Gesellschaft
für Informatik

Neuerungen und Anpassungen rund um ISO/IEC 27001:2013

Erfahrungsbericht eines Auditors

Uwe Rühl

Gesellschaft
für Informatik

Kurz zu meiner Person

bsi.

- Externer Client Manager (Lead Auditor) für ISO/IEC 27001, ISO 22301 und integrierte Managementsysteme

qSk!lls
innovation through education

- Trainer für Informationssicherheitsmanagement und Business-Continuity-Management

RÜHLCONSULTING

- Geschäftsführer eines auf ISMS und BCMS fokussierten Beratungshauses

Gesellschaft
für Informatik

Erfahrungen mit ISO/IEC 27001:2013 - Agenda

Agenda:

- Grundsätzliche Herausforderungen im Umgang mit Normrevisionen
- Besondere Herausforderungen der ISO/IEC 27001:2013
- Fazit

Gesellschaft
für Informatik

Erfahrungen mit ISO/IEC 27001:2013 - Agenda

Agenda:

- Grundsätzliche Herausforderungen im Umgang mit Normrevisionen
- Besondere Herausforderungen der ISO/IEC 27001:2013
- Fazit

Gesellschaft
für Informatik

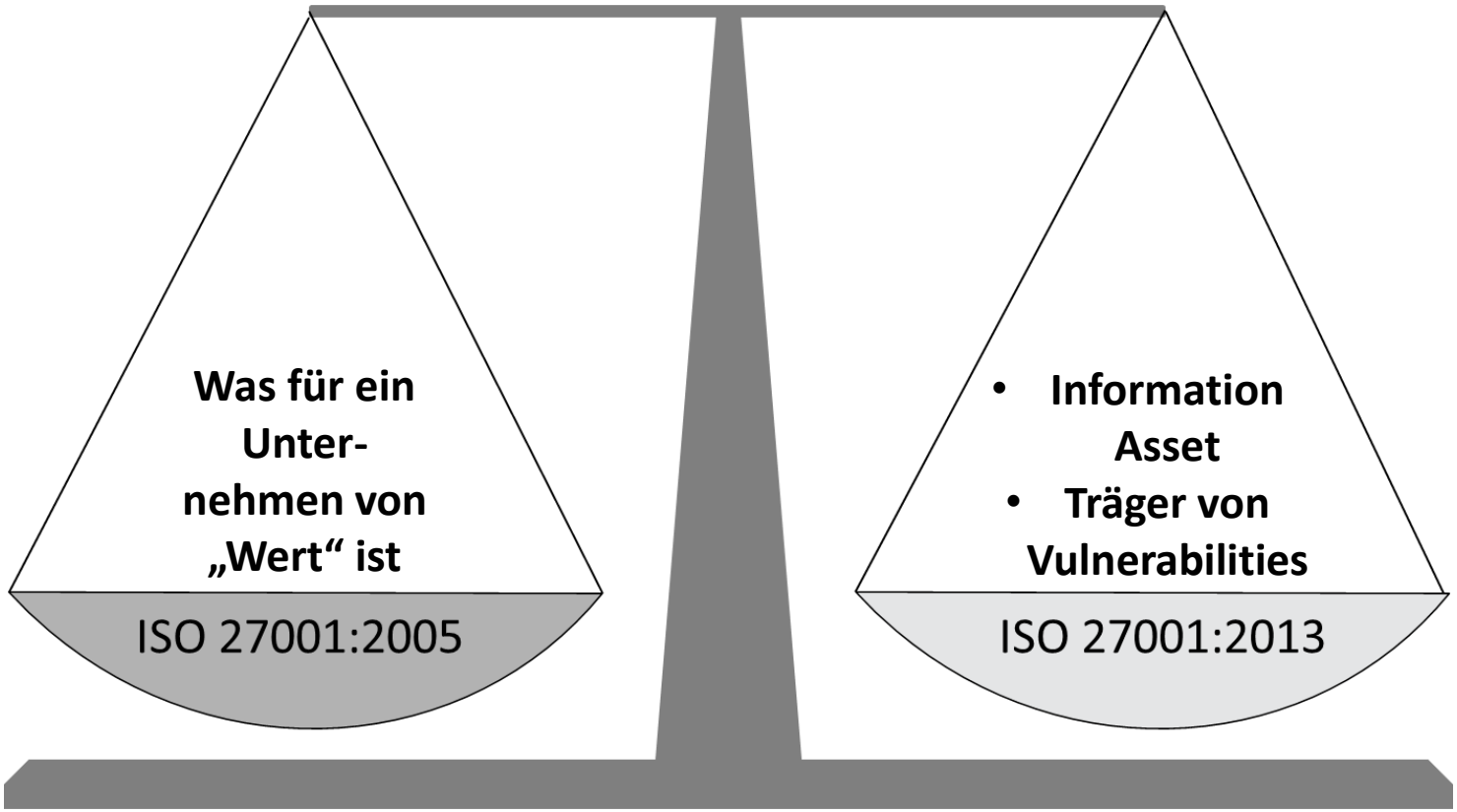
Neuer Annex SL der ISO

Kap.	Bezeichnung	Bemerkung
0	Introduction	Einführung zum Zweck der Norm
1	Scope	Anwendungsbereich der Norm selbst
2	Normative references	Verweise auf referenzierte Normen
3	Terms and definitions	Definition der Begriffe in dieser Norm
4	Context of the organization	Internal & external issues, Scope des MS
5	Leadership	Top Management commitment, Policy, Rollen
6	Planning	Risk and opportunities
7	Support	Ressourcen, fachliche Kompetenz, etc.
8	Operation	Umsetzung der Norm
9	Performance evaluation	Bewertung von Performance und Effectiveness
10	Improvement	Corrective Action, Continual improvement

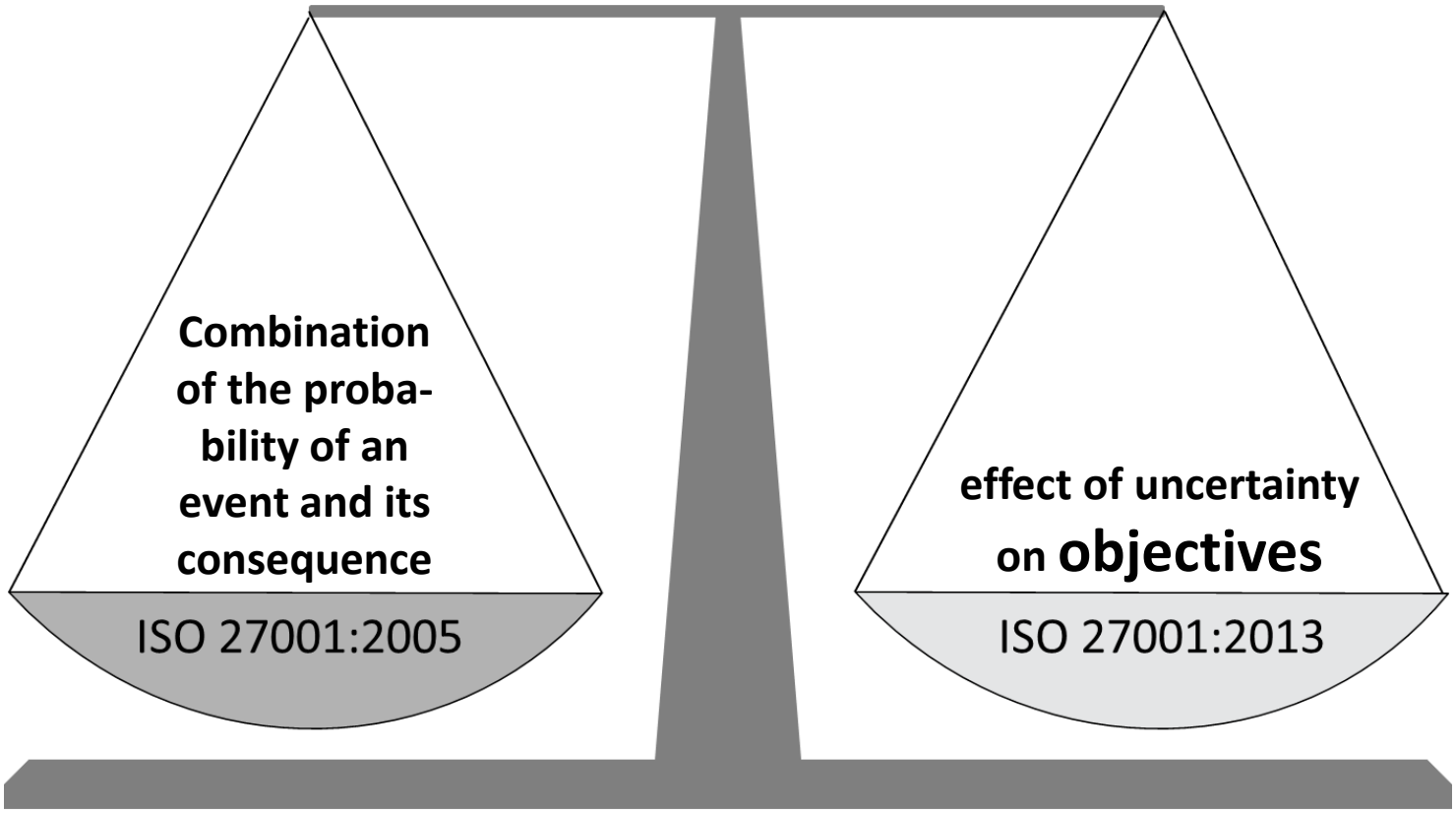

Interested Parties
NEEDS & EXPECTATIOS
Interested Parties
MANAGED INF SECURITY
Context of the organization
Improvement
Performance Evaluation
Leadership
Planning
Support
Operation
4
10
9
5
8
6
7
Annex A

Gesellschaft
für Informatik

Begriff Asset – Was verstehen wir darunter?



Begriff Risiko – Abhängig von Zielen!



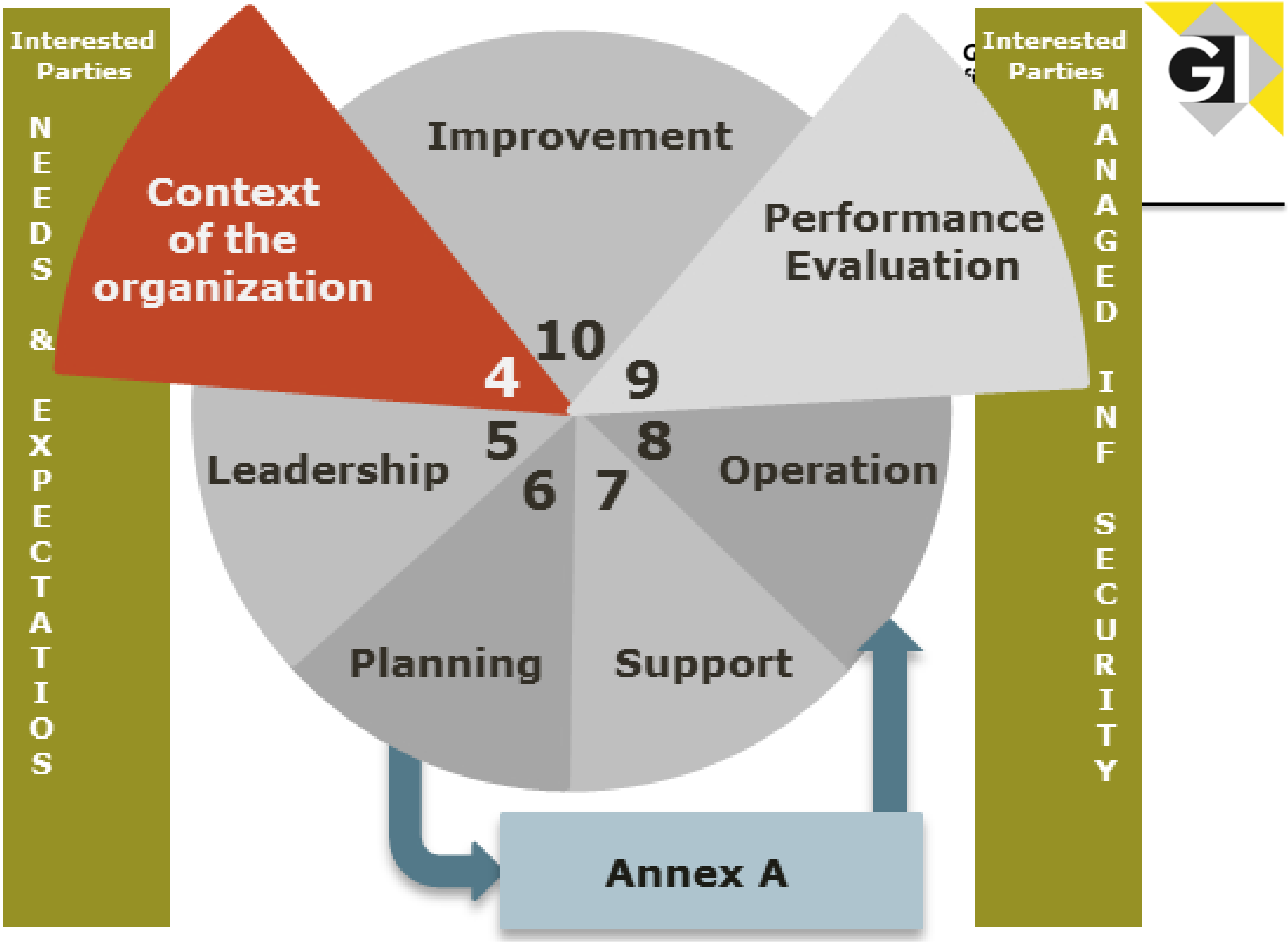
© Gesellschaft für Informatik e.V. (GI)

Gesellschaft
für Informatik

Erfahrungen mit ISO/IEC 27001:2013 - Agenda

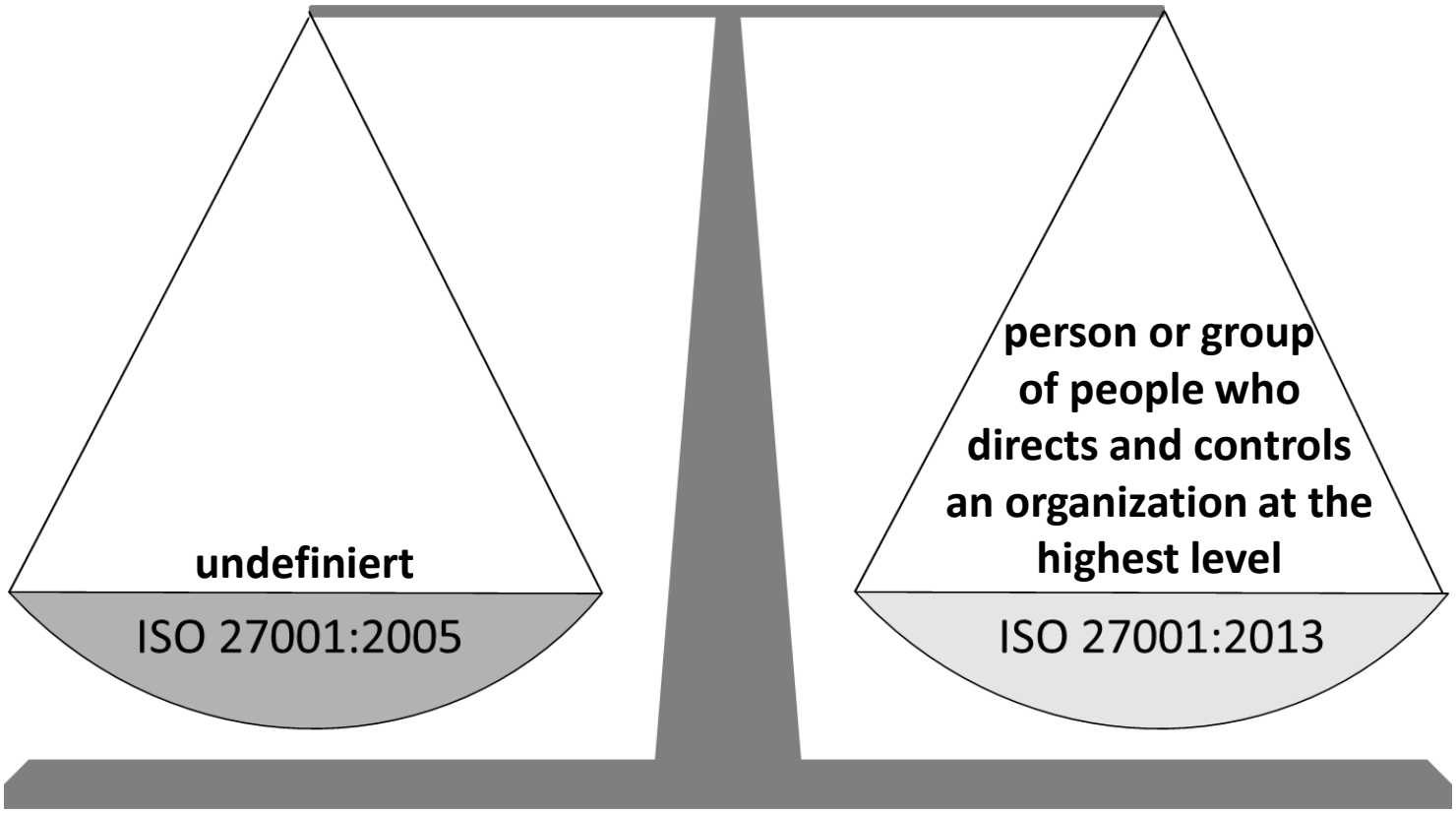
Agenda:

- Grundsätzliche Herausforderungen im Umgang mit Normrevisionen
- Besondere Herausforderungen der ISO/IEC 27001:2013
- Fazit


Interested Parties
NEEDS & EXPECTATIOS
Context of the organization
Improvement
Performance Evaluation
4
10
9
5
8
Leadership
6
7
Operation
Planning
Support
Annex A
Interested Parties
MANAGED INF SECURITY

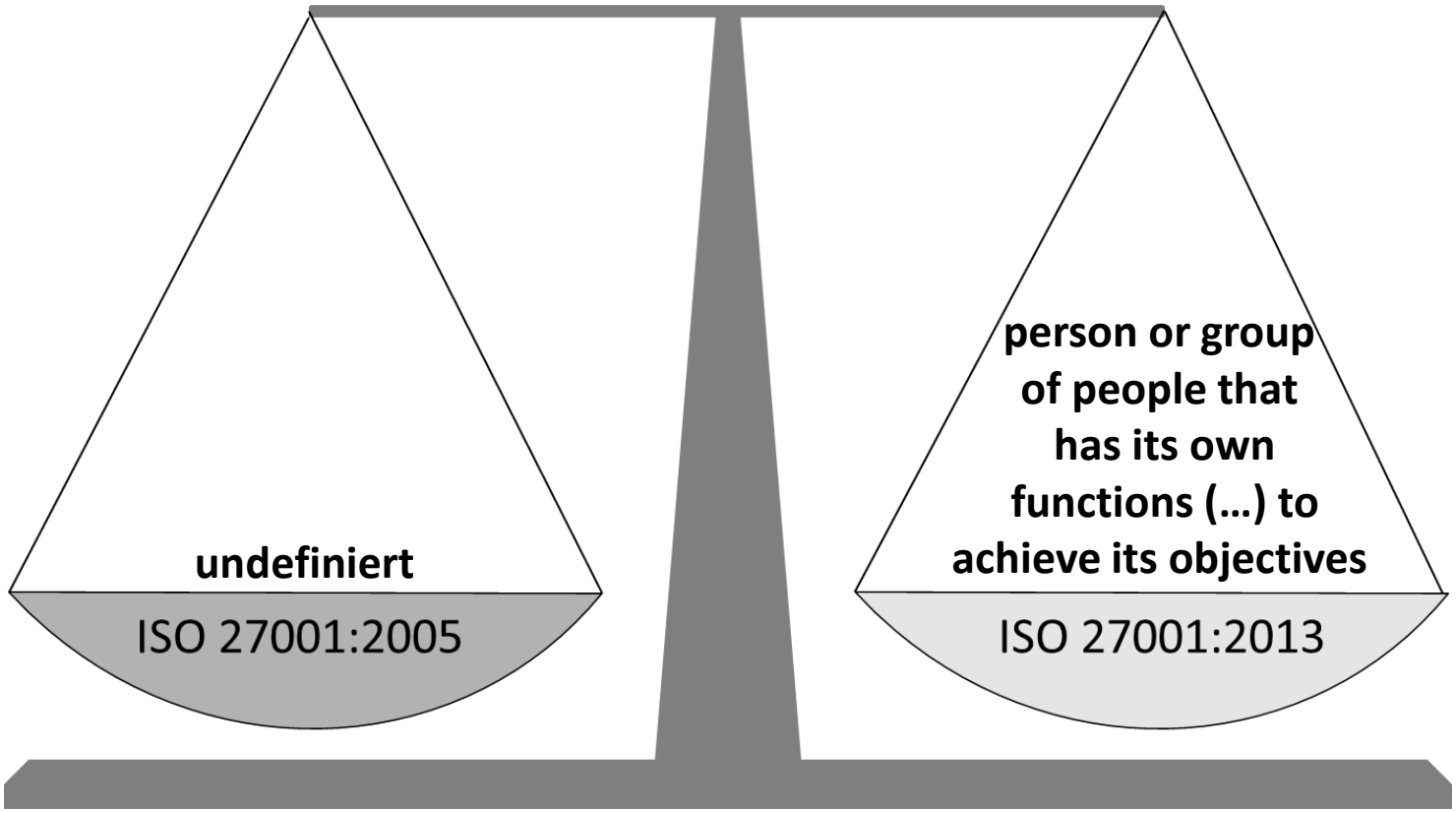
Gesellschaft
für Informatik

Management vs. Top Management



Gesellschaft
für Informatik

Scope – was ist eine Organisation?



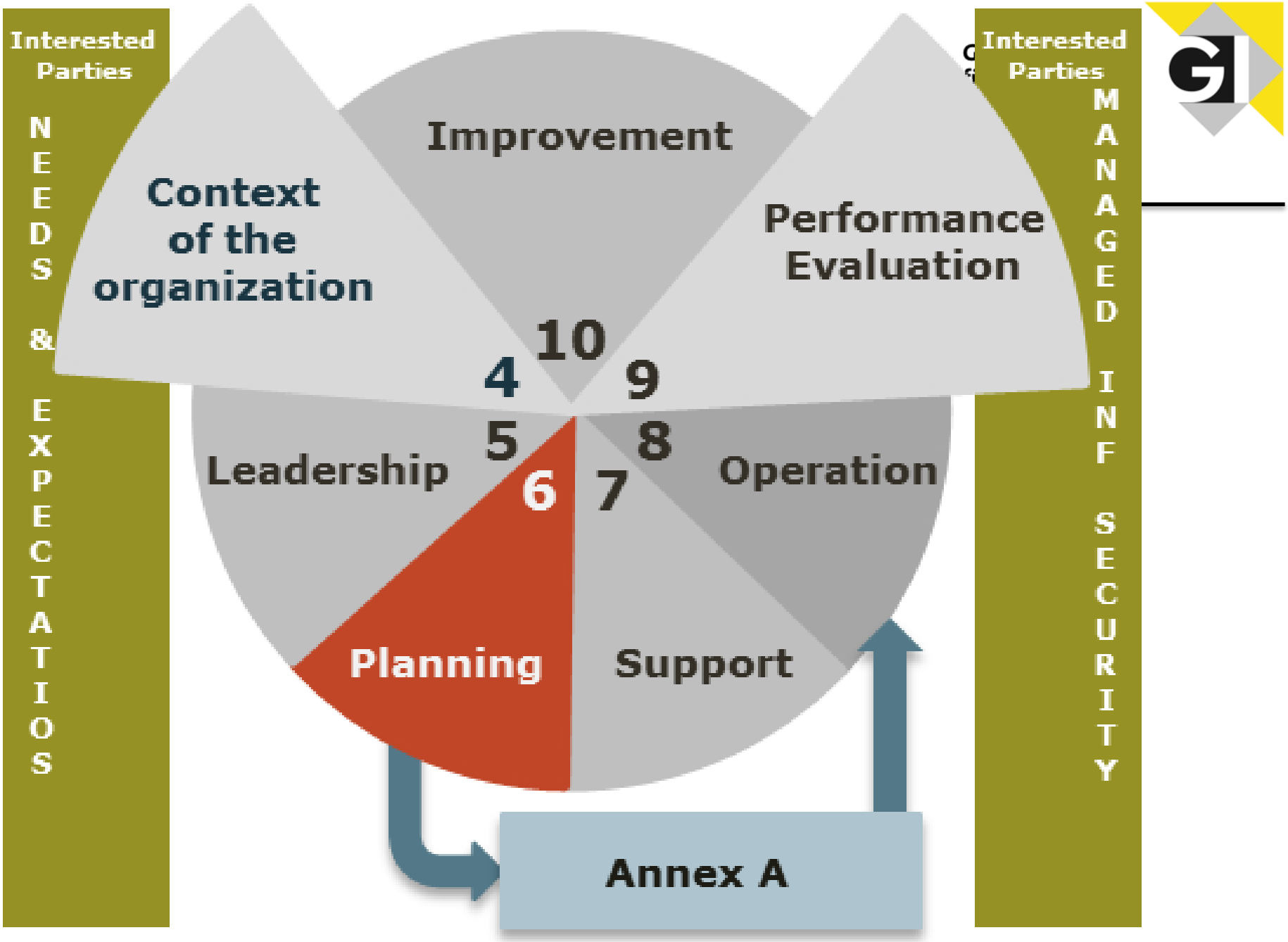
Knackpunkte

- Identifikation von ‚internal' und ‚external Issues' häufig nur oberflächlich
  - siehe hierzu bitte ISO/IEC 27000:2014 2.27 und 2.42
- Identifikation von Interested Parties und ‚Needs and Expectations' häufig unzureichend
  - Interested parties = Stakeholder: ‚person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity'
- Festlegung des Anwendungsbereiches häufig unzureichend
  - 4.3: , The organization shall determine the boundaries and applicability of the information security management system to establish its scope.'


Interested Parties
NEEDS & EXPECTATIOS
Interested Parties
MANAGED INF SECURITY
Context of the organization
Improvement
Performance Evaluation
Leadership
Operation
Planning
Support
4
10
9
5
8
6
7
Annex A

Knackpunkte

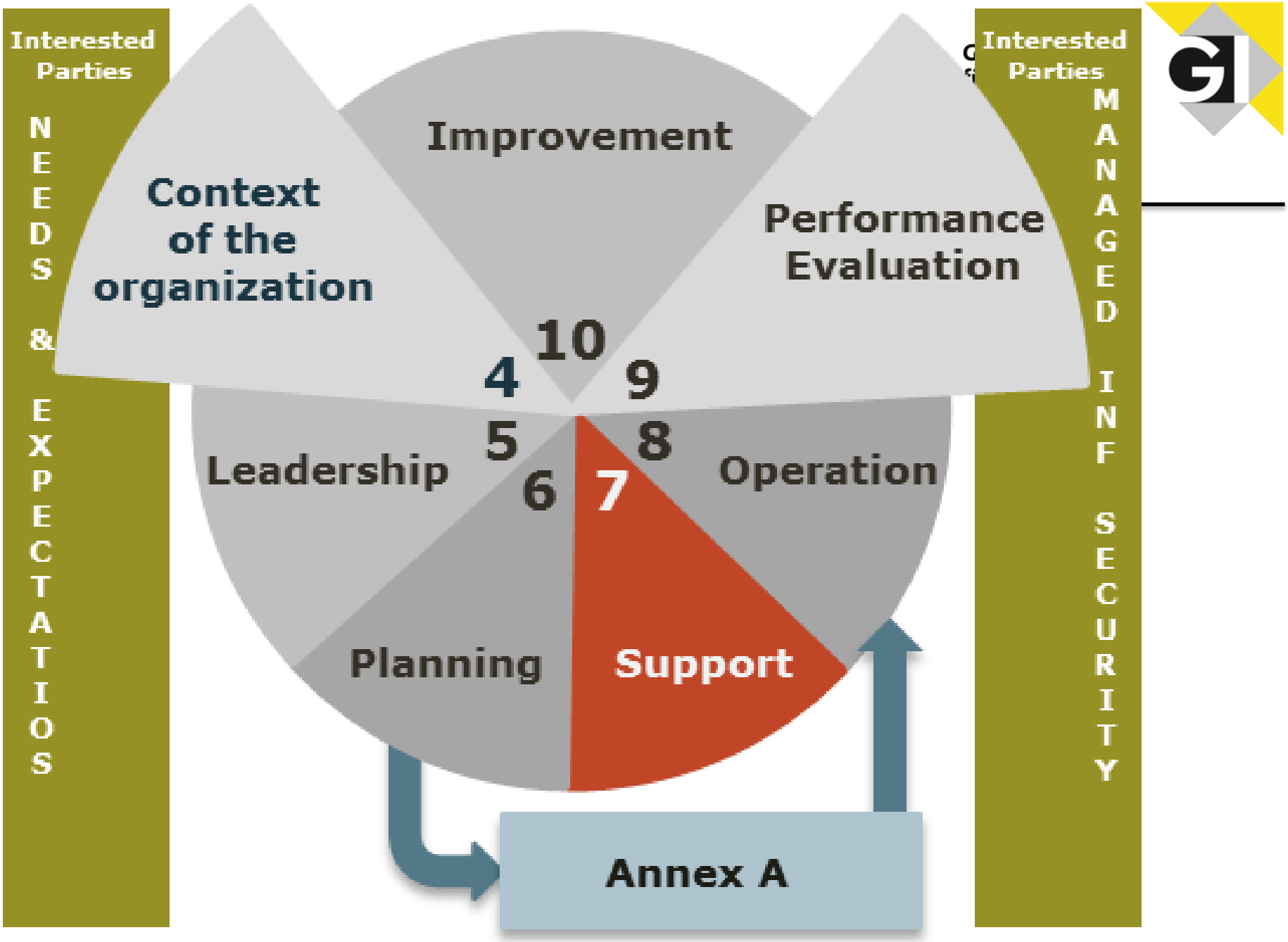
- Information Security Policy 5.2:
  - includes information security objectives (see 6.2) or provides the framework for setting information security objectives
- Information Security Objectives 6.2:
  - The organization shall establish information security objectives at relevant functions and levels.
  - Information security objectives shall:
    - a) be consistent with the information security policy;
    - b) be measurable (if **practicable**);


Interested Parties
NEEDS & EXPECTATIOS
Interested Parties
MANAGED INF SECURITY
Context of the organization
Improvement
Performance Evaluation
Leadership
Planning
Support
Operation
4
10
9
5
6
7
8
Annex A

Gesellschaft
für Informatik

Knackpunkte und neue Freiheiten

- Risk and opportunities 6.1.1
  - a) ensure the **information security management system** can achieve its intended outcome(s);
- Information Security Risk Assessment 6.1.2
  - apply the information security risk assessment process to identify risks associated with (…) **information** within the scope (…);
- Information Security Risk Treatment 6.1.3
  - b) Note: Organizations can design controls as required, or identify them from **any source → diese kann auch ISO/IEC 27001:2005 sein!**
  - obtain **risk owners'** approval of the information security risk treatment plan and acceptance of the residual information security risks.


Interested Parties
NEEDS & EXPECTATIOS
Interested Parties
MANAGED INF SECURITY
Context of the organization
Improvement
Performance Evaluation
Leadership
Planning
Support
Operation
Annex A
4
10
9
5
8
6
7

Gesellschaft
für Informatik

Knackpunkte

Communication 7.4

- manche Auditoren fordern hier eine ‚Kommunikationsmatrix' → diese ist in der Norm so nicht gefordert!

Documented Information 7.5

- kein dokumentiertes Verfahren mehr erforderlich, aber vermutlich sinnvoll
- insgesamt detaillierte Anforderungen


Interested Parties
NEEDS & EXPECTATIOS
Interested Parties
MANAGED INF SECURITY
Context of the organization
Improvement
Performance Evaluation
Leadership
Planning
Support
Operation
Annex A
4
5
6
7
8
9
10

Knackpunkte

| Operational planning and control 8.1

- The organization shall plan, implement and control the **processes needed** to meet information security requirements, (…) → Organisation legt fest, was erforderlich ist!
- The organization shall keep documented information to the extent necessary to have **confidence** that the processes have been carried out as planned.

Prüfpunkt: können Aktivitäten reproduziert werden? Sind Ergebnisse vergleichbar?

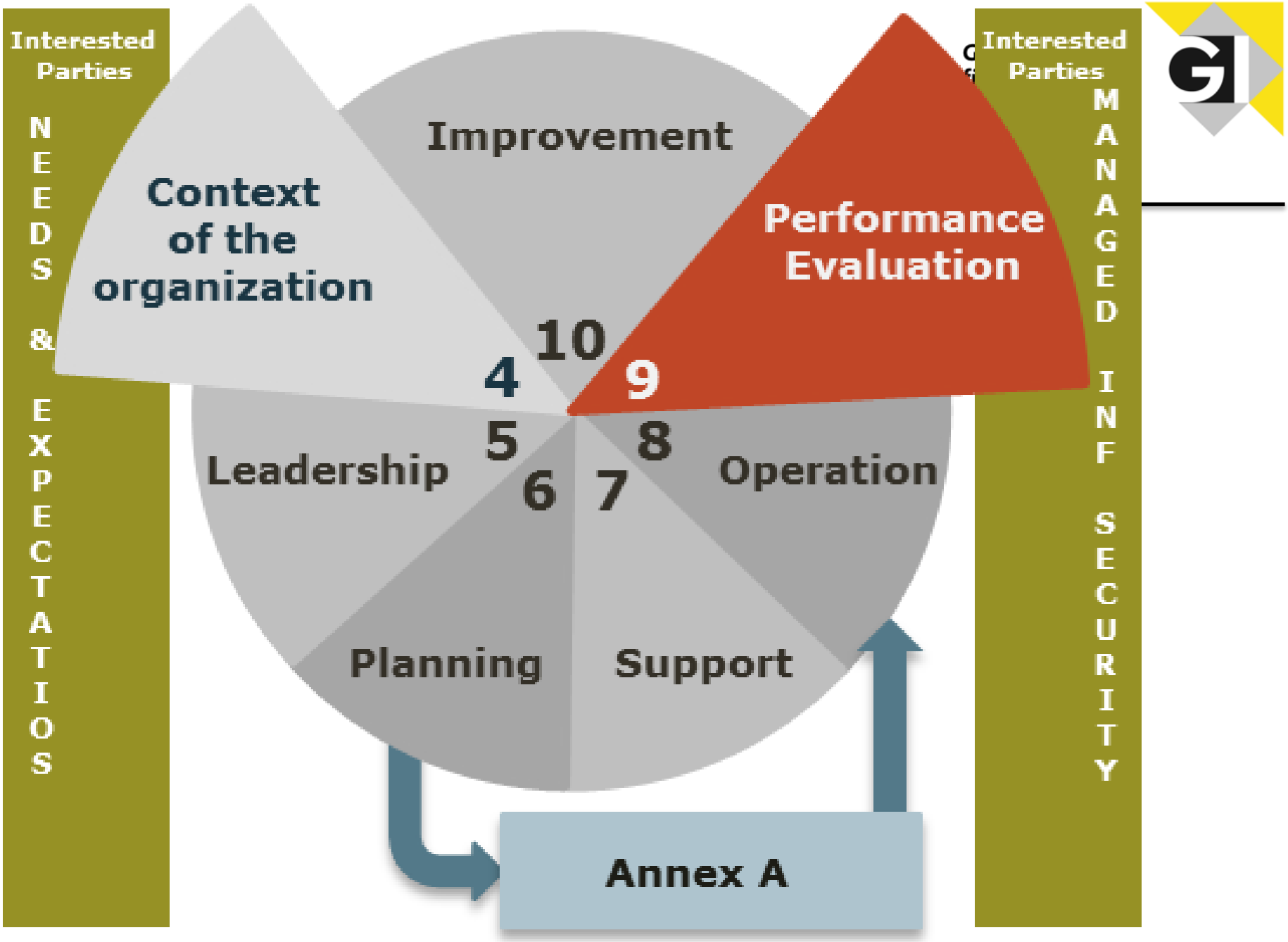
Gesellschaft
für Informatik

Knackpunkte

| Operational planning and control 8.1

- The organization shall control **planned changes**
  - Siehe auch A12.1.2 'Change Management' – hier sind Changes der Organisation, an Geschäftsprozessen oder informationsverarbeitenden Einrichtungen gemeint!
  - siehe auch A6.1.5 'Information Security in project management"
- (…) review the consequences of **unintended changes** (…)
  - Information Security Incident Management (siehe A16)
- The organization shall ensure that **outsourced processes** are determined and controlled
  - siehe A15 Supplier Relationships (**Knackpunkt A15.1.3 'Supply Chain'**)

Rechnen Sie damit, dass dies Kernpunkte des Audits sind!


Interested Parties
NEEDS & EXPECTATIONS
Interested Parties
MANAGED INF SECURITY
Context of the organization
Improvement
Performance Evaluation
Leadership
Operation
Planning
Support
Annex A
4
5
6
7
8
9
10

Gesellschaft
für Informatik

Knackpunkte und Freiheiten

- Monitoring, measurement, analysis and evaluation 9.1
  - The organization shall evaluate the information security **performance** and the **effectiveness** of the **information security management system**.
- (…) what needs to be monitored and measured, including information security **processes** and **controls**

Unternehmen legt fest, was unternommen wird, um die Wirksamkeit des gesamten Managementsystems zu bewerten!

Strenge Vorgabe der ISO/IEC 27001:2005 (“all controls or groups of controls”) gilt nicht mehr als Vorgabe!

Gesellschaft
für Informatik

Knackpunkte und Freiheiten

| Internal Audit 9.2 und Management Review 9.3

Kein dokumentiertes Verfahren mehr für Interne Audits

Auditprogramm muss Bedeutung der Prozesse und Ergebnisse vorhergehender Audits berücksichtigen!


Interested Parties
NEEDS & EXPECTATIONS
Interested Parties
MANAGED INF SECURITY
Context of the organization
Improvement
Performance Evaluation
Leadership
Planning
Support
Operation
Annex A
4
5
6
7
8
9
10

Gesellschaft
für Informatik

Knackpunkte

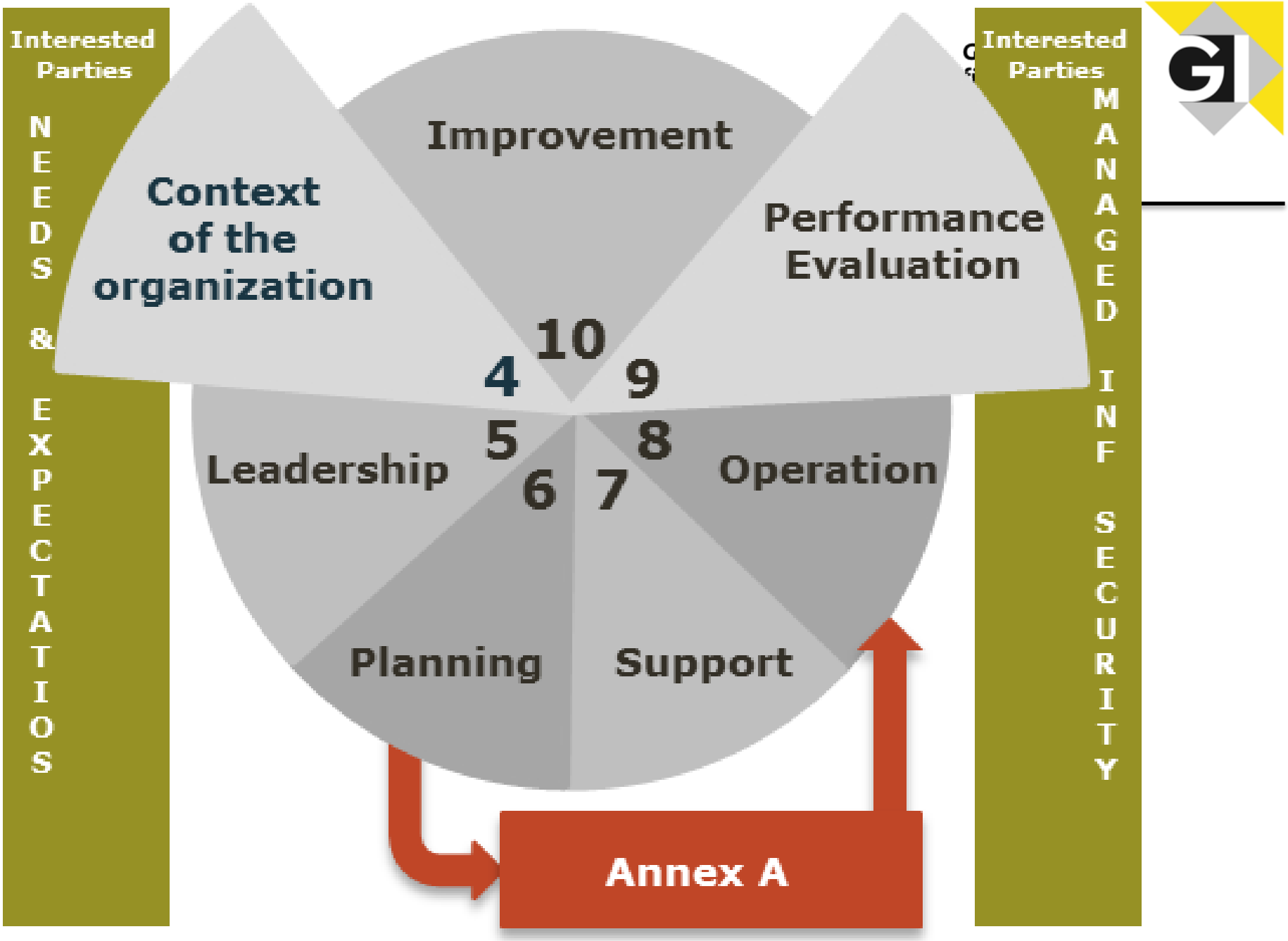
Nonconformity and corrective action 10.1

- **a)** react to the nonconformity
- **b)** evaluate the need for action to eliminate the causes of nonconformity

Kein dokumentiertes Verfahren mehr erforderlich!

Beachten Sie den Unterschied von

- Korrektur (10.1 a)
- Korrekturmaßnahme (10.1 b bis g)


Interested Parties
NEEDS & EXPECTATIOS
Interested Parties
MANAGED INF SECURITY
Context of the organization
Improvement
Performance Evaluation
Leadership
Operation
Planning
Support
4
10
9
5
8
6
7
Annex A

Gesellschaft
für Informatik

Schwerpunkte aus Anhang A

- A6.1.5 – Project Management
- A14.2 – Security in development and support processes
- A15 – Supplier relationships
- A17.2 - Redundancies

Gesellschaft
für Informatik

Erfahrungen mit ISO/IEC 27001:2013 - Agenda

Agenda:

- Grundsätzliche Herausforderungen im Umgang mit Normrevisionen
- Besondere Herausforderungen der ISO/IEC 27001:2013
- Fazit

Gesellschaft
für Informatik

Fazit aus Sicht des Auditors

- Norm hat eine höhere „Flugebene“ erreicht
  - Vorteile für das Unternehmen, Schwerpunkte festzulegen
  - Mehr Dynamik, bedingt durch den Business-Risk-Ansatz (‚**Internal and external Issues**‘)
  - Besondere Berücksichtigung von Zielen des ISMS
  - weniger formelle Dokumentationsanforderungen (‚**confidence**‘)
- Gleichzeit höhere Gewichtung auf
  - ausgelagerte Prozesse (A15 Supplier Relationship, ICT Supply Chain)
  - Development (A14.2)
  - Redundancies (A17.2)

Gesellschaft
für Informatik

Fazit aus Sicht des Auditors

- „Kalibrierung“ ist noch lange nicht abgeschlossen
- ISO/IEC 27006 noch in Working Draft, die etwas Hilfestellung für die Auditierung anbietet

- Erwarten Sie also durchaus ‚Dikussionen‘ mit Ihren Auditoren über die Auslegung der ISO/IEC 27001:2013!

Gesellschaft für Informatik

Wenn nach dem Vortrag noch Fragen auftauchen:

BSI Group Deutschland GmbH

Eastgate, Hanauer Landstraße 115

60314 Frankfurt

www.bsigroup.de

Uwe.Ruehl@RUEHLCONSULTING.de

Telefon 0911.47 75 28-30

...making excellence a habit.™