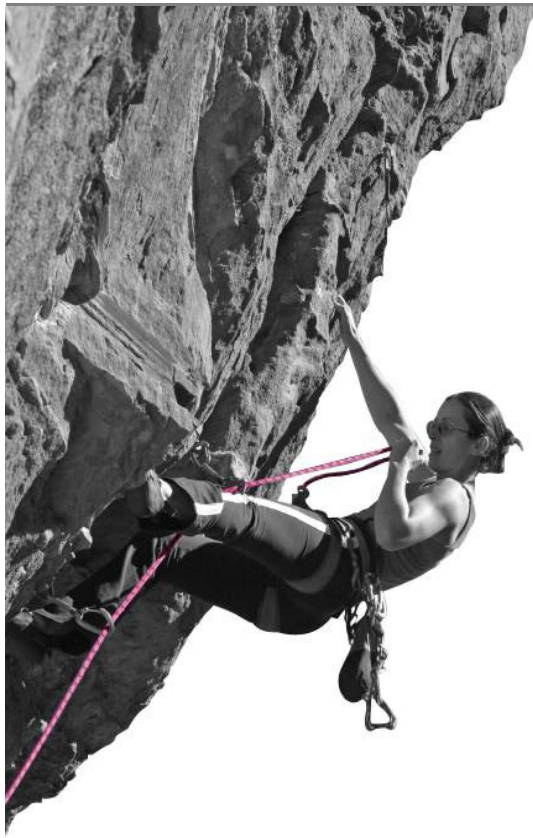
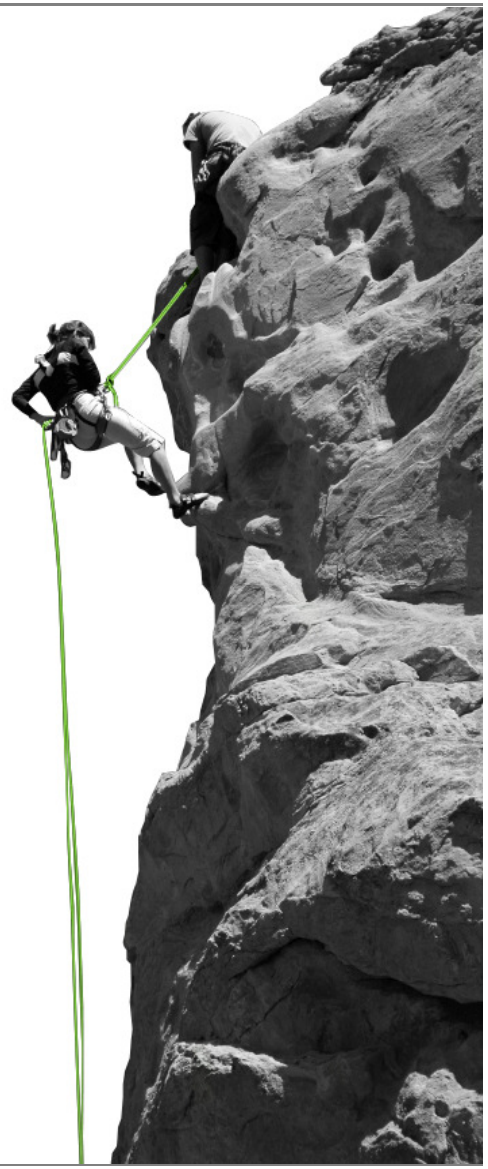


BT Germany
Vendor Security
GI-Fachgruppe SECMGT 11.11.11

Dr. Frank Kedziur
Head of Business Continuity, Security & Governance BT Germany

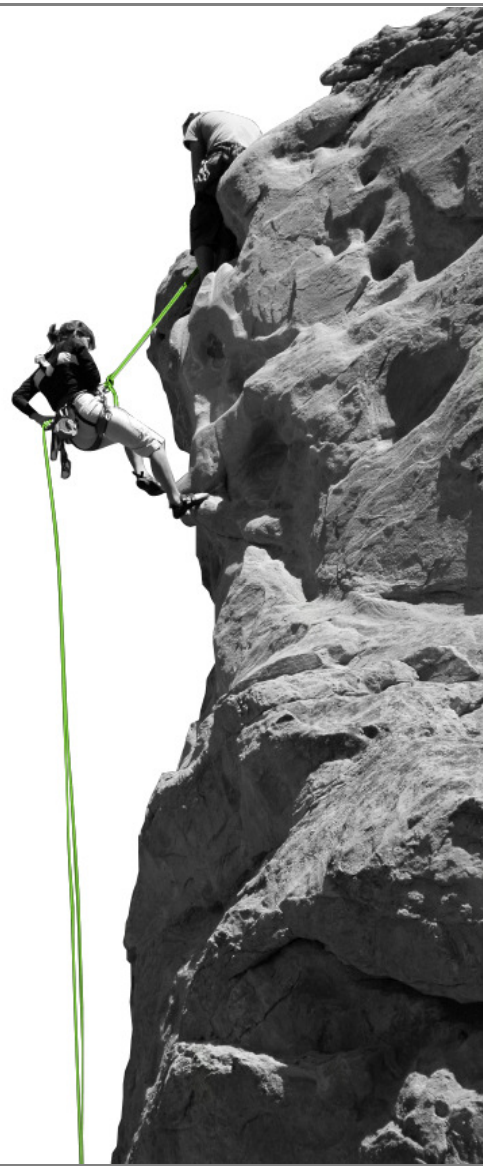
Agenda

- BT Zahlen und Fakten
- Portfolio
- Typische Ansätze für Vendor Security
  - Ansatz A: BT‘s Interne Sicherheit
  - Ansatz B: Ausschreibung über TPI
  - Ansatz C: gemeinsames ISMS
- FAQ zur Vendor Security



Agenda

- BT Zahlen und Fakten
- Portfolio
- Typische Ansätze für Vendor Security
  - Ansatz A: BT‘s Interne Sicherheit
  - Ansatz B: Ausschreibung über TPI
  - Ansatz C: gemeinsames ISMS
- FAQ zur Vendor Security



Globale Präsenz …

- …in Europa, Nord- und Südamerika sowie im asiatisch-pazifischen Raum
- Globales Netzwerk mit Serviceabdeckung in mehr als 170 Ländern der Erde
- Netzwerk-Kontrollzentren in Brüssel und Amsterdam, lokale Service- und Netzwerkmanagementzentren in 16 Ländern
- Rund 25.000 Mitarbeiter in über 50 Ländern
- Globales Account Management mit über 10.000 Mitarbeitern in Europa, den USA und Asien
- Erschließung neuer Märkte mit Fokus auf Südamerika und Südostasien
- Investitionen in neue Regionen wie Indien und China

… und lokale Stärke

- Flächendeckende Vertriebsorganisation mit sechs Geschäftsstellen
- Ein deutschlandweites, gemanagtes Netz
- City Fibre Networks in Frankfurt, München, Düsseldorf und Stuttgart
- 14 Rechenzentren, darunter Managed Hosting Data Centre
- Bandbreiten bis zu 10 Gbit/s
- Netzverfügbarkeit bis zu 99,999%
- Service-Desk-Team in Eschborn bei Frankfurt
- Umfassendes Know-how in ausgewählten Branchen

Zahlen und Fakten für das Geschäftsjahr 2010/11

	Umsatz in Mio.	Mitarbeiter
BT Group	20.076 £	92.600
BT Global Services	8.047 £	24.300
BT in Germany	794 €	1.300

Innovation als treibende Kraft bei BT

15 Milliarden € Investition in eines der weltweit innovativsten, globalen IP-Netzwerke – das 21st Century Network. Angeschlossen sind mehr als 140 Länder, insgesamt erreicht BT mehr als 170 Länder.

Größter F&E- Investor der europäischen Telekom-Branche

Innovation Scouts rund um den Globus

Allein in 2009/10 rund €3 Mrd. Investment in Netzwerkplattformen, Produkte und weitere Bereiche

Adastral Park: eines der weltweit führenden Forschungs- und Entwicklungs-zentren; 3.100 Wissenschaftler, gemeinsame Projekte mit über 25 Universitäten (u. a. MIT, Cambridge, Tsinghua)

Mehr als 8.000 Patente

21th Century Network

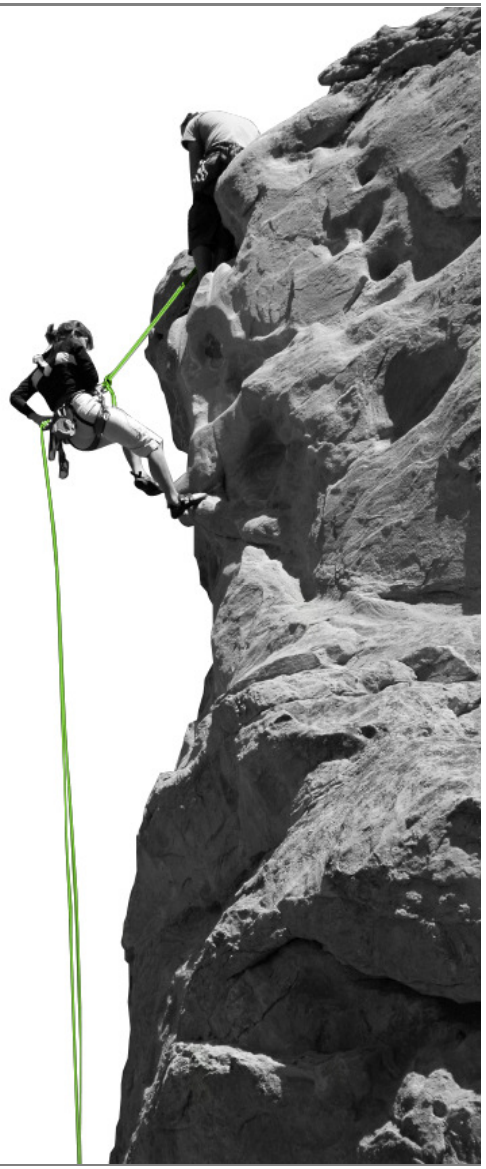
BT Unified Communications Video

BT Global Video Exchange

BT Virtual Data Centre

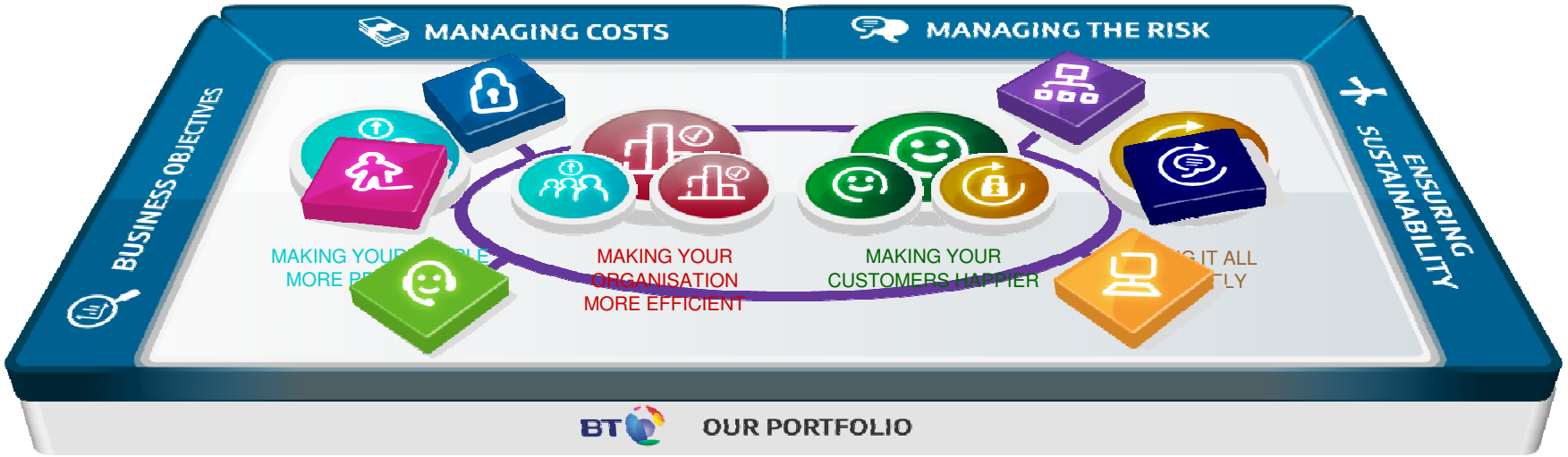
Agenda

- BT Zahlen und Fakten
- BT Portfolio
- Typische Ansätze für Vendor Security
  - Ansatz A: BT‘s Interne Sicherheit
  - Ansatz B: Ausschreibung über TPI
  - Ansatz C: gemeinsames ISMS
- FAQ zur Vendor Security



Herausforderungen für Ihr Unternehmen

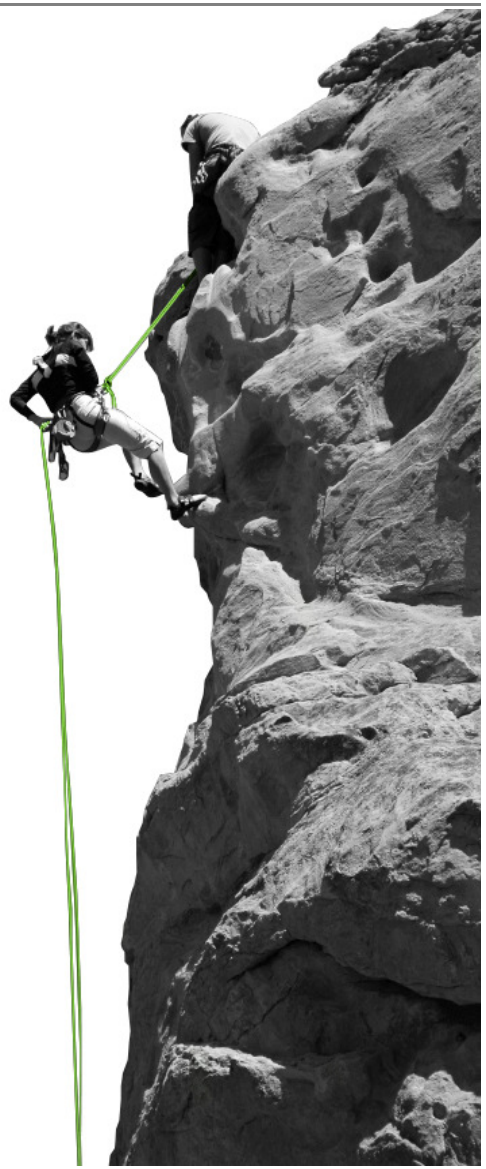
Die Antwort von BT



Unser Portfolio – Beyond the Network!

Agenda

- BT Zahlen und Fakten
- Portfolio
- Typische Ansätze für Vendor Security
  - Ansatz A: BT‘s Interne Sicherheit
  - Ansatz B: Ausschreibung über TPI
  - Ansatz C: gemeinsames ISMS
- FAQ zur Vendor Security



Die Umgebung

Schutz einer der größten Firmeninfrastrukturen der Welt

- 90K Mitarbeiter, 30K Externe
- 6K Gebäude in UK, 497 ausserhalb UK
- 120K Bildausweise, 180K Schlüssel-Tokens, 20K Zutrittsleser
- 175K Zutritte pro Tag (UK)
- 1M Zutrittsrequests p.a. im Self-Service
- 7K Server
- Intranet mit mehr 100K Usern
- Exchange-Installation mit 120K Usern
- 250 externe connections
- 14M unberechtigte Verbindungsversuche von aussen pro Tag
- 6M Spam-Mails pro Tag
- 2M Viren, 5M mögliche Attacken, 250K bestätigte Attacken pro Monat

Quelle: Thomas Eichacker „Interne Sicherheit bei BT“

BT

Die Sicherheitsorganisation

- 800 Mitarbeiter, UK und weltweit (160 CISSPs)
- Mitarbeit und Mitgliedschaft ISO, FIRST, ISF, etc.
- 160 Security-Patente
- Zentrale Kompetenzzentren
- Dezentrale Präsenz
- Security Operations Centre 24/7/365
- Security Incident Management Centre 24/7/365

Quelle: Thomas Eichacker „Interne Sicherheit bei BT“

BT

Die Sicherheitsmassnahmen (1/2)

- Einheitliche und weltweit gültige Sicherheits-Policy
- 24 ISO27001 Zertifikate, einschließlich „zentrales Sicherheitsmanagement“
- Einheitlicher Sicherheits-Evaluations- und Freigabe-Prozess für Systeme, Applikationen, Netze (BTSECS, derzeit 6K Registrierungen)
- Technische und organisatorische Regelungen für Third-Party-Access
- Klassifizierung von Daten und Informationen
- Klassifizierung von physischen Assets (Gebäude, technische Infrastruktur, Geräte, Gegenstände, etc)
- Sicherheitsmassnahmen bei Personalmassnahmen und Einstellungen
- Sicherheitsmassnahmen für Third Parties / Contractors
- Regelmässige verpflichtende Trainings (Security, AV, Datenschutz, Anti-Corruption and Bribery)

Quelle: Thomas Eichacker „Interne Sicherheit bei BT“

BT

Die Sicherheitsmassnahmen (2/2)

- Gebäudesicherheit
- Clear Desk/Clear Screen
- Netzwerk-Sicherheit
- Flächendeckendes Sicherheits-Patch- und Antivirusmanagment

- Zugriffskontrolle
- Logon/Passwort-Sicherheit
- Information Security Incident Management

- Business Continuity Management
- Datenschutz
- Geheimschutz / Government Security

- Regelmäßige interne Audits und Notfallübungen

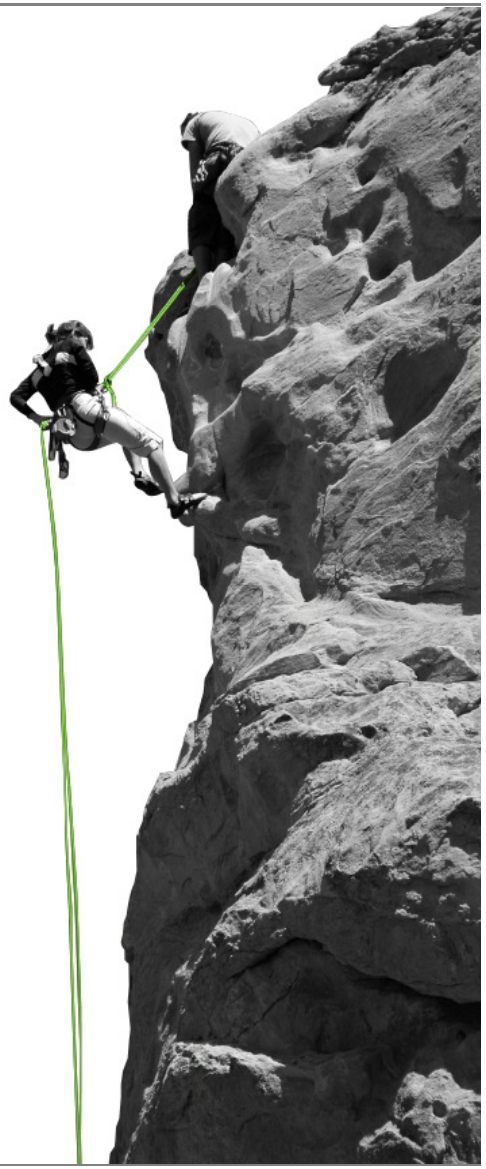
Quelle: Thomas Eichacker „Interne Sicherheit bei BT“

Ansatz A: Baseline Security der BT ausreichend

- Kunde überzeugt sich durch verfügbare Zertifikate, SAS70-Ergebnisreports, ggf. Anschauung, Stichproben etc. von der zugrundeliegenden Sicherheit der BT Plattform und betrachtet das verbleibende Risiko für sich als akzeptabel.

Agenda

- BT Zahlen und Fakten
- Portfolio
- Typische Ansätze für Vendor Security
  - Ansatz A: BT‘s Interne Sicherheit
  - Ansatz B: Ausschreibung über TPI
  - Ansatz C: gemeinsames ISMS
- FAQ zur Vendor Security



Technology Partners International (TPI)

Quick Facts zu TPI

- **Founded 1989** from Dennis A. McGuire and Warren Gallant
- **Headquarter - Houston (The** Woodlands), Texas

Business

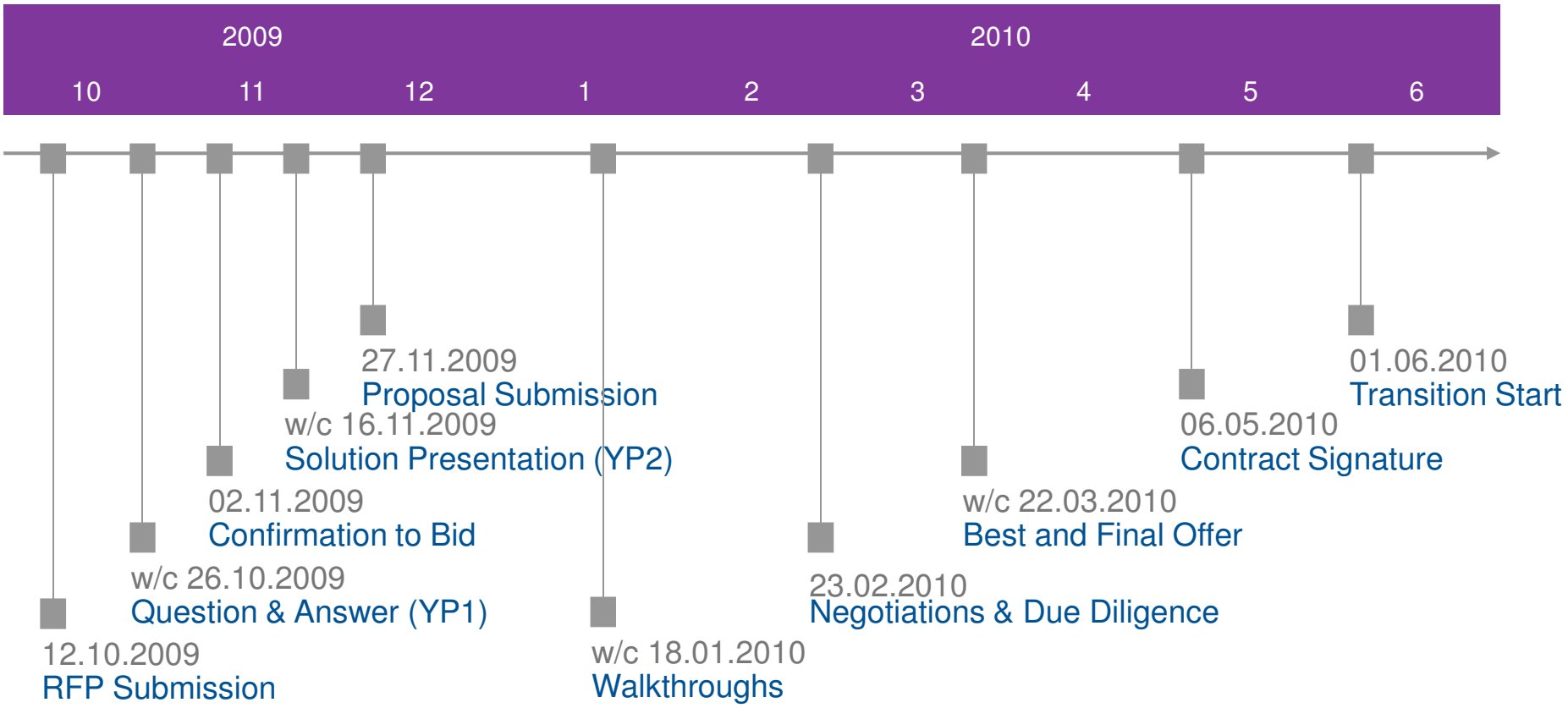
TPI ist die weltweit führende Firma für die Unterstützung von Organisationen zur Optimierung ihrer Geschäftstätigkeit, durch die beste Kombination von Insourcing, Offshoring, Shared Services und Outsourcing.

Our Mission is our Passion

To be the most informed source of objective expertise to guide organizations through fundamental change to their business support operations.

Quelle: Stefan Winghardt & Jan Brandt „TPI“

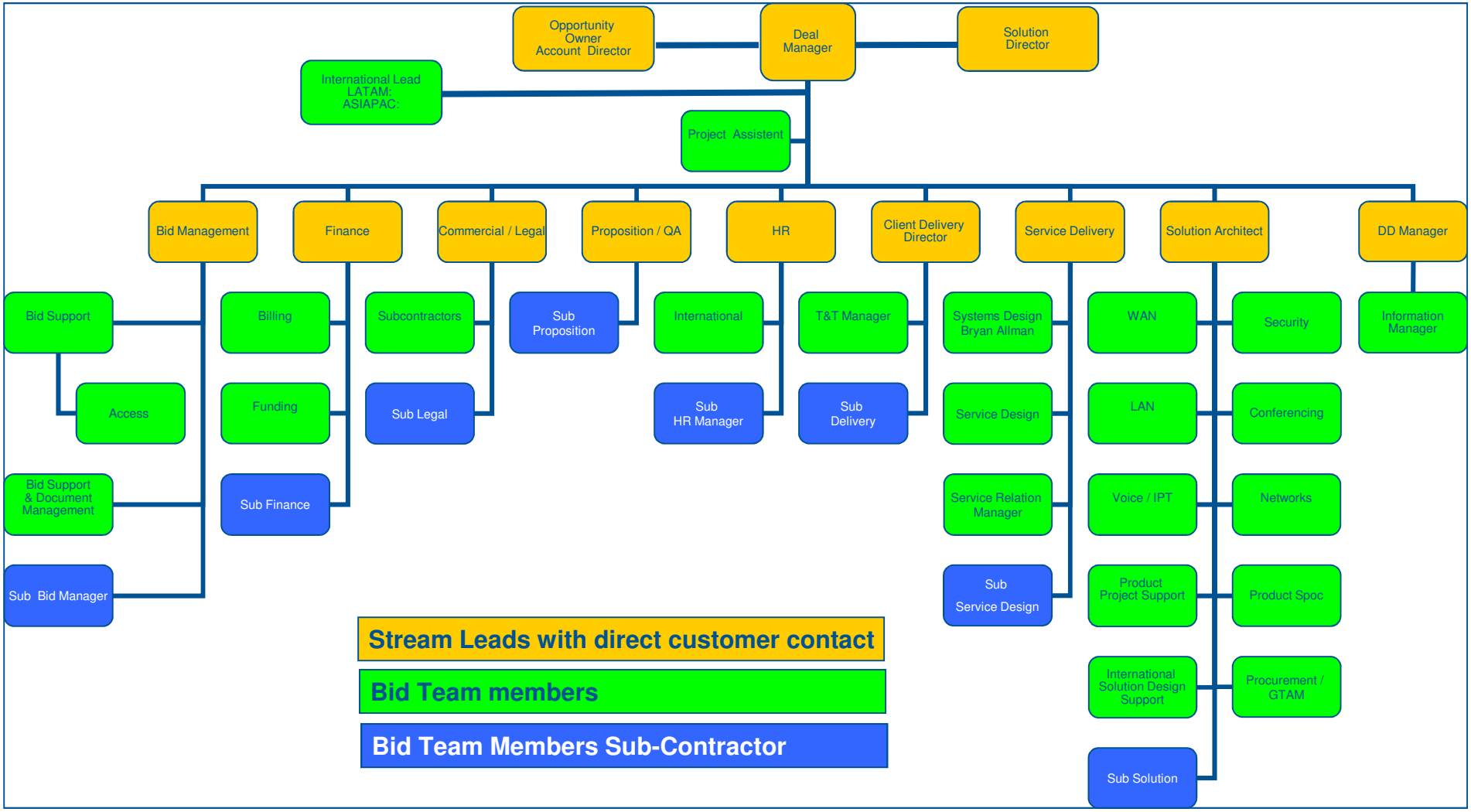
Project Time Line



Project break at year end (19.12.2009 – 10.01.2010)

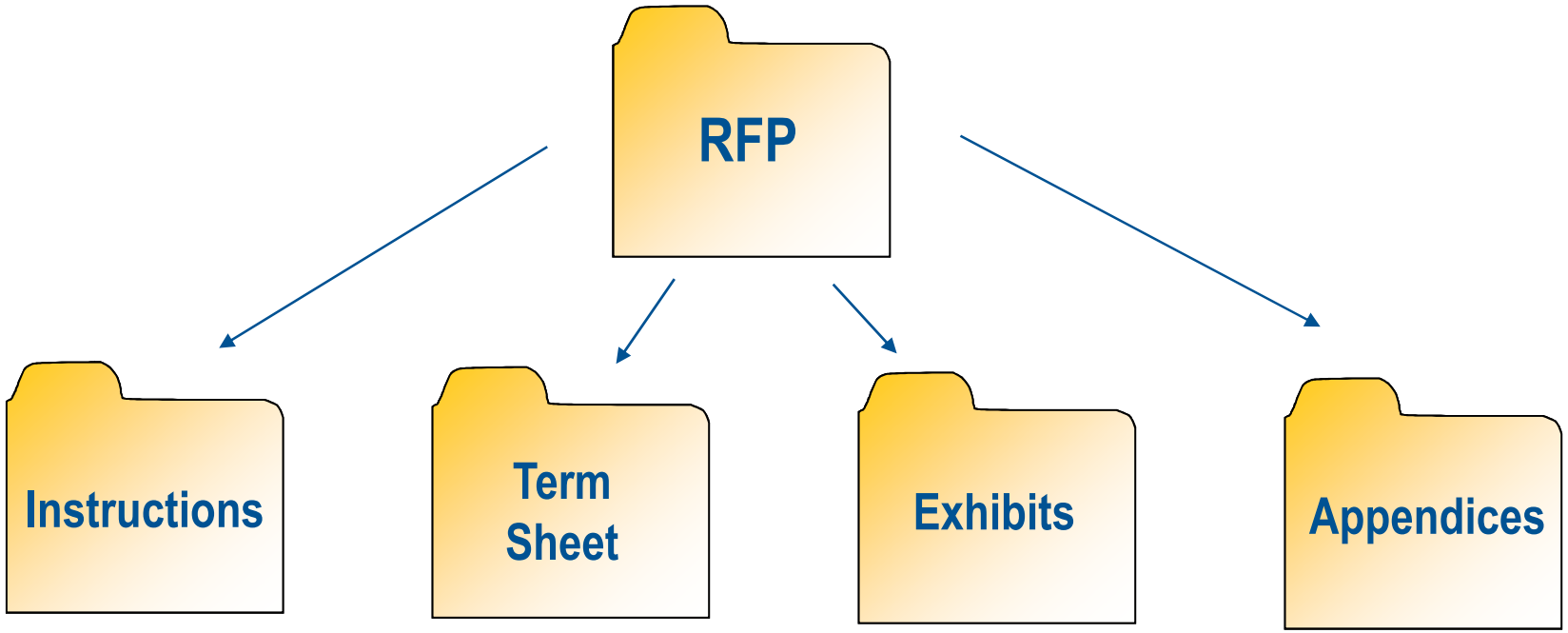
Quelle: Stefan Winghardt & Jan Brandt „TPI“

TPI Team Structure Prime - Example



Quelle: Stefan Winghardt & Jan Brandt „TPI“

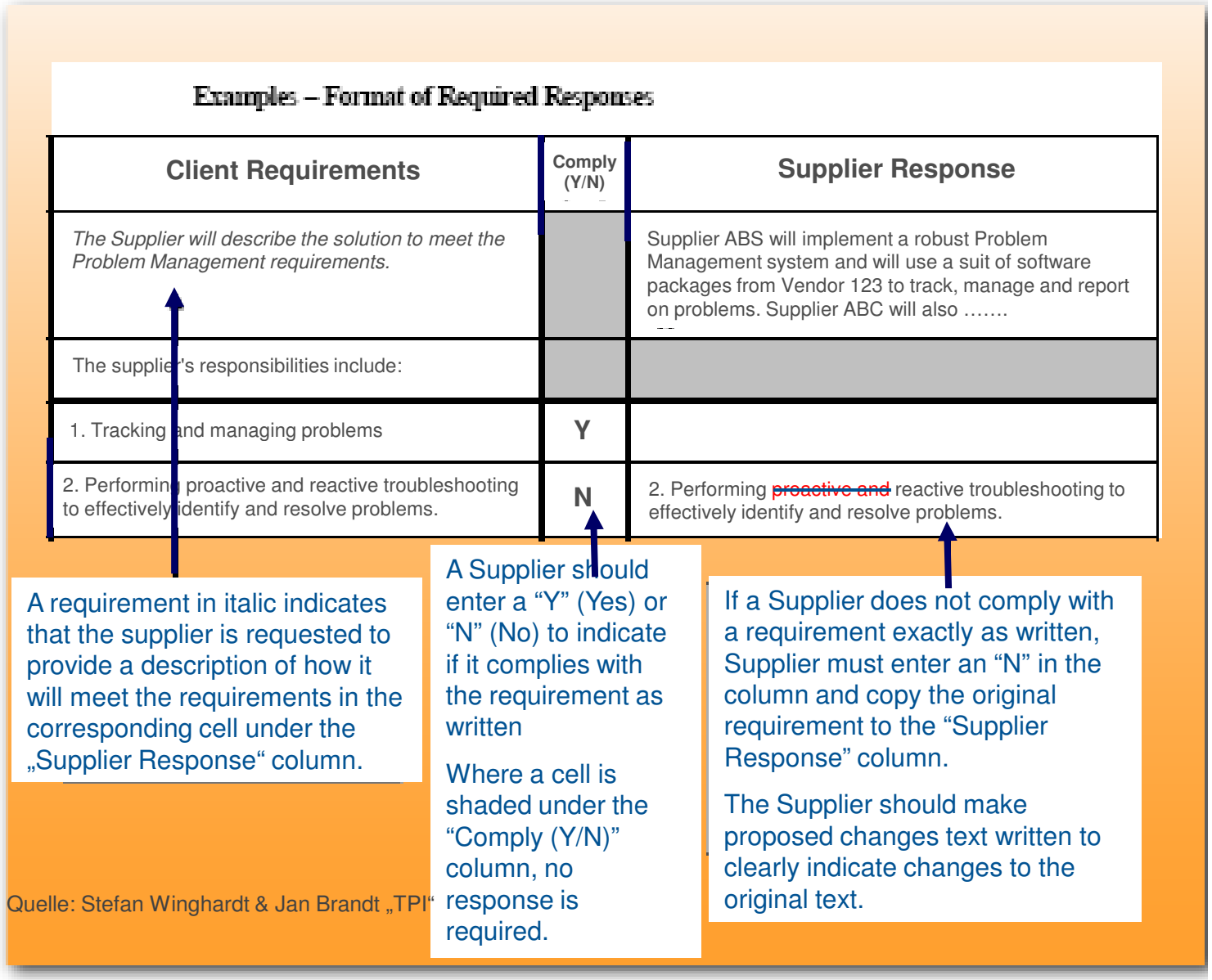
RFP Structure



TPI Document Overview

Quelle: Stefan Winghardt & Jan Brandt „TPI“

Example format Y/N Questions



Examples – Format of Required Responses

Client Requirements	Comply (Y/N)	Supplier Response
The Supplier will describe the solution to meet the Problem Management requirements.		Supplier ABS will implement a robust Problem Management system and will use a suit of software packages from Vendor 123 to track, manage and report on problems. Supplier ABC will also …….
The supplier's responsibilities include:		
1. Tracking and managing problems	Y	
2. Performing proactive and reactive troubleshooting to effectively identify and resolve problems.	N	2. Performing ~~proactive and~~ reactive troubleshooting to effectively identify and resolve problems.

A requirement in italic indicates that the supplier is requested to provide a description of how it will meet the requirements in the corresponding cell under the „Supplier Response“ column.

A Supplier should enter a “Y” (Yes) or “N” (No) to indicate if it complies with the requirement as written

Where a cell is shaded under the “Comply (Y/N)” column, no response is required.

If a Supplier does not comply with a requirement exactly as written, Supplier must enter an “N” in the column and copy the original requirement to the “Supplier Response” column.

The Supplier should make proposed changes text written to clearly indicate changes to the original text.

Quelle: Stefan Winghardt & Jan Brandt „TPI“

Fig 3 – Format of required responses

Ansatz B: Nutzung der TPI Struktur

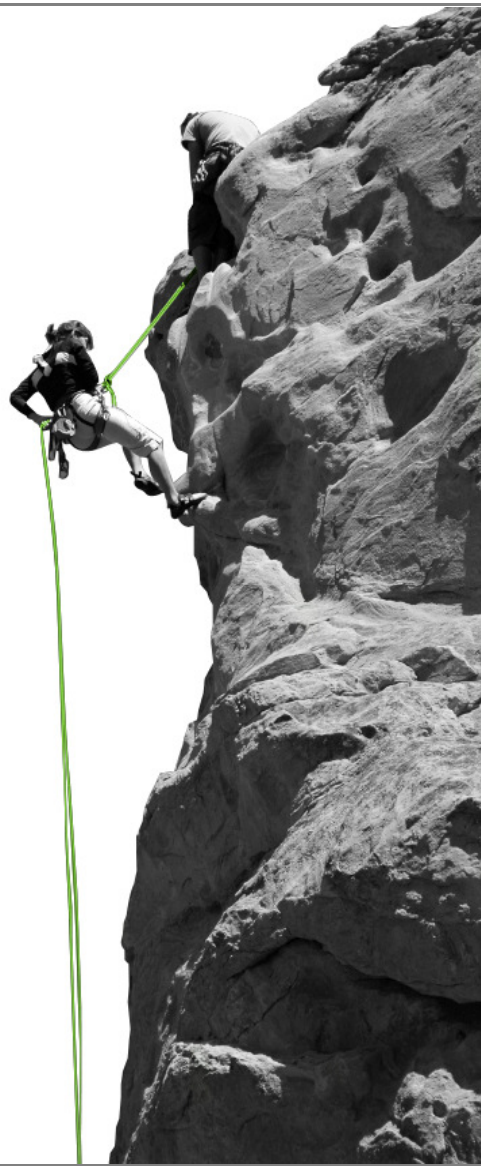
- Kunde schließt sich beim Bid-Prozess ganz oder teilweise den sorgfältig vorbereiteten und erprobten TPI-(Maximal)Anforderungen an und erhält eine entsprechende vertragliche Absicherung.

- Bemerkung: Es kommt vor, dass unbedacht mehr von den von TPI vorgeschlagenen Security-Elementen verlangt werden, als bei genauer Nachfrage benötigt werden => Aufwand und Preis!

BT

Agenda

- BT Zahlen und Fakten
- Portfolio
- Typische Ansätze für Vendor Security
  - Ansatz A: BT‘s Interne Sicherheit
  - Ansatz B: Ausschreibung über TPI
  - Ansatz C: gemeinsames ISMS
- FAQ zur Vendor Security



Security Risk Analysis and Management

… mit dem Ziel eines gemeinsamen

Information Security Management System (ISMS)

Starting Point:

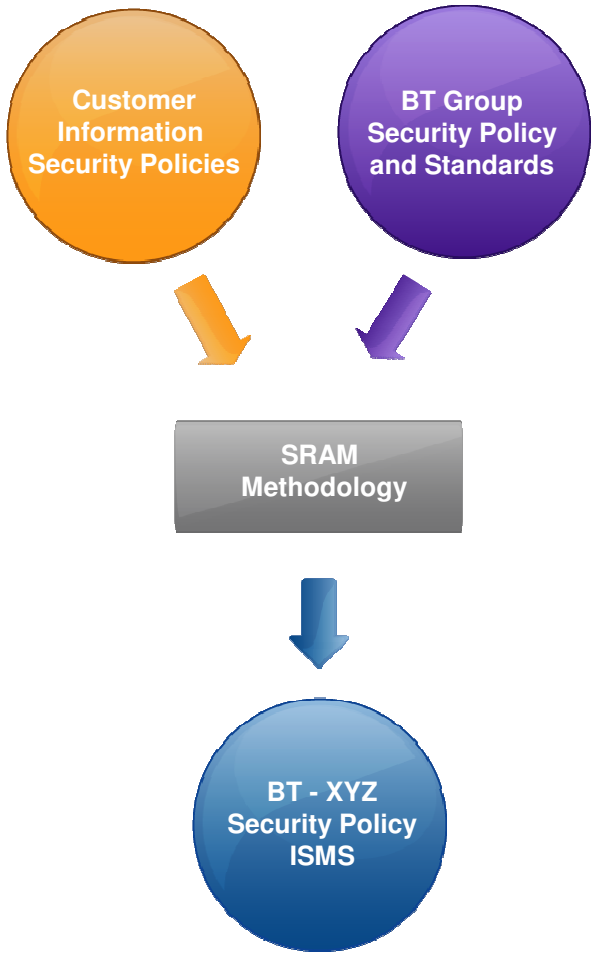
- Multiple different Security Policies and Standards
- How to audit?

SRAM Methodology:

- Identification of critical Information Assets and Scoping
- Business Impact Analysis
- Threat and Vulnerability Assessment for selected sites
- Tool-based Risk Calculation
- Tool based Countermeasure and Policy Generation
- Review of Countermeasures against Customer Policies
- Risk Treatment Plan
- Statement of Applicability
- Gain Approval by Customer

Results:

- BT's Customer Service specific Security Policy and Countermeasures based on Customer's Information Security Risks
- Compliance checks against the new Security Policy
- Risk Assessments for new sites/services can be added easily
- ISMS defined
- Compliance with ISO 27001:2005

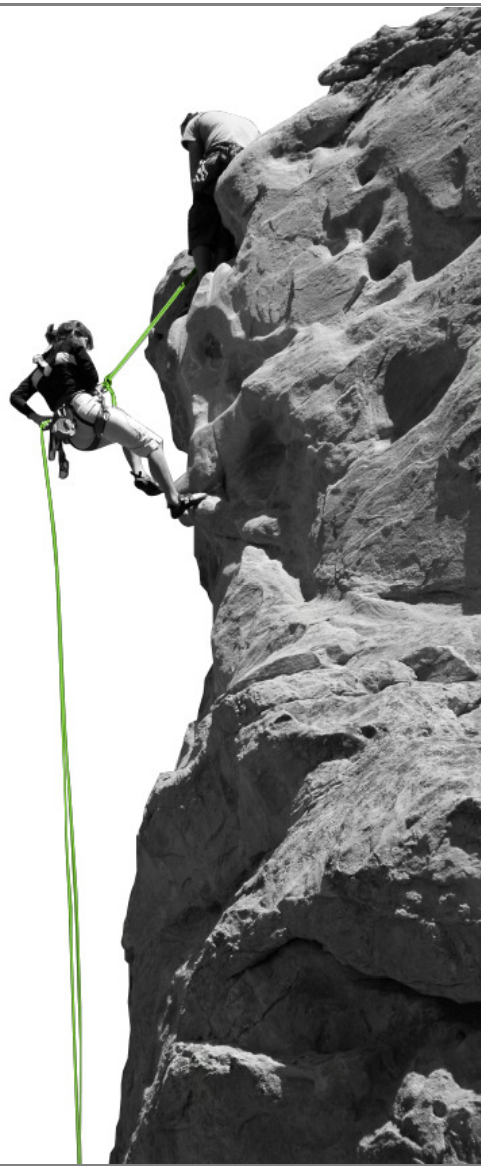


Ansatz C: Maßgeschneidertes ISMS (ISO27001)

- Kunde und BT stecken den Scope eines gemeinsamen ISMS nach Best Practice / ISO27001 ab.
- Im Allgemeinen höchstmögliche Sicherheit bei bester Kosteneffizienz.
- Zusätzliche Sicherheitsmaßnahmen beschränken sich auf die gemäß Risikoanalyse als notwendig ermittelte Bereiche.
- Gern bei Revision und Wirtschaftsprüfern gesehen

Agenda

- BT Zahlen und Fakten
- Portfolio
- Typische Ansätze für Vendor Security
  - Ansatz A: BT‘s Interne Sicherheit
  - Ansatz B: RFP über TPI
  - Ansatz C: gemeinsames ISMS
- FAQ zur Vendor Security



FAQ zu IT Audits

- - Viele Kunden wünschen individuelle Audits, was für Sie als Dienstleister einen hohen Aufwand bedeuten kann
  - FK: In der Tat. Wir versuchen auch meist, allen Wünschen zu entsprechen. Viele Fälle regeln sich über den Preis. Wir schlagen alternative Standardlösungen/Best Practice vor.
- - Kunden benutzen oft sehr unterschiedlich strukturierte Fragebögen
  - FK: Das ist weniger das Problem, solange inhaltlich die Fragen mit Best Practice konform gehen.
- - Kunden gehen teilweise sehr in die Tiefe (fragen z.B. nach Algorithmen und Logging-Konzepten), manchmal wird nur an der Oberfläche gekratzt
  - FK: Wir versuchen die Ursache für die tiefgehende Anforderung zu ergründen und einen alternativen Vorschlag mit weniger Aufwand jedoch vergleichbarem Ergebnis (Risiko für das Business) vorzulegen.
- - Manchmal reicht den Kunden eine bestehende Zertifizierung (wie ISO 2700x), manchmal reicht es nicht aus
  - FK: in der Tat. Siehe Ansatz A, B und C zur Vendor Security. Im Einzelfall versuchen wir stets, den Business-Hintergrund der Anforderung zu ermitteln, um eine angemessen kostengünstige Lösung zu finden.

BT

FAQ zu IT Audits

- - Wie gehen Sie mit den in Kundenaudits gefundenen "Issues" um? Werden diese behoben? Wie reagieren Kunden, wenn Sie die "Issues" nicht beheben?
  - FK: Wenn die Issues im Verantwortungsbereich von BT liegen, müssen sie selbstverständlich zeitnah auf eigene Kosten beseitigt werden.
- - Tragen die Kundenaudits dazu bei, um relevante "Issues" bei Ihnen aufzudecken, oder werden nie wirkliche "Issues" gefunden?
  - FK: Es ist wohl der großen Zahl externer Audits geschuldet, dass seit langer Zeit nur noch minor Issues behandeln werden müssen. Irgend etwas findet jeder gute Auditor, aber es ist meist mit überschaubarem Aufwand verbunden.
- - Wer trägt die Kosten für ein Kundenaudit, und die Behebung der "Issues"?
  - FK: wenn die Anforderungen über die Baseline (Fall A) hinausgehen, trägt der Kunde die Kosten. Bei Findings, die BT zu verantworten hat, trägt BT die Kosten.

BT

FAQ zu IT Audits

- - Wie sähe aus Ihrer Sicht ein ideales Umfeld in der Wirtschaft aus, um den Aufwand für Kundenaudits zu reduzieren (bei gleichzeitiger Qualitätserhöhung)?
  - FK: Vereinheitlichung von Organisationsstrukturen und Prozessen ähnlich ITIL. Ein Hauptproblem heute stellt m.E. die uneinheitliche Einbindung der Security im Unternehmen dar und die damit verbundene Budget- und Verantwortungssituation. Ist Security nur ein technischer, aber unproduktiver Teil der IT? Warum werden immer mehr Unternehmen Opfer von Hacker-Angriffen? Was gilt es denn zu schützen: die Server, die IT oder den guten Ruf, das intellectual Property und die Kundendaten des Unternehmens? Je mehr hier vereinheitlich wird, je mehr kann eine Standardisierung im Sinne von Best Practice helfen, effizienter und besser die Unternehmen zu schützen.
- - Welche Rolle hat das Information Security Management für Sie als Dienstleister? Trägt es z.B. zu Ihrer Wettbewerbsfähigkeit bei?
  - Wir wollen unseren Kunden Qualität bieten. Information Security ist ein elementar wichtiger Bestandteil der Qualität (siehe Auto, Spielzeug, Demokratie). Insofern ist die Rolle kritisch und trägt – vorausgesetzt die vorige Frage wird von Unternehmen entsprechend beantwortet – wesentlich zur Wettbewerbsfähigkeit bei.

BT

Vielen Dank

[V1.1 – 20111019]