

TU UNTERNEHMENSBERATUNG GMBH

IT-Sicherheit

Ergebnisse einer empirischen Untersuchung

16.11.2006



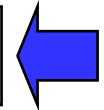
Vorstellung TU Unternehmensberatung

Einsatzgebiet	Deutschlandweit, mit Schwerpunkt auf dem Nordwesten
Zielkunden	Inhabergeführter Mittelstand
Unser Anspruch	Dem Unternehmer bei allen Aufgabenstellungen ein kompetenter Sparringspartner sein
Beraterstruktur*	4 Senior-Berater 9 Berater
Netzwerk	5 Freie Mitarbeiter Treuhand Oldenburg Grant Thornton



Inhaltsverzeichnis

I	Einleitung	Seite 4
II	Benchmark	Seite 7
III	IT-Sicherheitsmanagement	Seite 43





Einleitung

- Bedeutung der IT für die Unternehmen -

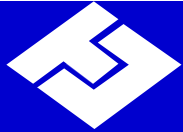
- **Ohne IT-Unterstützung** sind Geschäftsprozesse **kaum noch wirtschaftlich** und damit **wettbewerbsfähig**.
- Die **Anforderungen aus der Globalisierung** führen zu Konzepten wie virtuelle Firmen, Supply Chains/Lieferketten, eCommerce etc., die stark von **Information und Kommunikation abhängig** sind.
- Die Nutzung als reines Instrument zur **Rationalisierung** (z. B. in der Buchhaltung) **ist dem Einsatz als strategisches Instrument der Unternehmenssteuerung gewichen**.



Einleitung

- Bedeutung der IT für die Unternehmen -

- ↪ Die **Bedeutung** der IT für die Unternehmen ist bereits hoch, wird aber noch **weiter zunehmen**.
- ↪ Entsprechend **steigen die Anforderungen** an **Verfügbarkeit** und **Sicherheit der IT** laufend.



Einleitung

- Auszug aus der Liste möglicher Compliance-Anforderungen -

Beispiele für IT-relevante Gesetze, Verordnungen, Erlasse etc.

- BGB, HGB (Bürgerliches und Handelsgesetzbuch)
- AO (Abgabenordnung), GDPdU (Grundsätze für den Datenzugriff und die Prüfbarkeit digitaler Unterlagen)
- KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich)
- AktG (Aktiengesetz), GmbHG (GmbH-Gesetz)
- UrhG (Urhebergesetz)
- GoBS (Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme)
- TKG (Telekommunikationsgesetz), TDG (Teledienstgesetz),
- BDSG (Bundesdatenschutzgesetz), TDDSG (Teledienstschutzgesetz)
- Europäische Richtlinie über Datenschutz bei der elektronischen Kommunikation
- Basel II (Rating)
- SOX (Sarbanes Oxley Act)

Unternehmensspezifische Regelungen



Einleitung

- Definition IT- Sicherheit -

Ziel ist es, die Verarbeitung, Speicherung und Kommunikation von Informationen so zu gestalten, dass die primären Sicherheitskriterien

- **Vertraulichkeit, Verfügbarkeit, Integrität, Verbindlichkeit und Authentizität**

und die sekundären Sicherheitskriterien

- **Nachvollziehbarkeit, Nachweisbarkeit, Erkennungs-, Alarmierungs- und Abwehrfähigkeit**

der Informationen und Systeme in ausreichendem Maße sichergestellt werden.

IT-Sicherheit steht in diesem Zusammenhang dafür

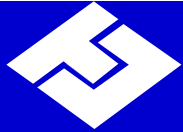
- die Systeme **vor Gefahren** bzw. **Bedrohungen** zu **schützen**, **Schaden** zu **vermeiden** und **Risiken** zu **minimieren**.



Inhaltsverzeichnis

I	Einleitung	Seite 4
II	Benchmark	Seite 7
III	IT-Sicherheitsmanagement	Seite 43

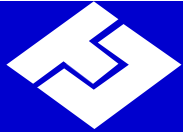




Benchmark

- Grundlagen -

- Die empirische Auswertung basiert auf den Ergebnissen von **45 IT-Systemprüfungen**.
- Die Prüfungen wurden zum großen Teil durch die Wirtschaftsprüfungsgesellschaft **Treuhand Oldenburg**, aber auch durch die **Unternehmen selbst** beauftragt.
- Die qualitativen Auditergebnisse wurden nach einem einheitlichen Verfahren in **quantitative Aussagen** überführt und so grafisch darstellbar gemacht.
- Der Prüfungsumfang basiert auf dem IDW Prüfungsstandard **PS 330**, reduziert um die Aspekte Softwarefunktionalität, Geschäftsprozesse und Internes Kontrollsystem.



Benchmark

- Struktur des Prüfumfangs -

Die Erhebungsmenge der geprüften Unternehmen setzt sich wie folgt zusammen:

Nach Branche

Dienstleistungen	7
Bau	4
Produktion	
Herstellung LM	5
Fertigung	22
Handel	7

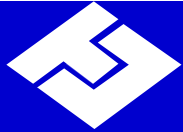
LM = Lebensmittel

Nach Anzahl Arbeitnehmer

1-9	0
10-49	2
50-99	10
100-199	16
200-499	8
500-999	7
1000-1999	2

Nach Umsatz in Mio. €

bis 10	4
10 bis 30	21
30 bis 50	7
50 bis 100	7
größer 100	6

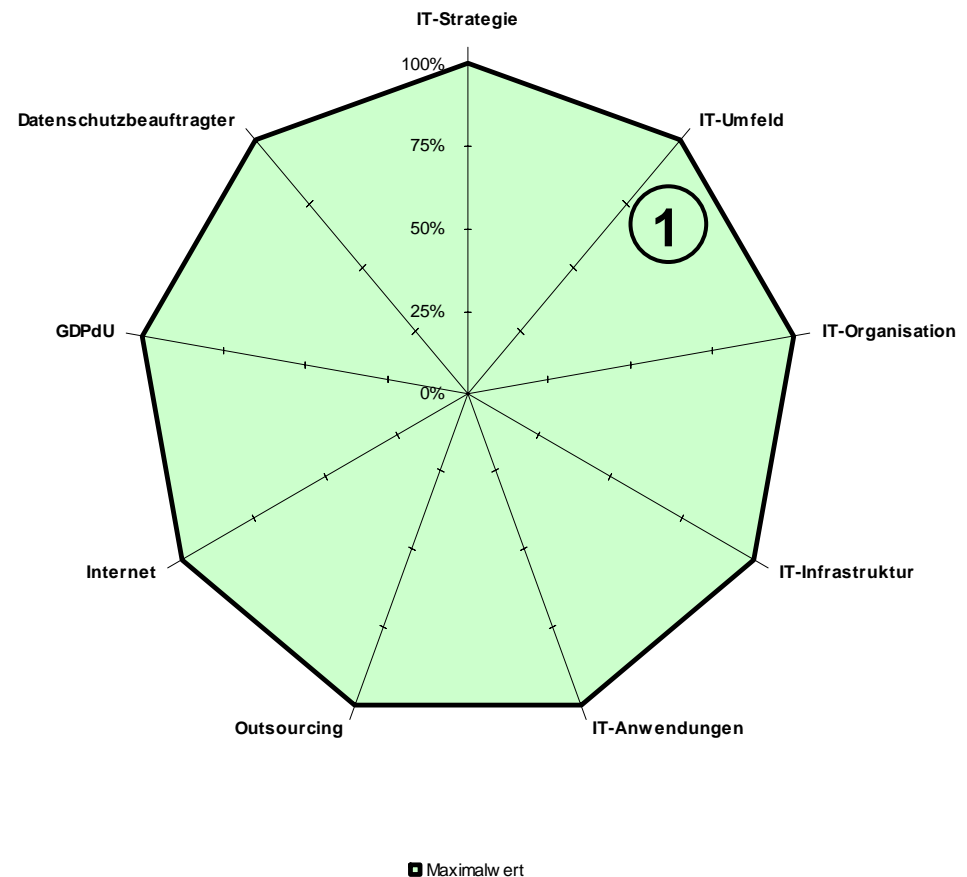


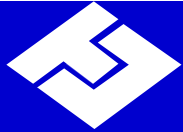
Benchmark

- Gesamtübersicht Ebene 1 -

In den Grafiken werden in der ersten Ebene die Rubriken dargestellt und ihnen der Maximalwert 100% zugeordnet.

Gesamtübersicht





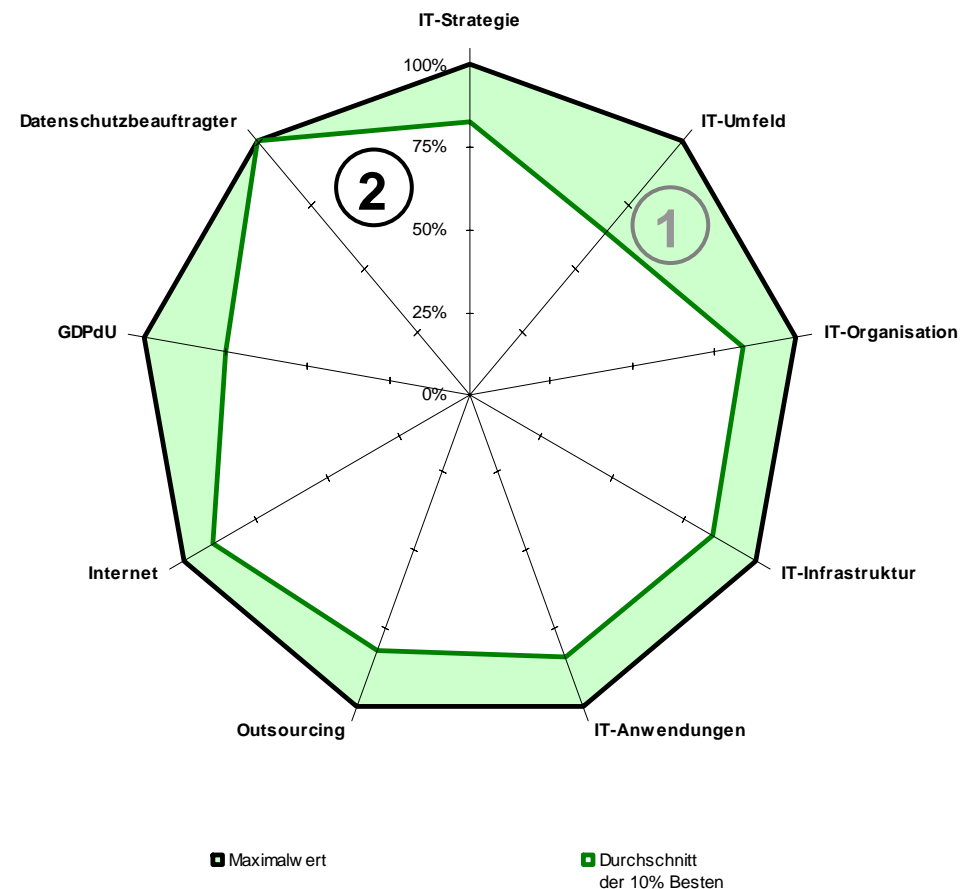
Benchmark

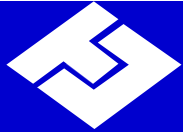
- Gesamtübersicht Ebene 2 -

In den Grafiken werden in der ersten Ebene die Rubriken dargestellt und ihnen der Maximalwert 100% zugeordnet.

In der zweiten Ebene ist das Spinnennetz abgetragen, das aus dem Mittelwert der besten 10% der auditierten Unternehmen resultiert.

Gesamtübersicht





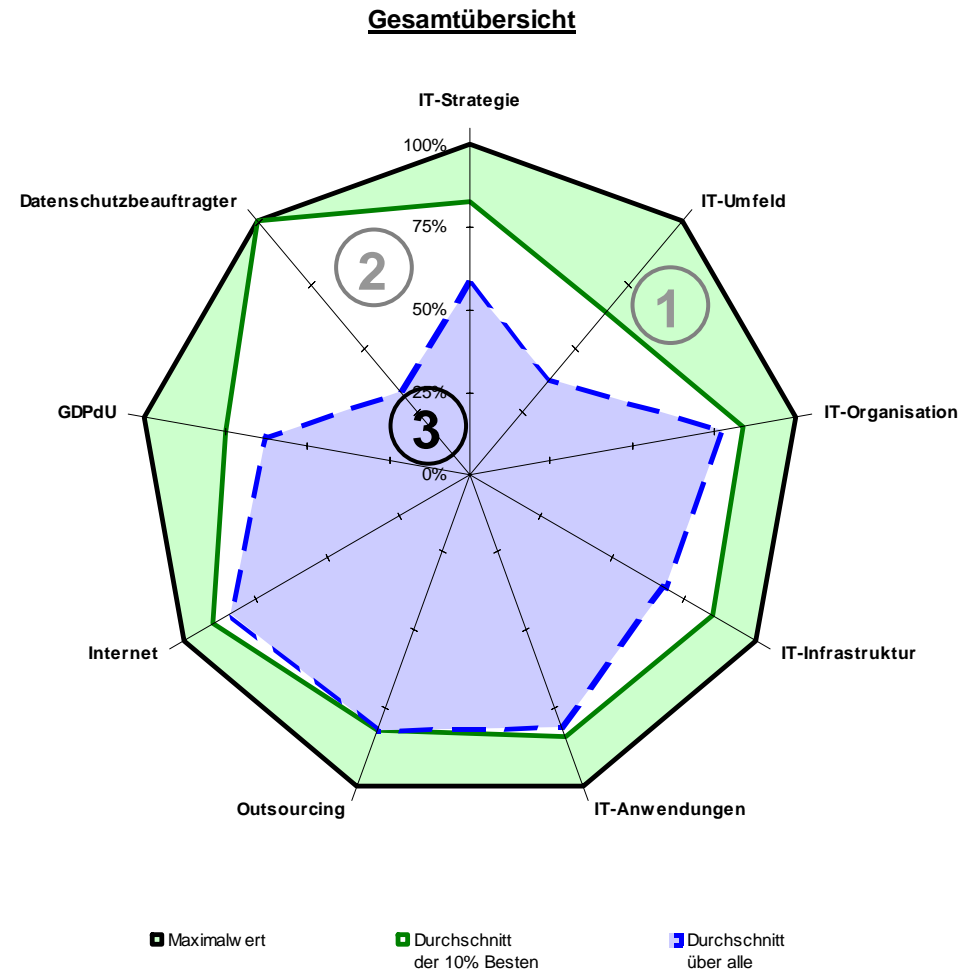
Benchmark

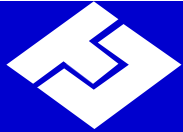
- Gesamtübersicht Ebene 3 -

In den Grafiken werden in der ersten Ebene die Rubriken dargestellt und ihnen der Maximalwert 100% zugeordnet.

In der zweiten Ebene ist das Spinnennetz abgetragen, das aus dem Mittelwert der besten 10% der auditierten Unternehmen resultiert.

In der dritten Ebene wird der Mittelwert aus den Ergebnissen aller auditierter Unternehmen abgetragen.





Benchmark

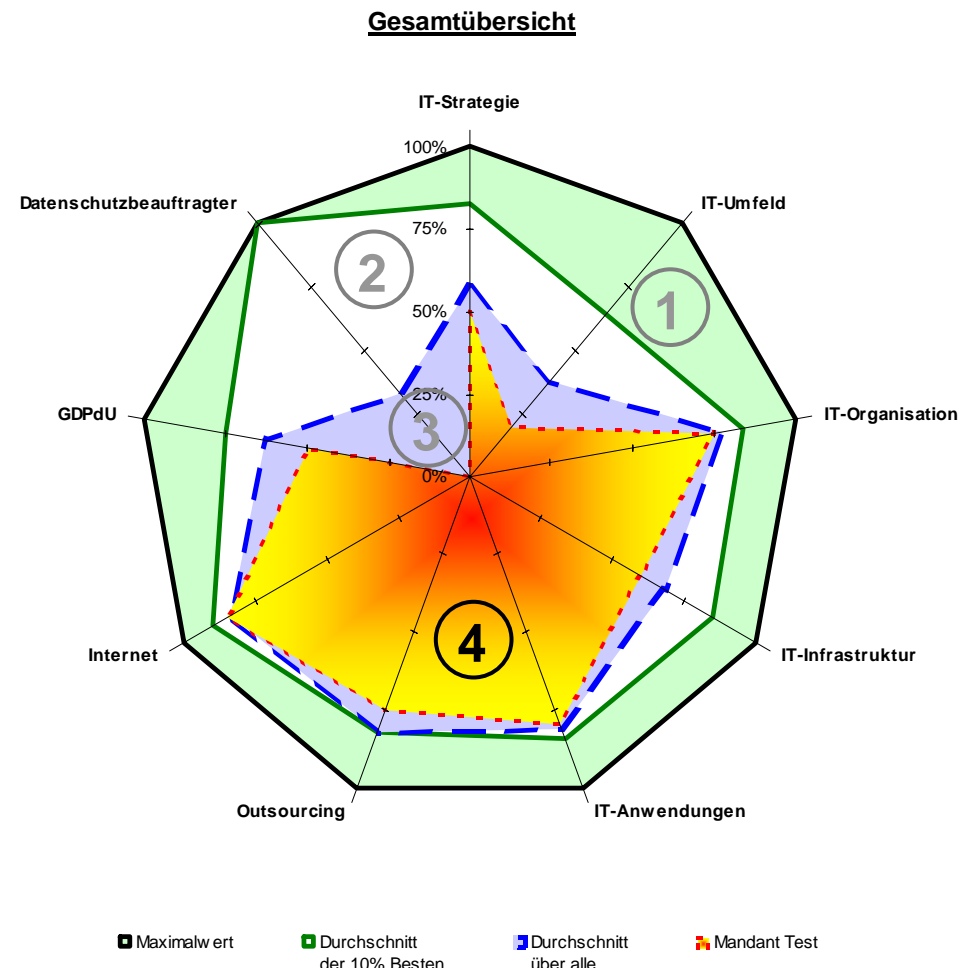
- Gesamtübersicht Ebene 4 -

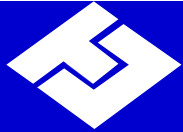
In den Grafiken werden in der ersten Ebene die Rubriken dargestellt und ihnen der Maximalwert 100% zugeordnet.

In der zweiten Ebene ist das Spinnennetz abgetragen, das aus dem Mittelwert der besten 10% der auditierten Unternehmen resultiert.

In der dritten Ebene wird der Mittelwert aus den Ergebnissen aller auditierter Unternehmen abgetragen.

In der letzten Ebene werden die Ergebnisse des auditierten Unternehmens zum Vergleich mit denen anderen Ebenen eingestellt.

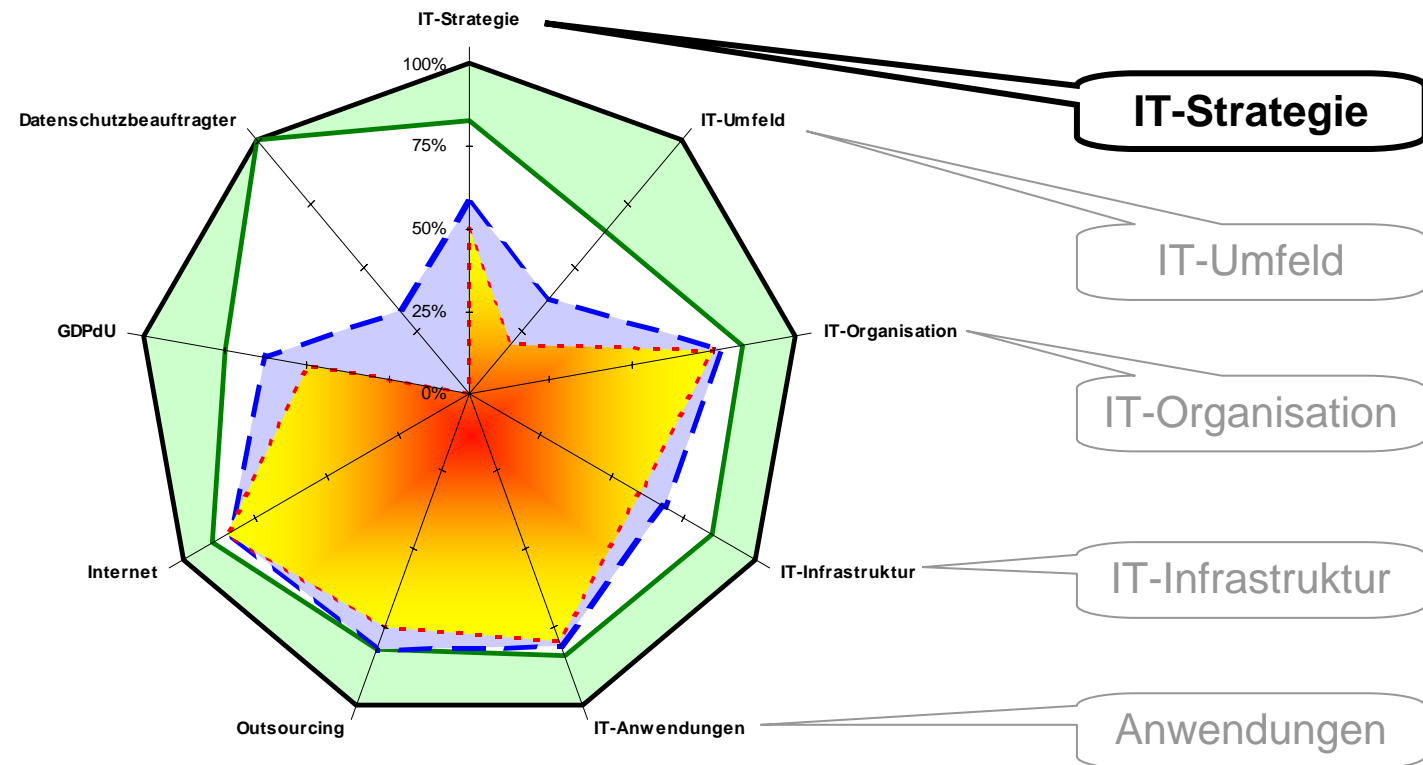




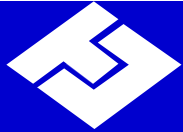
Benchmark

- Gesamtübersicht -

Gesamtübersicht



■ Maximalwert ■ Durchschnitt der 10% Besten ■ Durchschnitt über alle ■ Mandant Test



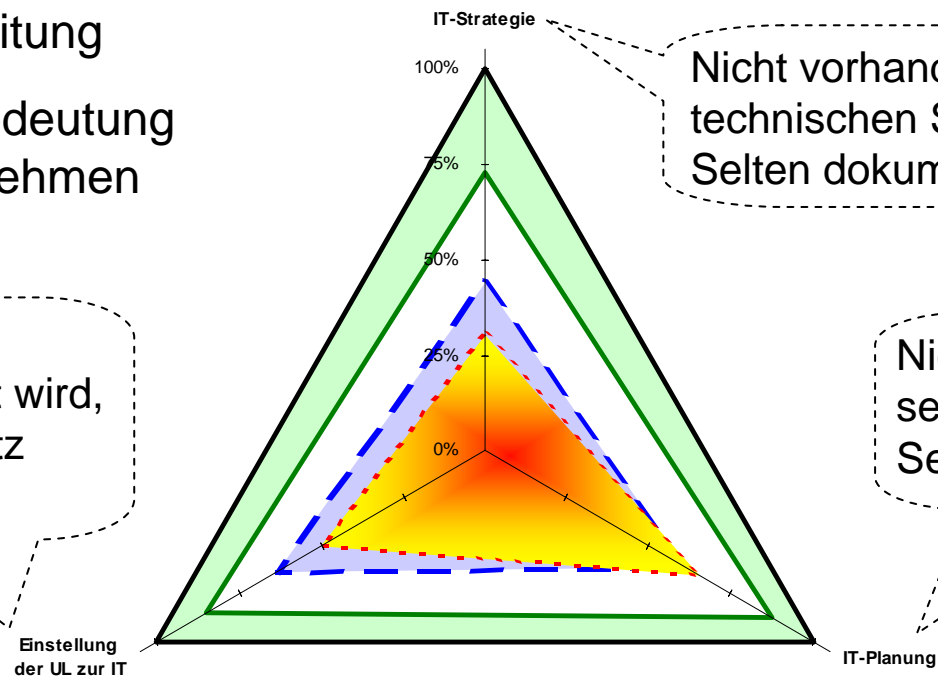
Benchmark

- IT-Strategie -

Rubrik IT-Strategie

- Vorbehaltsaufgaben der Unternehmensleitung
- Definition der Bedeutung der IT im Unternehmen

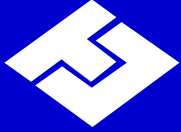
IT ist ein Kostenblock.
Was in die IT gesteckt wird,
soll sich in Mehrumsatz
rechnen.



Nicht vorhanden oder entspricht
technischen Selbstverständnissen.
Selten dokumentiert.

Nicht vorhanden oder
sehr grob gehalten.
Selten dokumentiert.

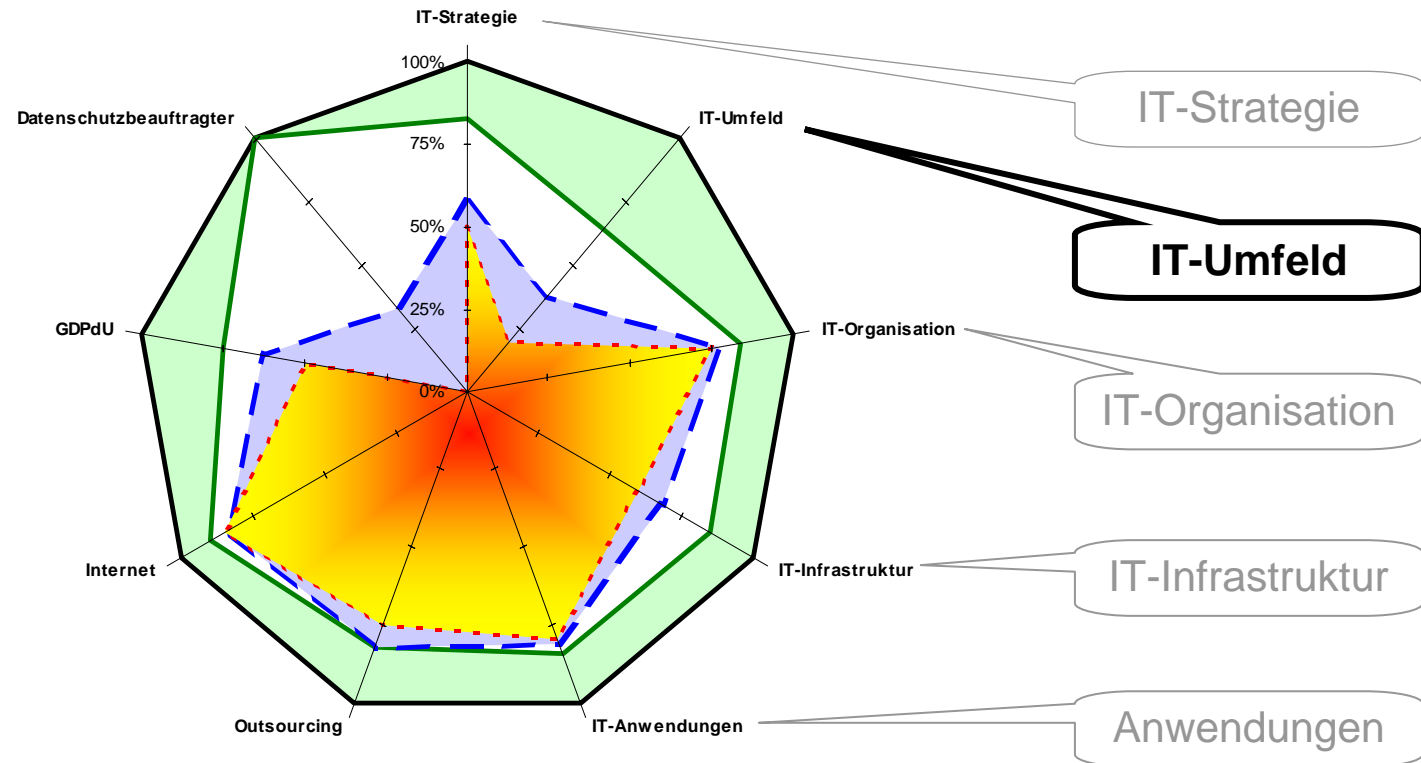
■ Maximalwert ■ Durchschnitt der 10% Besten ■ Durchschnitt über alle ■ Mandant Test



Benchmark

- Gesamtübersicht -

Gesamtübersicht



■ Maximalwert ■ Durchschnitt der 10% Besten ■ Durchschnitt über alle ■ Mandant Test

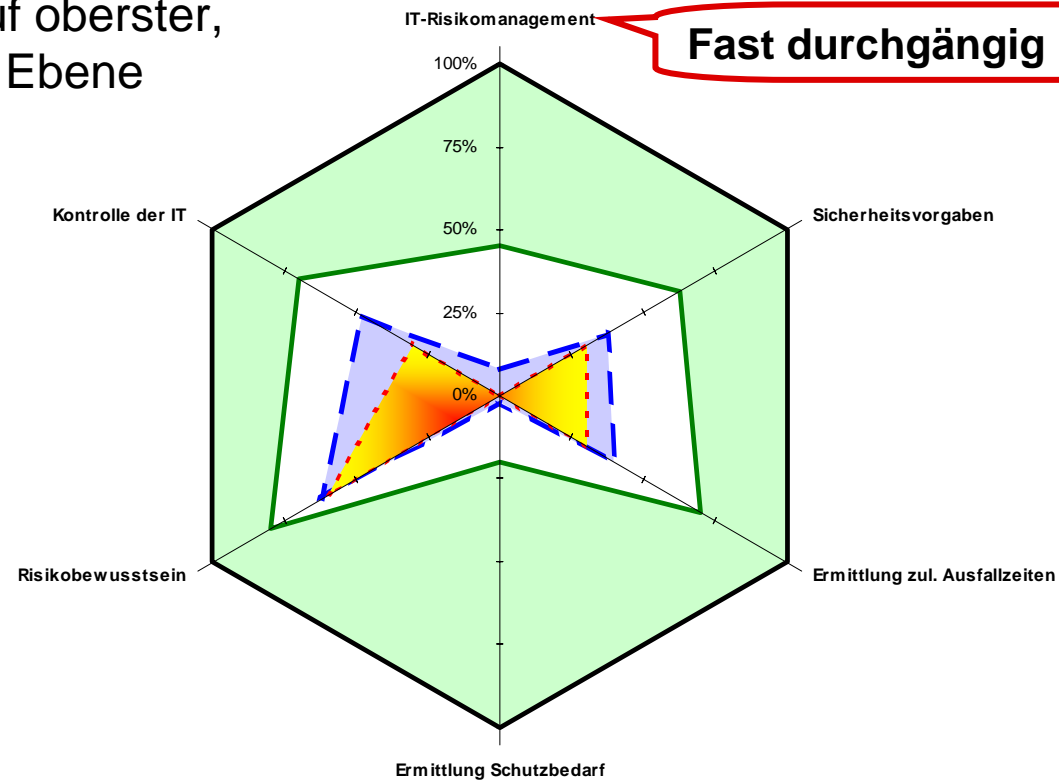


Benchmark

- IT-Umfeld -

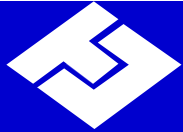
Rubrik IT-Umfeld

- IT-Sicherheit auf oberster, konzeptioneller Ebene



Fast durchgängig nicht vorhanden.

■ Maximalwert ■ Durchschnitt der 10% Besten ■ Durchschnitt über alle ■ Mandant Test



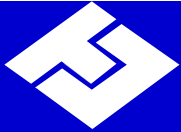
Benchmark

- Leitfaden Haftungsrisiken BITKOM 1*) -

Auszug „Strategische Aufgaben“

Nr.	Pflicht bzw. Regelungs-/ Handlungsbedarf	Verantwortlichkeiten		Persönliche Haftung ggü.		Rechtsgrundlagen der Pflicht bzw. des Regelungs-/ Handlungsbedarfs	Potentielle Schäden und sonstige Nachteile für das Unternehmen bei Pflichtverletzung bzw. Nichtregelung	Ansprüche Dritter (z.B. Kunden, Betroffene)
		Vorstand/GF	Aufsichtsrat	Unternehmen	Dritten			
1.	Sicherstellung einer bedarfs- und rechtskonformen IT-Nutzung					<ul style="list-style-type: none"> ▪ Gesellschaftsrecht § 91 II AktG ▪ § 43 GmbHG ▪ (KonTraG) 	<ul style="list-style-type: none"> ▪ Unternehmensverluste durch Ausfall der Systeme ▪ Insolvenz ▪ Verteuerung der Unternehmenskredite ▪ Ggf. Verlust von Versicherungsschutz für das Unternehmens ▪ Imageschaden nach Verlust von personenbezogenen Daten aufgrund von Sicherheitslücken 	<ul style="list-style-type: none"> ▪ Schadensersatz
						<ul style="list-style-type: none"> ▪ Gesellschaftsrecht § 116 AktG ▪ (KonTraG) 		

1*) Der vollständige Leitfaden kann unter http://www.bitkom.org/de/publikationen/38337_31034.aspx abgerufen werden

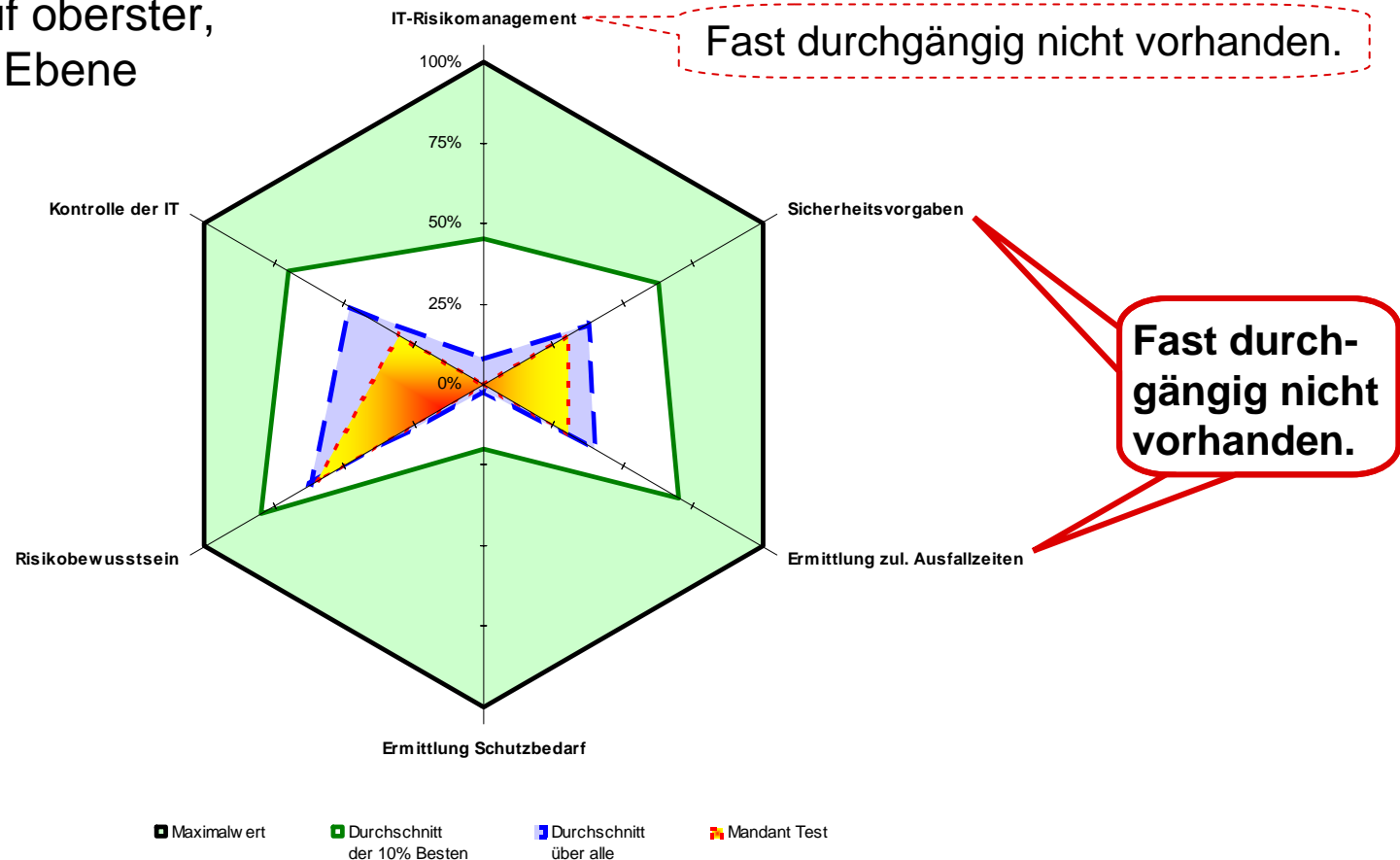


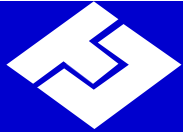
Benchmark

- IT-Umfeld -

- IT-Sicherheit auf oberster, konzeptioneller Ebene

Rubrik IT-Umfeld





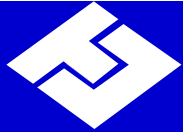
Benchmark

- Leitfaden Haftungsrisiken BITKOM 1*) -

Auszug „Konzeptionelle Aufgaben“

Nr.	Pflicht bzw. Regelungs-/ Handlungsbedarf	Verantwortlichkeiten			Persönliche Haftung ggü.		Rechtsgrundlagen der Pflicht bzw. des Regelungs-/ Handlungsbedarf	Potentielle Schäden und sonstige Nachteile für das Unternehmen bei Pflichtverletzung bzw. Nichtregelung	Ansprüche Dritter (z.B. Kunden, Betroffene)
		Vorstand/GF	behr. DSB	IT-Leiter	Unternehmen	Dritten			
1.	Einführung eines Sicherheitskonzepts (inkl. Katastrophen- und Zugriffsschutz) und eines Datenschutzkonzeptes						<ul style="list-style-type: none"> Gesellschaftsrecht § 91 II AktG / § 43 GmbHG 	<ul style="list-style-type: none"> Unternehmensverluste durch Ausfall der Systeme Insolvenz Verlust von Daten aufgrund von Sicherheitslücken Ggf. Verlust von Versicherungsschutz für das Unternehmen Verteuerung der Unternehmenskredite 	<ul style="list-style-type: none"> Schadensersatz
					*AN	*AN	<ul style="list-style-type: none"> Datenschutzrecht §9 und Anlage zu § 9 		
					*AN	*AN	<ul style="list-style-type: none"> Ergibt sich regelmäßig aus dem Arbeitsvertrag 		
2.	Ständige Aktualisierung des Sicherheits-/ Datenschutzkonzeptes				*AN	*AN	<ul style="list-style-type: none"> s. o. Ziffer 1 	<ul style="list-style-type: none"> Unternehmensverluste durch Ausfall der Systeme Verlust von Daten aufgrund von Sicherheitslücken 	<ul style="list-style-type: none"> Schadensersatz
					*AN	*AN			

1*) Der vollständige Leitfaden kann unter http://www.bitkom.org/de/publikationen/38337_31034.aspx abgerufen werden

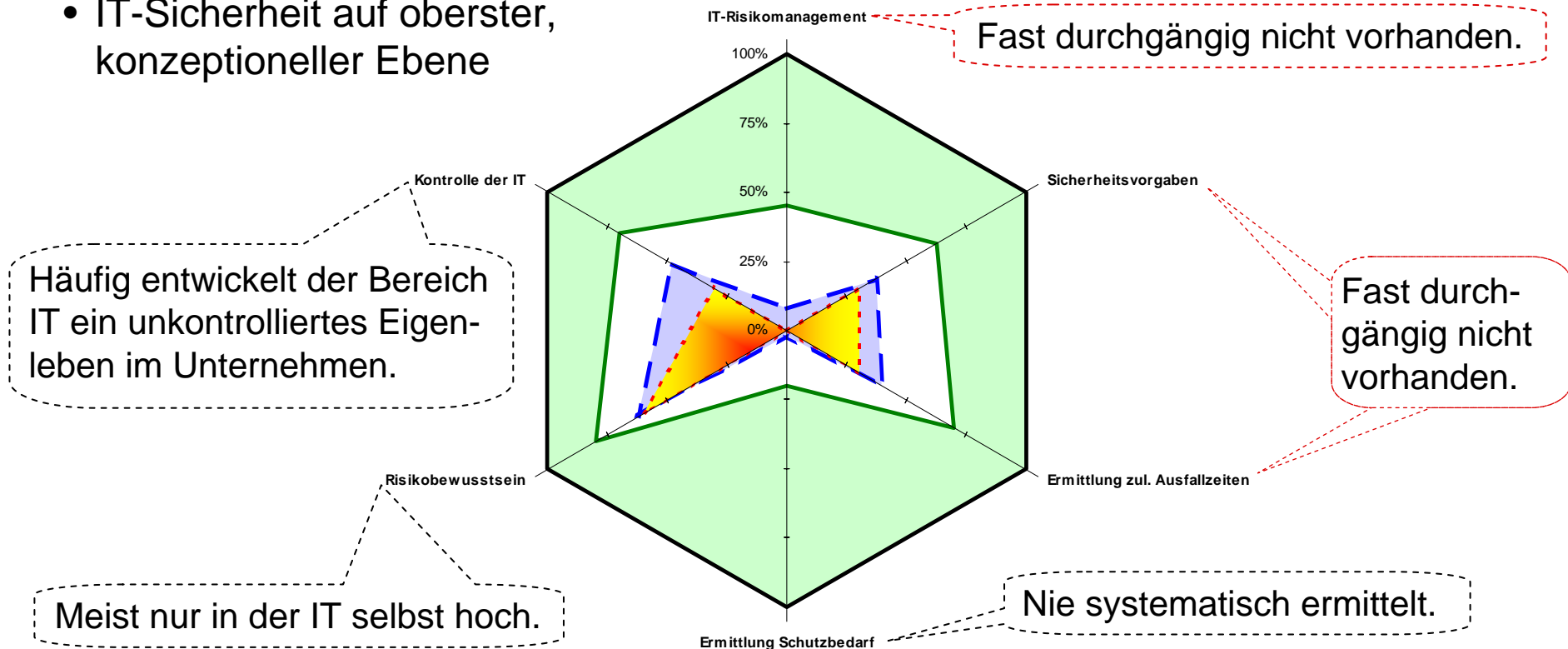


Benchmark

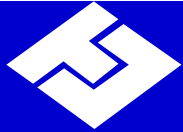
- IT-Umfeld -

Rubrik IT-Umfeld

- IT-Sicherheit auf oberster, konzeptioneller Ebene



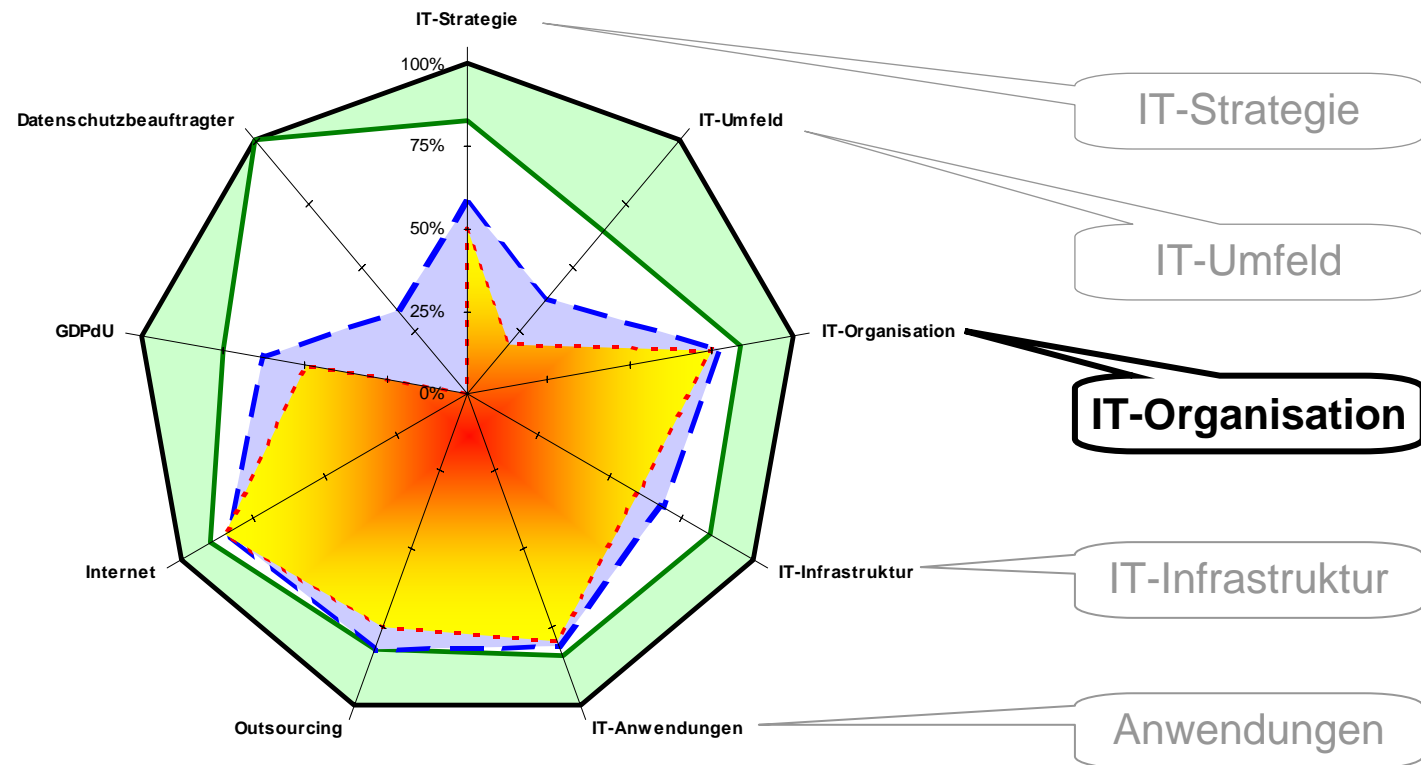
■ Maximalwert ■ Durchschnitt der 10% Besten ■ Durchschnitt über alle ■ Mandant Test



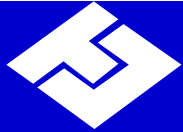
Benchmark

- Gesamtübersicht -

Gesamtübersicht



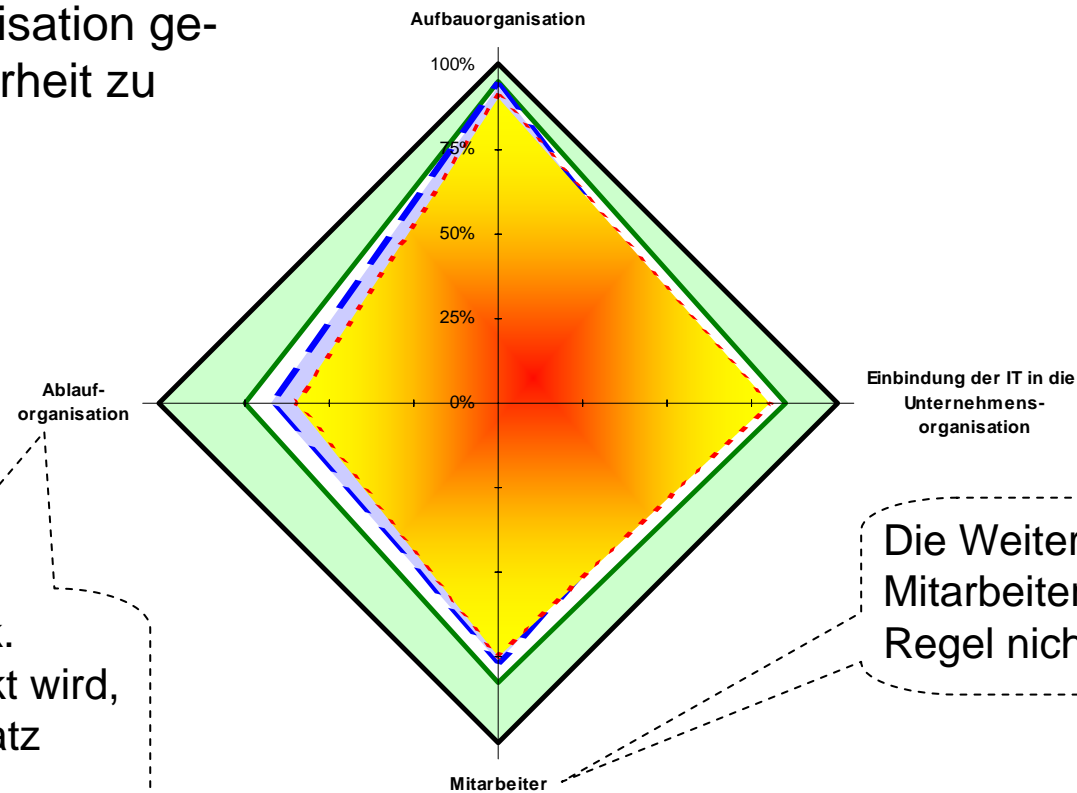
■ Maximalwert ■ Durchschnitt der 10% Besten ■ Durchschnitt über alle ■ Mandant Test



Benchmark - IT-Organisation -

Rubrik IT-Organisation

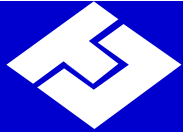
- Ist die IT-Organisation geeignet, IT-Sicherheit zu unterstützen.



IT ist ein Kostenblock. Was in die IT gesteckt wird, soll sich in Mehrumsatz rechnen.

Die Weiterbildung der Mitarbeiter wird in der Regel nicht geplant.

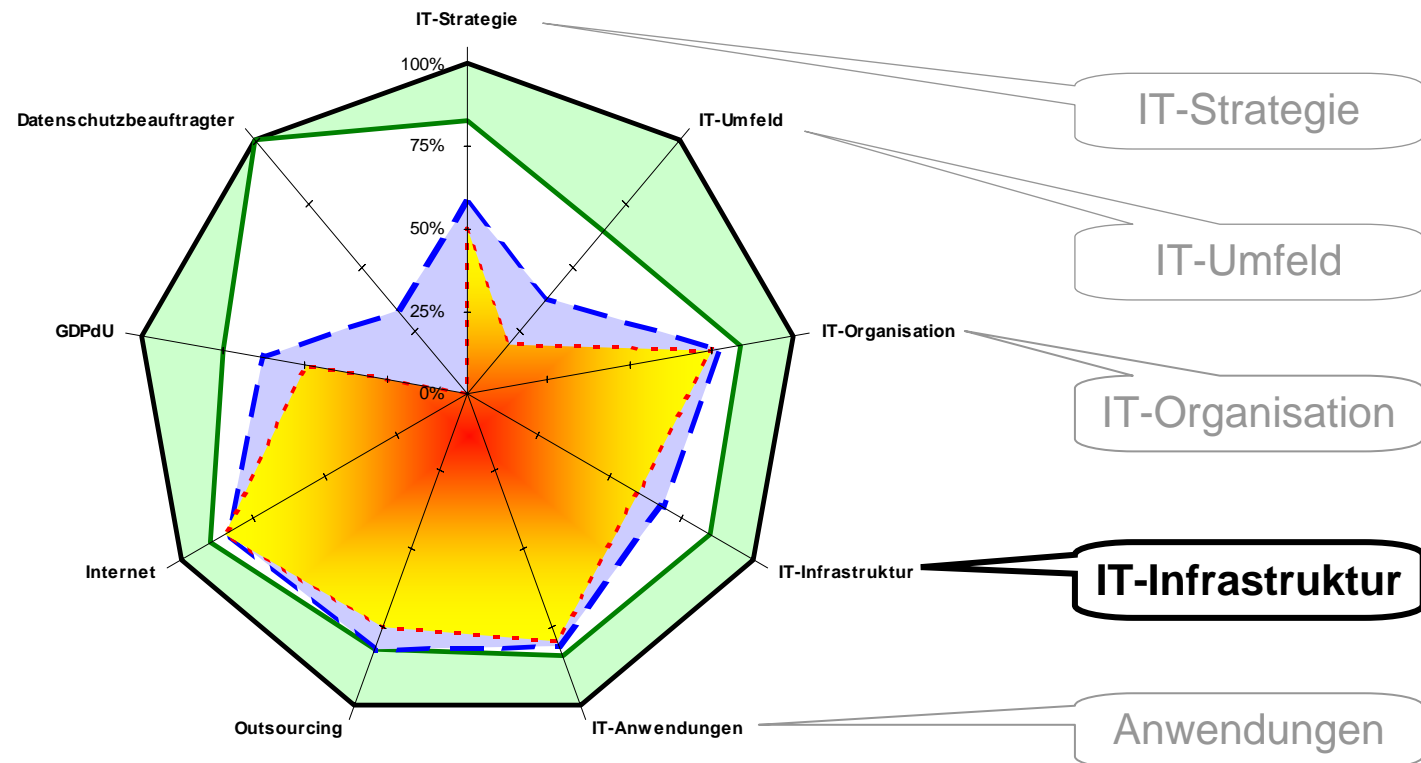
■ Maximalwert ■ Durchschnitt der 10% Besten ■ Durchschnitt über alle ■ Mandant Test



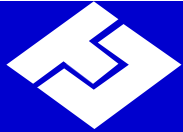
Benchmark

- Gesamtübersicht -

Gesamtübersicht

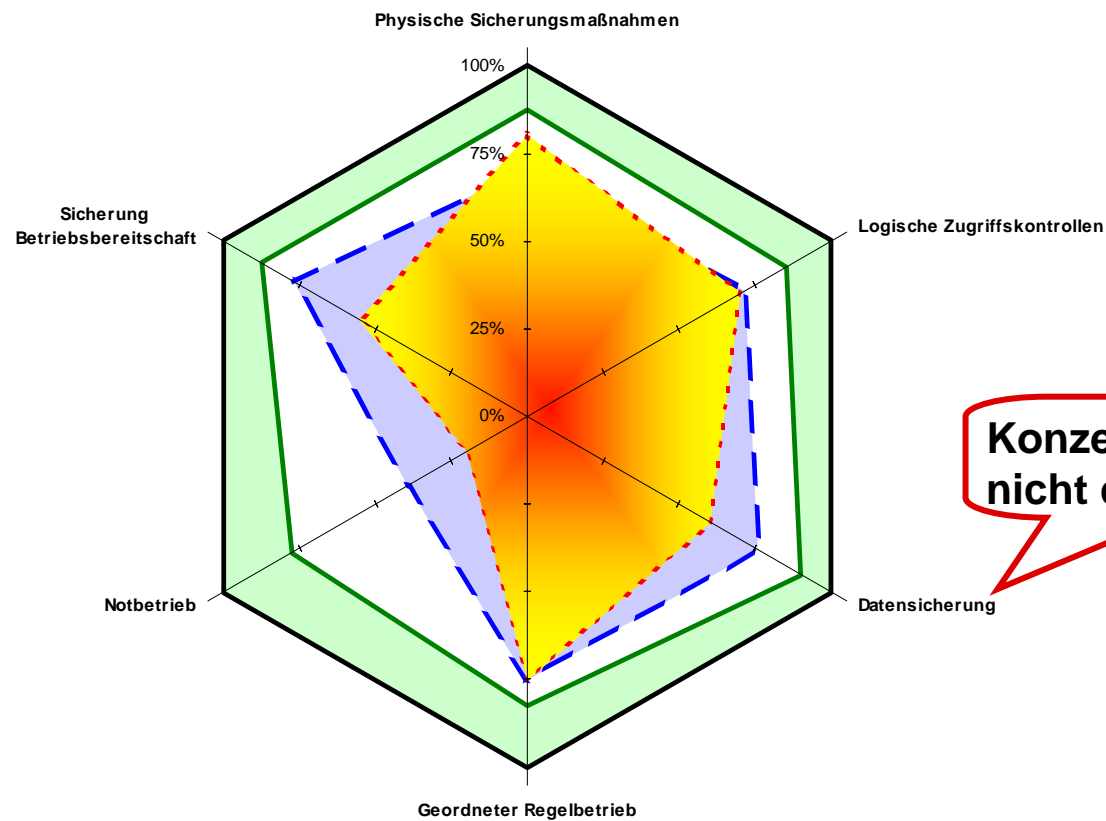


■ Maximalwert ■ Durchschnitt der 10% Besten ■ Durchschnitt über alle ■ Mandant Test



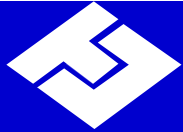
Benchmark - IT-Infrastruktur -

Rubrik IT-Infrastruktur



Konzepte sind häufig nicht dokumentiert.

■ Maximalwert ■ Durchschnitt der 10% Besten ■ Durchschnitt über alle ■ Mandant Test



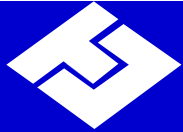
Benchmark

- Leitfaden Haftungsrisiken BITKOM 1*) -

Auszug „Operative Aufgaben“

Nr.	Pflicht bzw. Regelungs-/ Handlungsbedarf	Verantwortlichkeit				Persönliche Haftung ggü		Rechtsgrundlagen der Pflicht bzw. des Regelungs-/ Handlungsbedarfs	Potentielle Schäden und sonstige Nachteile für das Unternehmen bei Pflichtverletzung bzw. Nichtregelung	Ansprüche Dritter (z.B. Kunden, Betroffene)
		Vorstand/GF	betr. DSB	IT-Leiter	Mitarbeiter	Unternehmen	Dritten			
6.	Durchführung regelmäßiger Backups							<ul style="list-style-type: none"> ▪ Erhebliche Behinderungen bis hin zum Unternehmensstillstand bei Datenverlusten ▪ Produktionsausfall ▪ Sonstige Vermögensverluste ▪ Imageverlust ▪ Datenverlust ▪ Wegen überwiegenden Mitverschuldens auch kein Schadensersatz von Dritten, die Datenverluste verursachen 	<ul style="list-style-type: none"> ▪ Schadensersatz von Vertragspartnern Zivilrecht §§ 280 I / § 254 BGB (nur ggü. Dritten) 	
						*AN	*AN			
						*AN	*AN			

1*) Der vollständige Leitfaden kann unter http://www.bitkom.org/de/publikationen/38337_31034.aspx abgerufen werden

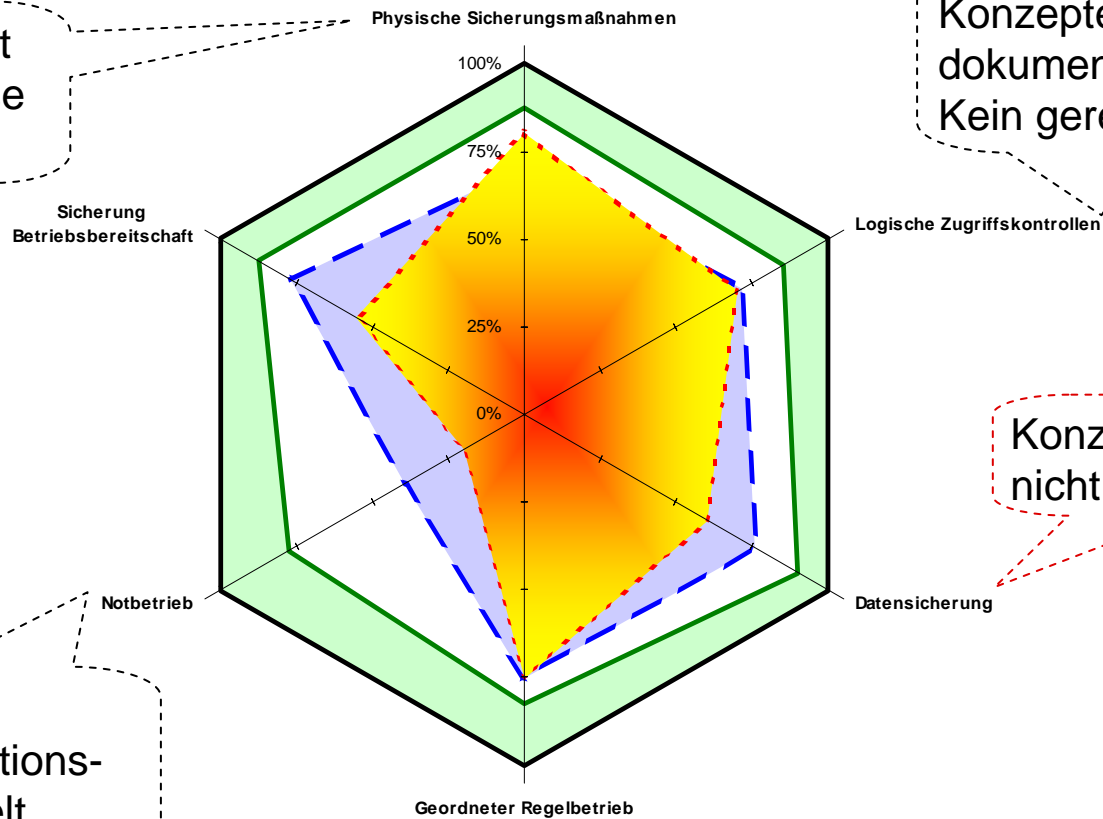


Benchmark - IT-Infrastruktur -

Rubrik IT-Infrastruktur

Zusammenhang mit Unternehmensgröße ist erkennbar.

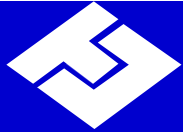
Konzepte sind nicht dokumentiert. Kein geregelter Prozess.



Konzepte sind häufig nicht dokumentiert.

Selten vorhanden. Es wird auf „Situationsintelligenz“ abgezielt.

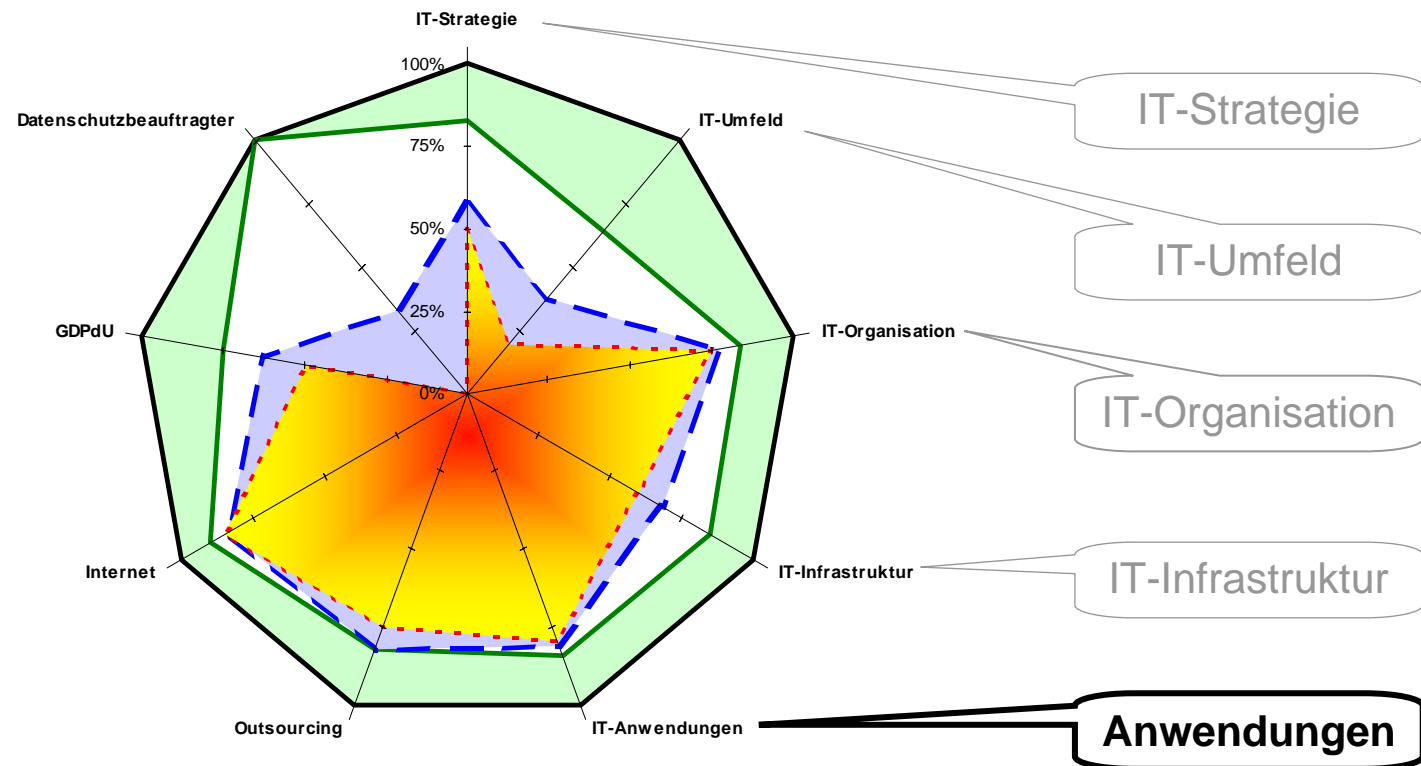
■ Maximalwert ■ Durchschnitt der 10% Besten ■ Durchschnitt über alle ■ Mandant Test



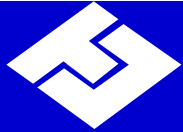
Benchmark

- Gesamtübersicht -

Gesamtübersicht



■ Maximalwert ■ Durchschnitt der 10% Besten ■ Durchschnitt über alle ■ Mandant Test



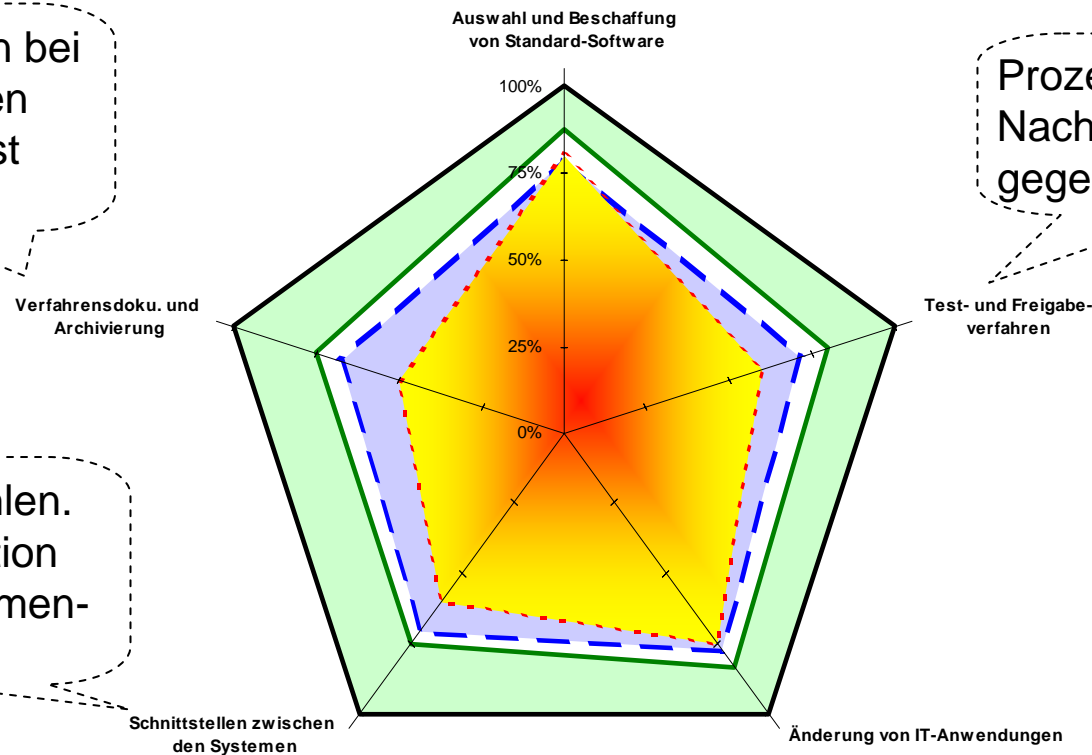
Benchmark - IT-Anwendungen -

Rubrik IT-Anwendungen

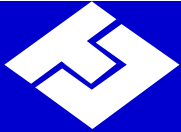
Die Dokumentation bei Eigenentwicklungen und Änderungen ist schwach.

Prozess nicht geregelt. Nachweisbarkeit nicht gegeben.

Kontrollschritte fehlen. Keine Dokumentation der Systemzusammenhänge.



■ Maximalwert ■ Durchschnitt der 10% Besten ■ Durchschnitt über alle ■ Mandant Test

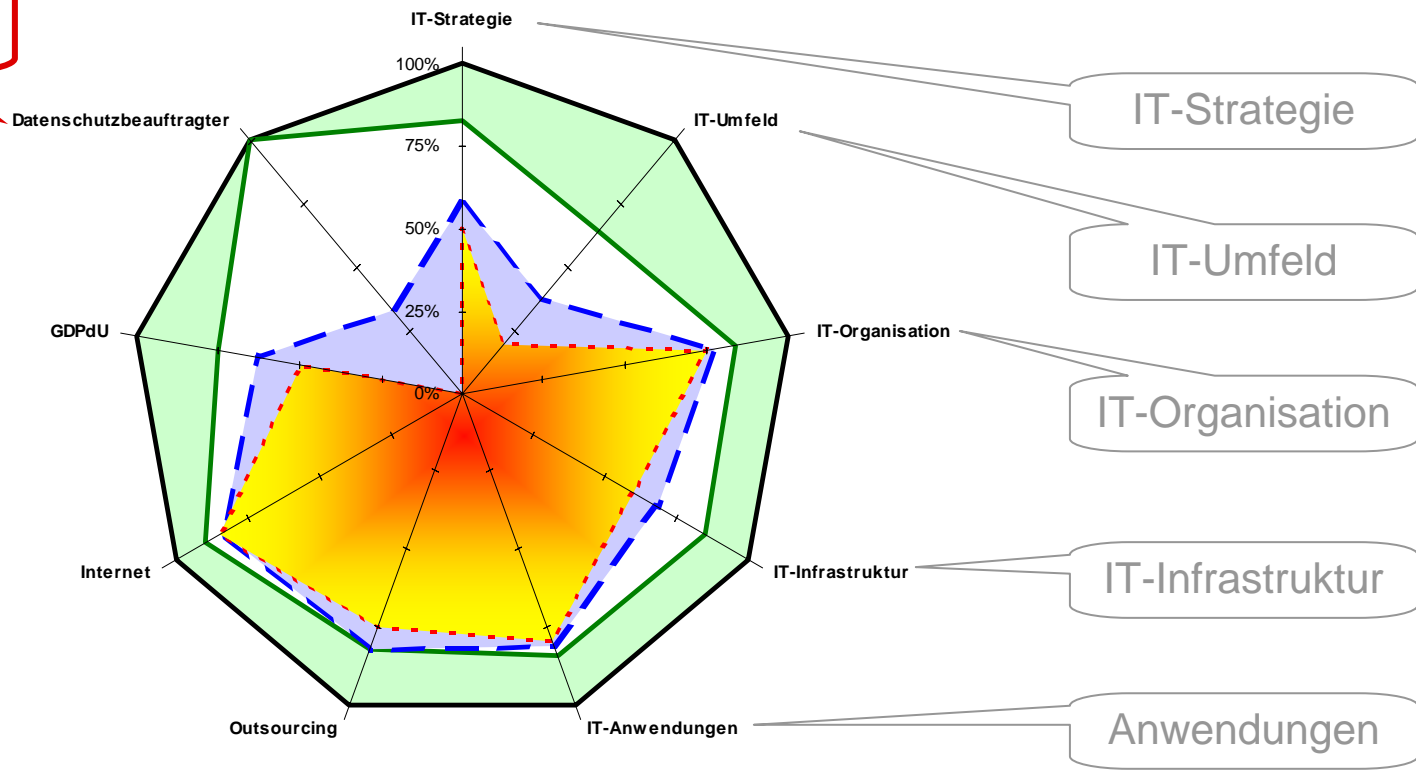


Benchmark

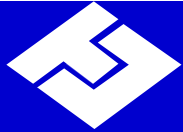
- Gesamtübersicht -

Gesamtübersicht

Die 10% Besten haben einen bestellt.



■ Maximalwert ■ Durchschnitt der 10% Besten ■ Durchschnitt über alle ■ Mandant Test



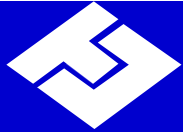
Benchmark

- Leitfaden Haftungsrisiken BITKOM 1*) -

Auszug „Operative Aufgaben“

Nr.	Pflicht bzw. Regelungs-/ Handlungsbedarf	Verantwortlichkeit				Persönliche Haftung ggü		Rechtsgrundlagen der Pflicht bzw. des Regelungs-/ Handlungsbedarfs	Potentielle Schäden und sonstige Nachteile für das Unternehmen bei Pflichtverletzung bzw. Nichtregelung	Ansprüche Dritter (z.B. Kunden, Betroffene)
		Vorstand/GF	betr. DSB	IT-Leiter	Mitarbeiter	Unternehmen	Dritten			
2.	Datenschutzrechtliche Konformität sicherstellen							<ul style="list-style-type: none"> Datenschutzrecht § 7 BDSG / § 9 BDSG § 43 BDSG § 44 BDSG Gesetz gegen unlauteren Wettbewerb § 3, 4 Nr. 11 UWG § 10 	<ul style="list-style-type: none"> Aufsichtsbehörde kann Maßnahmen zur Beseitigung anordnen oder auch den Einsatz einzelner Verfahren untersagen, dadurch erhebliche Behinderungen bis hin zum Unternehmensstillstand, Produktionsausfall, sonstige Vermögensverluste, z.B. Ersatz bzw. Modifikation der Verfahren Kosten durch Pflicht zur Abberufung des DS-Beauftragten und Einsetzung eines neuen Bußgeld bis € 250.000 § 43 BDSG Zwangsgelder Freiheitsstrafe bis 2 Jahre Strafrecht § 203 StGB 	<ul style="list-style-type: none"> Schadensersatz Zivilrecht § 823, Abs. II BGB Unterlassung Abmahnung U. U. Gewinnabschöpfung § 10 UWG
						*AN	*AN	<ul style="list-style-type: none"> Datenschutzrecht §§ 4g, 38, Abs. 5 BDSG 		

1*) Der vollständige Leitfaden kann unter http://www.bitkom.org/de/publikationen/38337_31034.aspx abgerufen werden



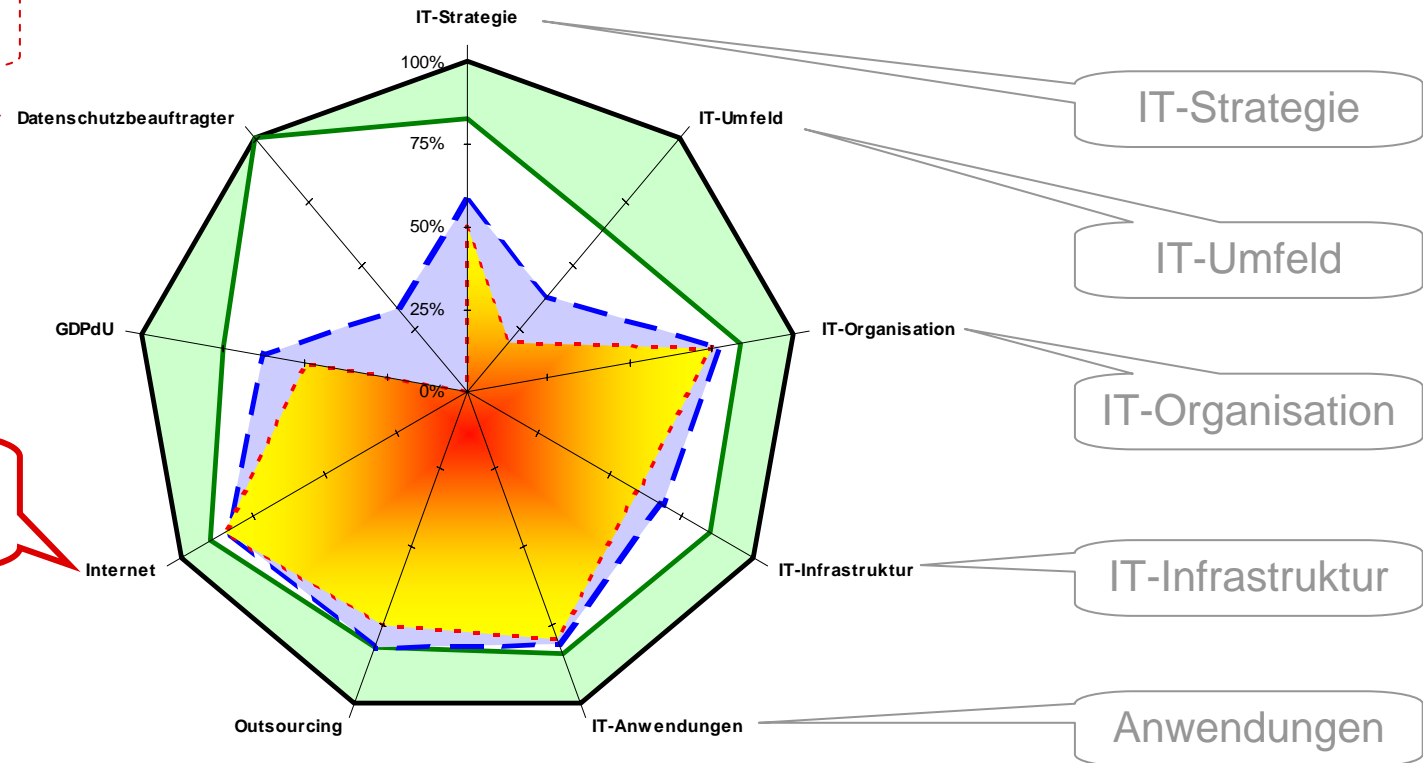
Benchmark

- Gesamtübersicht -

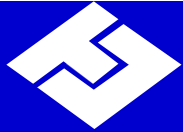
Gesamtübersicht

Die 10% Besten haben einen bestellt.

Abschottung durch Firewall und Antivirensoftware.



■ Maximalwert ■ Durchschnitt der 10% Besten ■ Durchschnitt über alle ■ Mandant Test



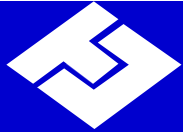
Benchmark

- Leitfaden Haftungsrisiken BITKOM 1*) -

Auszug „Operative Aufgaben“

Nr.	Pflicht bzw. Regelungs-/ Handlungsbedarf	Verantwortlichkeit				Persönliche Haftung ggü		Rechtsgrundlagen der Pflicht bzw. des Regelungs-/ Handlungsbedarfs	Potentielle Schäden und sonstige Nachteile für das Unternehmen bei Pflichtverletzung bzw. Nichtregelung	Ansprüche Dritter (z.B. Kunden, Betroffene)
		Vorstand/GF	betr. DSB	IT-Leiter	Mitarbeiter	Unternehmen	Dritten			
3.	Einsatz von SPAM- und Viren-Filtern abwägen							<ul style="list-style-type: none"> TKG § 88 TKG § 206 II Nr. 2 StGB Strafrecht § 85 II TKG i.V.m. § 206 II Nr. 2 StGB oder § 303 a StGB 	<ul style="list-style-type: none"> Schäden und Nachteile unterschiedlich, je nach Vorgehen der Unternehmensleitung: <ul style="list-style-type: none"> Verzicht auf E-Mail Filter: Haftung ggü. Dritten bei tatsächlichen Schäden (z.B. Datenverlust durch Viren) Einsatz von E-Mail Filter: u. U. rechtliche und praktische Probleme mit Mitarbeitern und Dritten Schaden durch Vernichtung wichtiger Information Freiheitsstrafe bis zu 5 Jahren oder Geldstrafe 	<ul style="list-style-type: none"> Unterlassung Schadensersatz Zivilrecht § 823 Abs. 2 BGB § 1004 BGB i.V.m. § 40 TKG Schadensersatz Kosten bei Unterlassungsklage, evtl. einstweiligem Verfügungsverfahren bzw. Abmahnung
4.	Regelung für die Nutzung von E-Mail und Internet am Arbeitsplatz							<ul style="list-style-type: none"> Grundgesetz Art.2 i.V.m. Art.1 Zivilrecht §§ 611, 242 BGB Datenschutzrecht §§ 1 II; 27 I BDSG Telekommunikationsgesetz §§ 1, 88, 89, 91ff TKG Teledienstegesetz § 1f. TDG Teledienstedatenschutzgesetz §§ 3-6 TDDSG. Ggf. Betriebsverfassungsgesetz §§ 75, 80, 87, 88, 90 BetrVG 	<ul style="list-style-type: none"> Verstöße gegen Datenschutzvorschriften Mangelnde Transparenz/Mangelnde Kontrollmöglichkeiten Kosten durch die Dienstenutzung durch die Mitarbeiter Imageschäden Beschlagnahme 	

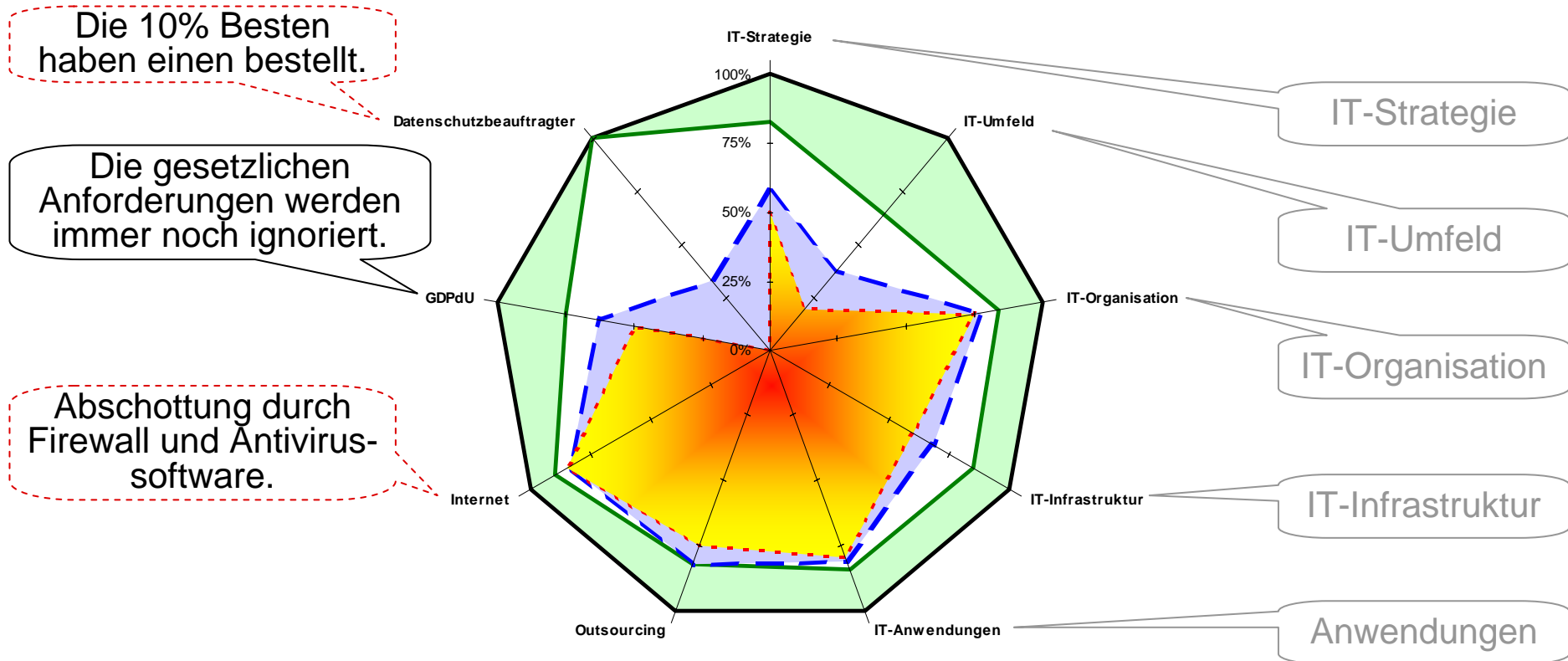
1*) Der vollständige Leitfaden kann unter http://www.bitkom.org/de/publikationen/38337_31034.aspx abgerufen werden



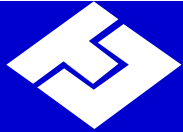
Benchmark

- Gesamtübersicht -

Gesamtübersicht



■ Maximalwert ■ Durchschnitt der 10% Besten ■ Durchschnitt über alle ■ Mandant Test



Benchmark

- Haftungsausschluss -

- Bei GmbH's kann im Geschäftsführervertrag eine Haftungsbeschränkung für fahrlässiges Verhalten festgeschrieben werden. Bei AG's ist das nicht möglich.
- Versicherungen wie die „directors & officers liability insurance“ greifen nicht bei wissentlicher Pflichtverletzung des Versicherten. Da heute das Wissen über IT-Risiken schon weit verbreitet ist, kann mangelhafte IT-Sicherheit schnell als Pflichtverletzung ausgelegt werden.

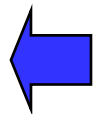
Fazit: Ein **Haftungsausschluss** ist nur **eingeschränkt** möglich.

Deshalb sollten **vorbeugende Maßnahmen** ergriffen werden.



Inhaltsverzeichnis

I	Einleitung	Seite 4
II	Benchmark	Seite 7
III	IT-Sicherheitsmanagement	Seite 43





IT-Sicherheitsmanagement

- Treiberfaktoren -

- **Gesicherte** Kenntnis über die möglichen Risiken und deren Kosten und Eintrittswahrscheinlichkeiten.
- **Verbesserte** Unterstützung der Geschäftsprozesse durch mehr Transparenz.
- **Anforderungsgerechte** Bereitstellung von Informationen.
- Geheimhaltung **sensibler Unternehmensdaten**.
- **Funktionsstüchtiges Netzwerk** mit Geschäftspartnern.
- **Positiver Imageeffekt** bei Partnern, Kunden, Lieferanten und Umwelt.
- **Vermeidung** von persönlicher Haftung, Bußgeldern, Geldstrafen oder Zulassungsentzug.
- **Günstigere** Unternehmenskredite (Basel II).
- **Erhalt** von Versicherungsschutz.



IT-Sicherheitsmanagement

- IT-Sicherheitsstandards / Best Practices -

Gängige Standards zum Sicherheitsmanagement.

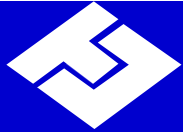
- ISO 17799 (Best Practices zum Management von Informationssicherheit).
- ISO 2700X (Sicherheitsleitfaden. Z.T. abgeleitet aus dem British Standard 7799).
- IT-GSHB (Grundschatzhandbuch des BSI).

Standards für Bewertung und Zertifizierung von IT-Sicherheit.

- ITSEC (Information Technology Security Evaluation Criteria).
- CC (Common Criteria, basiert auf ISO 15408).

Best Practices für IT-Sicherheit.

- Cobit (Control Objectives for Information and Related Technologie) .
- Prüfungsstandard 330, 331, 880 und Fait 1, 2, 3 des Institut der Wirtschaftsprüfer.
- ITIL (IT-Infrastructure Library).



IT-Sicherheitsmanagement

- Umsetzungsprojekt -

Phasen bei Einführung eines IT-Sicherheitsmanagements:

- Vorgaben der Unternehmensleitung an die IT und die IT-Sicherheit
- Aufbau eines Risikofrüherkennungssystems
- Feststellung des Schutzbedarfs der Komponenten
- Erarbeitung von Maßnahmen zur Risikominimierung
- Durchführung von „make or buy“ Untersuchungen (Nutzung von managed security services [mms] oder eigene Administration)
- Erstellung und Umsetzung spezifischer Sicherheitskonzepte (Datensicherung, Zugriffsschutz, Notfallkonzept, ...)
- Erstellung und Umsetzung von Policies (Datenschutz, eMail- und Internetnutzung, Anwenderrichtlinien, ...)
- Installation von Prozessen zur Gewährleistung der Kontinuität des Sicherheitsmanagements



TU UNTERNEHMENSBERATUNG GMBH

Vielen Dank!

TU Unternehmensberatung GmbH

Dipl.-Ing., Dipl.-Wirt.-Ing.

Torsten Vick-Lehnberg

Langenweg 55

26125 Oldenburg

0441-9710-254

(www.tu-unternehmensberatung.de)