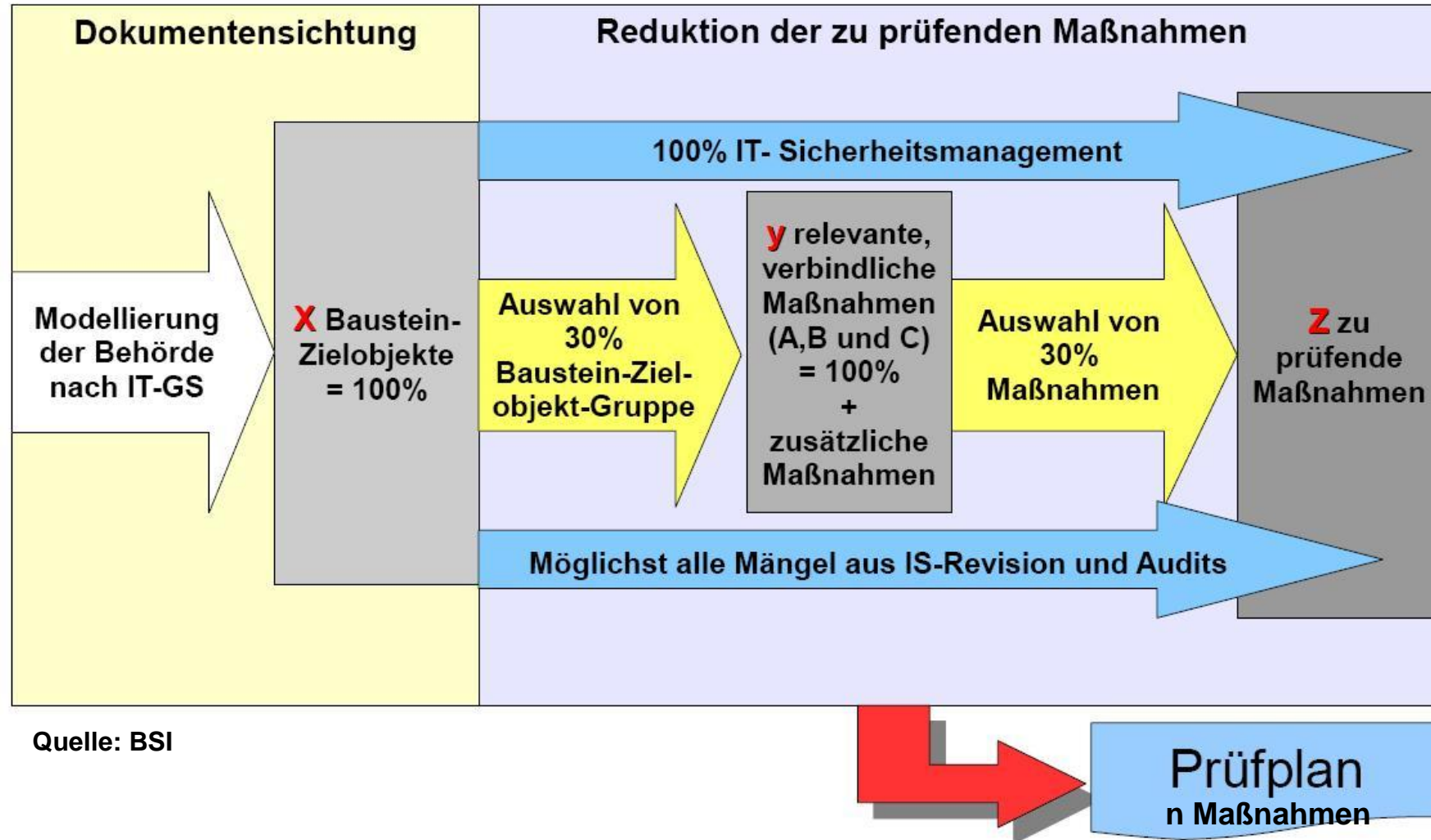
Projekt: IT-Sicherheitsleitfaden für Kommunen in Brandenburg



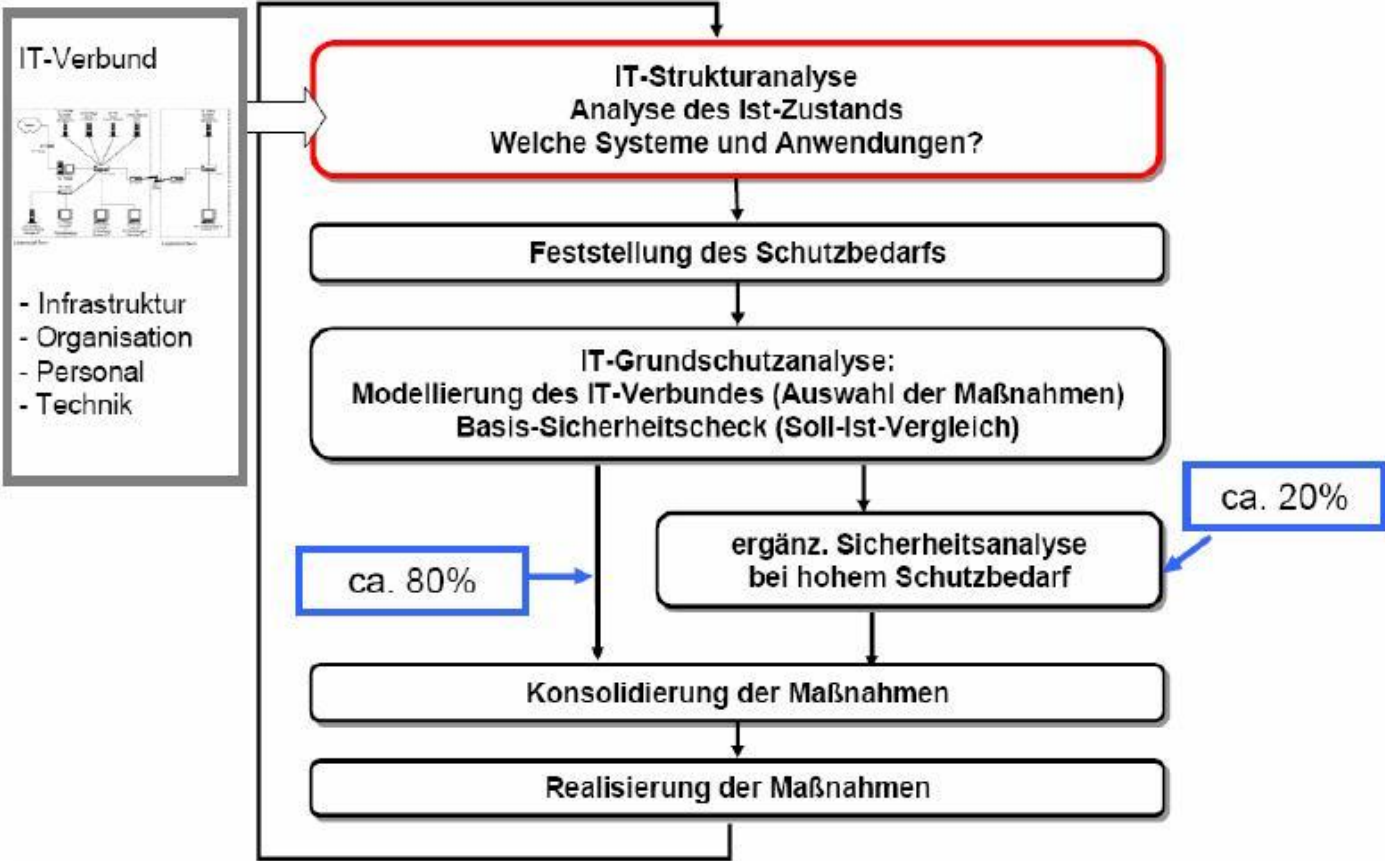
- Baustein A:** Einführungsworkshop IT-Sicherheit nach IT-Grundschutz des BSI
- Baustein B:** IT-Sicherheitscheck und IS-Kurzrevison
- Sicherheitsüberblick durch eine IS-Kurzrevison
 - Umfassender IT-Sicherheitscheck
 - Beratung bei der Erstellung eines IT-Sicherheitskonzeptes nach IT-Grundschutz des BSI:
 - Ø Beratung bei der Durchführung einer IT-Strukturanalyse
 - Ø Beratung bei der Durchführung einer Schutzbedarfsfeststellung
 - Ø Beratung bei der Modellierung und des Basissicherheitschecks
 - Ø Beratung bei der ergänzenden Sicherheitsanalyse und Risikoanalyse
 - Ø Erstellung eines Realisierungsplanes für die sich aus dem Konzept ergebenden IT-Sicherheitsmaßnahmen
 - Ø Bereitstellung von Hilfsmittel
- Baustein C:** Schulung und Ausbildung
- Ø TISP – Das europäische Zertifikat
 - Ø iSECMA – International Certified Professional for IT-Security Management

Weitere Informationen unter <http://www.sesambb.de/>

Erstellung eines risikoorientierten Prüfplans



IT-Strukturanalyse für ausgewählte Fachverfahren



Ihre Ansprechpartner



IABG mbH

Christian Köhler | Leiter Key Account Management InfoKom

Alt Moabit 94 | 10559 Berlin | ckoehler@iabg.de

Tel: ++49 30 / 293991-50 | Fax: ++49 30 / 293991-66