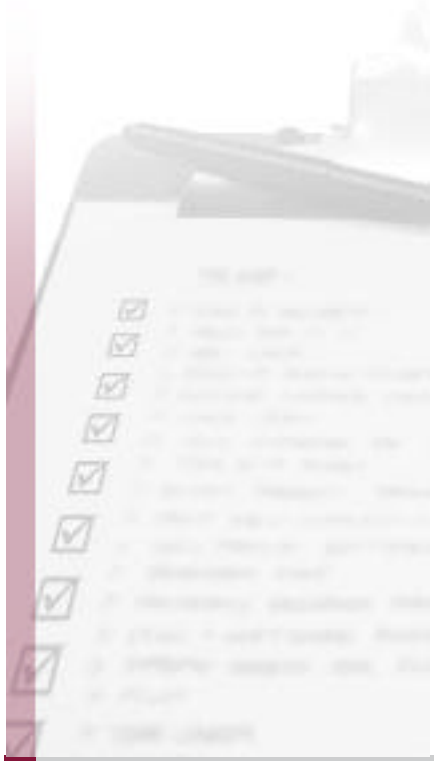
IDW PS 330 contra BSI GSHB und BS7799 am Beispiel mittelständischer Unternehmen

.consulting .solutions .partnership

Florian Oelmaier, msg systems ag

Agenda

1. Vorstellung
2. Hintergründe
3. Prüfungsstandard
4. Zusammenfassung
5. Fragen / Diskussion



Überblick msg systems ag

.consulting .solutions .partnership

Als produktbasiertes Lösungs- und Service-Haus agieren wir unter den Top 25 der IT-Berater und Systemintegratoren in Deutschland.

Kerngeschäft:	**Branchenspezifische Gesamtlösungen** (Beratung, Anwendung, Systemintegration)
Gründung:	**1980**
Geschäftssitz:	**Ismaning / München**
Vorstand:	**Hans Zehetmaier (Vorsitzender)** **Karl-Martin Klein** **Pius Pflügler** **Volker Reichenbach**
Mitarbeiter:	**> 2000**

Standorte

.consulting .solutions .partnership

Leistungsspektrum

Kompetenz zur Beratung und Durchführung sämtlicher Projekte im Bereich der IT Sicherheit mit langjährigem Schwerpunkt im Bereich Applikationssicherheit.

Leistungsspektrum

- Full-Service für Business-Lösungen
- Individuelle Anwendungsentwicklung
- SAP-Beratung und -Entwicklung

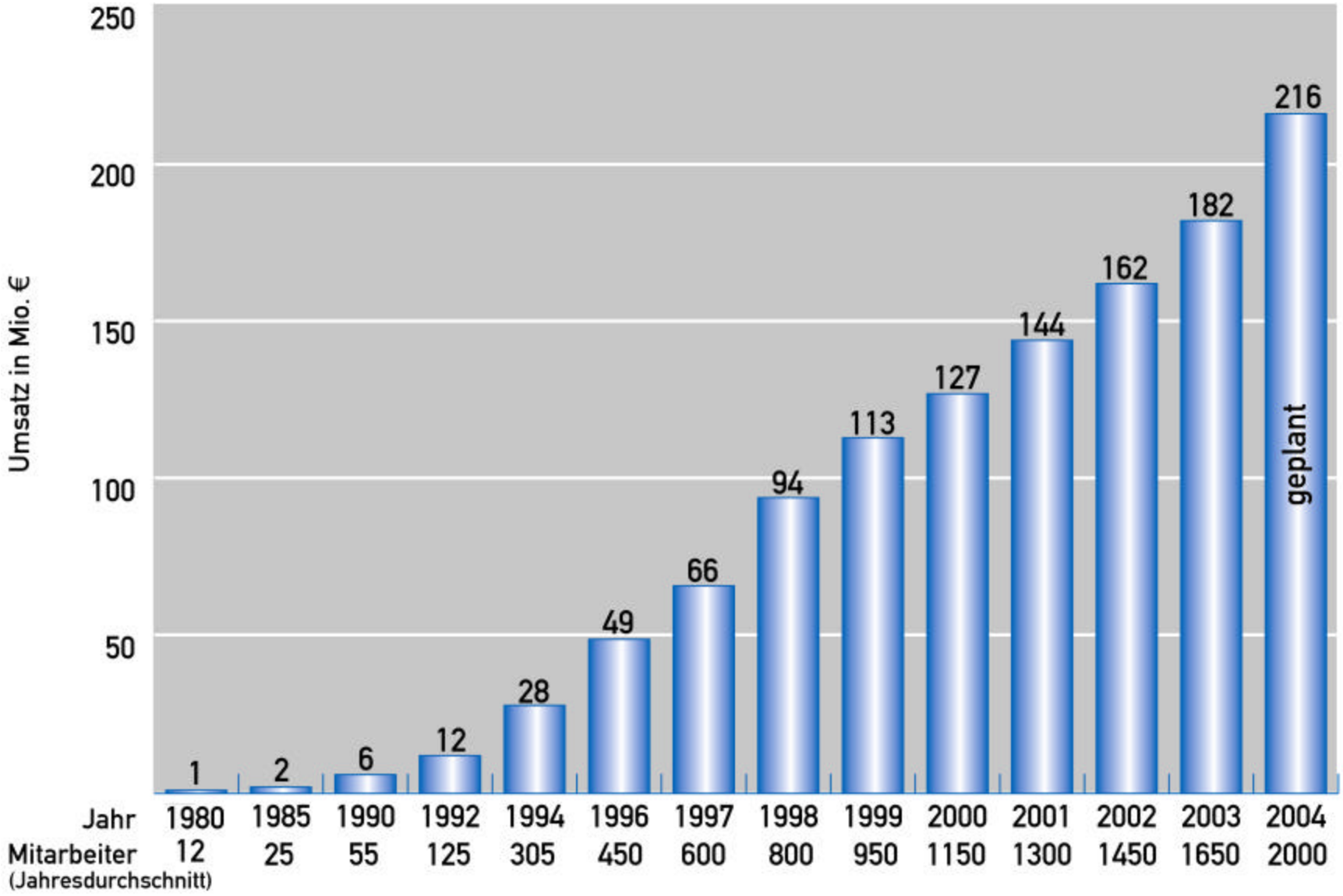
Branchenlösungen

- Versicherungen
- Finanzdienstleistungen
- Gesundheitswesen

Seit 1996 nach DIN EN ISO 9001 zertifiziert

Umsatz- und Mitarbeiterentwicklung

.consulting .solutions .partnership



Branchen und Kunden (Auszug)

.consulting .solutions .partnership

Versicherungen

- ADAC-Versicherung
- Allstate, USA
- Allianz
- AMB Generali
- AOK
- Aspecta
- AXA
- Basler Versicherungen,CH
- Bayer. Beamten Vers.
- Folksam
- Gerling
- Gothaer Rück
- Hannover Rück
- Helvetia Patria, CH
- HUK Coburg
- Münchener Rück
- NÜRNBERGER Vers.
- Quelle Versicherungen
- Sparkassenversicherung
- UNIQA
- Versicherungskammer Bayern
- Wiener Städtische, A
- Winterthur, CH
- Zurich Fin. Services, CH

Finanzdienstleistungen

- Bankgesellschaft Berlin
- Bayerische Landesbank
- BHW
- BMW Financial Services
- Commerzbank
- Deutsche Bank
- DZ BANK
- Dresdner Bank
- Deutsche Börse Systems
- Finanz IT
- HELABA
- HSBC Trinkaus & Burkhardt
- HSH Nordbank
- IZB SOFT
- Bayerische Landesbausparkasse (LBS)
- Sparkassen Informatik
- Bausparkasse Schwäbisch Hall
- Stadtsparkasse Köln
- VW Financial Services
- WestLB

Gesundheitswesen

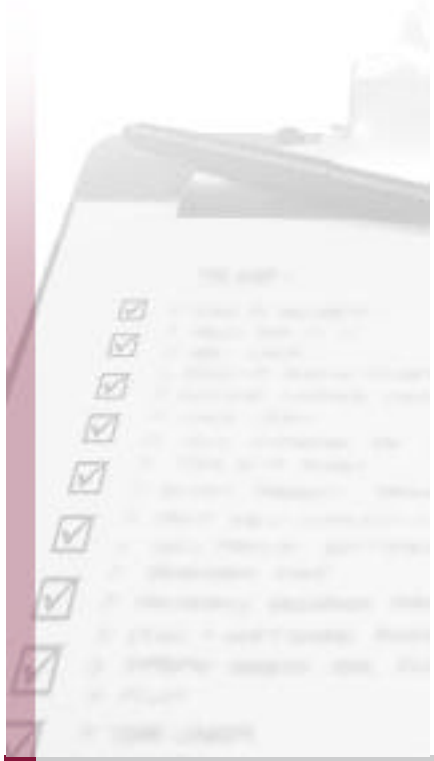
- Allianz PKV
- BARMER Ersatzkasse
- Bau Berufsgenossenschaft Rheinland/Westf.
- BKK Allianz
- BKK Berlin
- BKK futur
- Bundesinnungskrankenkasse Gesundheit(BIG)
- Deutsche Krankenversicherung (DKV)
- DRG-Institut (IneK gGmbH)
- Hanseatische KK
- IKK-Bundesverband
- IKK Sachsen-Anhalt
- Johanniter-Krankenhaus Bonn
- Kaiserswerther Diakonie
- Kliniken d. Landesverbandes Rheinland
- PKV Verband
- SIGNAL Krankenvers.
- Techniker Krankenkasse

Industrie/Behörden/Touristik

- AUDI AG
- BMW AG
- Brunata
- Bundeswehr/-Marine
- Deutsche Telekom
- E.ON
- Europ. Patentamt
- GASAG
- Gebühreneinzugszentrale (GEZ)
- Hoffmann Werkzeuge
- Messer Griesheim
- PREMIERE
- Renault Nissan Deutschland
- Rolls Royce Deutschland
- TUI
- VW AG
- Wacker-Chemie

Agenda

1. Vorstellung
2. Hintergründe
3. Prüfungsstandard
4. Zusammenfassung
5. Fragen / Diskussion



Warum prüfen Wirtschaftsprüfer IT-Systeme?

Erfahrungen aus Enron, Worldcom & Co.

- **Steuerumgehung**
- **Intransparenz**
- **Bereicherung**
- **Kontrollverlust**

=> Vertrauensverlust in die Wirtchaft

Warum prüfen Wirtschaftsprüfer IT-Systeme?

Gesetzlicher Auftrag:

- **Der Jahresabschluss eines Unternehmens hat unter Beachtung der Grundsätze ordnungsgemäßer Buchführung ein den tatsächlichen Verhältnissen entsprechendes Bild der Vermögens-, Finanz- und Ertragslage zu vermitteln (§264 HGB)**
- **Ein Wirtschaftsprüfer hat seine Prüfung so anzulegen, dass Unrichtigkeiten und Verstöße gegen diese Pflicht erkannt werden (§§ 317 HGB)**

Warum prüfen Wirtschaftsprüfer IT-Systeme?

IT-Systeme können dabei nicht außen vor bleiben:

- **Controlling und Verwaltung sind essentiell vom IT-Einsatz abhängig**
- **IT ist in fast allen Unternehmen ein wichtiger Produktionsfaktor**
- **Gesetzliche Vorschriften, die die Prüfung von Risiken auch durch IT-Einsatz vorschreiben (KontraG)**
- **(Basel II)**

Warum prüfen Wirtschaftsprüfer IT-Systeme?

- **Forderung des internationalen Dachverbands IFAC (International Federation of Accountants)**
- **Nationale Umsetzung des internationalen Auditing Standards ISA 401**
- **Institut der Wirtschaftsprüfer empfiehlt die Aufnahme einer Prüfung nach PS330 in den Prüfungsplan (keine jährliche Wiederholung!)**

Wann ist ein Unternehmen prüfungspflichtig?

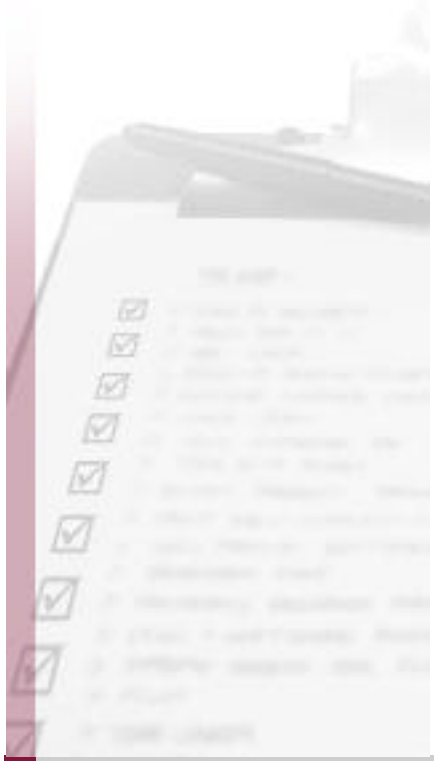
- **Jedes Unternehmen kann seinen Abschluss freiwillig prüfen lassen**
- **Prüfungspflichtig sind mittelgroße und große Kapitalgesellschaften nach HGB, d.h. wenn 2 der drei Kriterien erfüllt bzw. überschritten sind besteht Prüfungspflicht (die Beträge gelten ab dem Wirtschaftsjahr 2004):**
  - 4.015 TEUR Bilanzsumme nach Abzug eines auf der Aktivseite ausgewiesenen Fehlbetrags
  - 8.030 TEUR Umsatzerlöse in den zwölf Monaten vor Abschlussstichtag
  - Im Jahresdurchschnitt fünfzig Arbeitnehmer

Vorteile der Prüfungen für Unternehmen

- Notwendig für einen uneingeschränkten Bestätigungsvermerk im Abschluss
- Wirtschaftlichen Schaden vermeiden (Haftung des WP!)
- Persönliche Haftung durch IT-Leiter und Geschäftsführer „abwenden“
  (OLG Hamm: positive Vertragsverletzung aus seinem Arbeitsvertrag bei angestelltem IT-Leiter wegen Nicht-Einhaltung der Sicherheitspolicy => persönlich finanziell verantwortlich)
- Gesetzliche Vorgaben erfüllen
- Außendarstellung gegenüber z.B. der Kreditwirtschaft (Basel II?)

Agenda

1. Vorstellung
2. Hintergründe
3. Prüfungsstandard
4. Zusammenfassung
5. Fragen / Diskussion

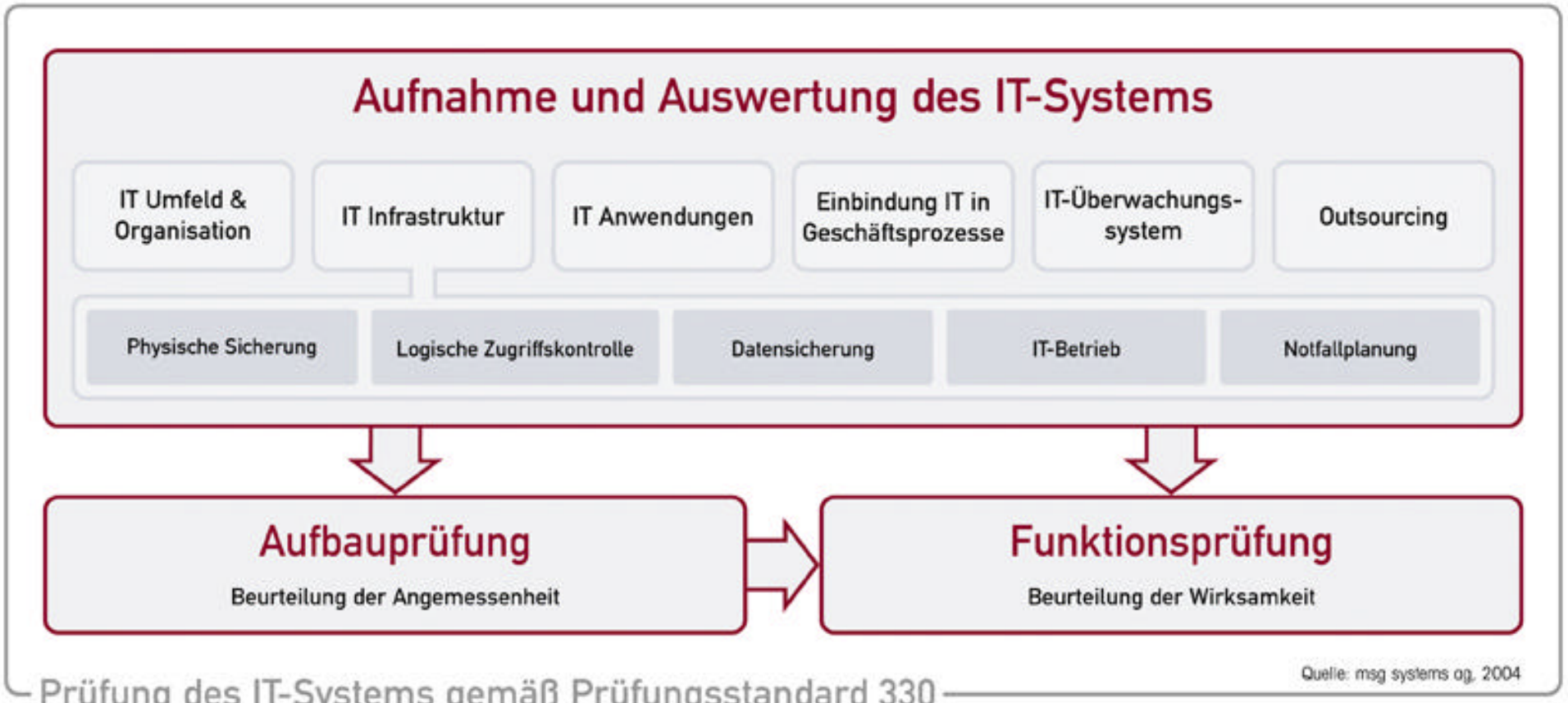


Prüfungsumfang ist eingeschränkt auf IT-Systeme die dazu dienen, Daten zu verarbeiten die direkt oder indirekt „rechnungslegungs-relevant“ sind, d.h. für:

- **Buchführung**
- **Jahresabschluss**
- **Lagebericht**

D.h. in Prosa: alle IT-Systeme, durch deren Gefährdung dem Unternehmen oder dessen Eigentümern ein wirtschaftlicher Schaden entstehen könnte.

IDW PS-330 Prüfungsumfang



Prüfung des IT-Systems gemäß Prüfungsstandard 330

IDW PS330 Prüfungskriterien

- **Vollständigkeit**
- **Richtigkeit**
- **Zeitgerechtigkeit**
- **Ordnung**
- **Nachvollziehbarkeit**
- **Unveränderlichbarkeit**

Die „üblichen“ IT-Sicherheitsziele werden dementsprechend als „nur“ Voraussetzung behandelt:

- **Authentizität**
- **Autorisierung**
- **Vertraulichkeit**
- **Verbindlichkeit**
- **Integrität**
- **Verfügbarkeit.**

IDW PS330 Risikoindikatoren

- **Abhängigkeit**
- **Änderungen**
- **Know-How und Ressourcen**
- **Geschäftliche Ausrichtung**

Anzuwenden auf Unternehmens- und Prüffeldebene.

Keine „statische“ Prüfung, sondern:

- **Prüfung der Angemessenheit**

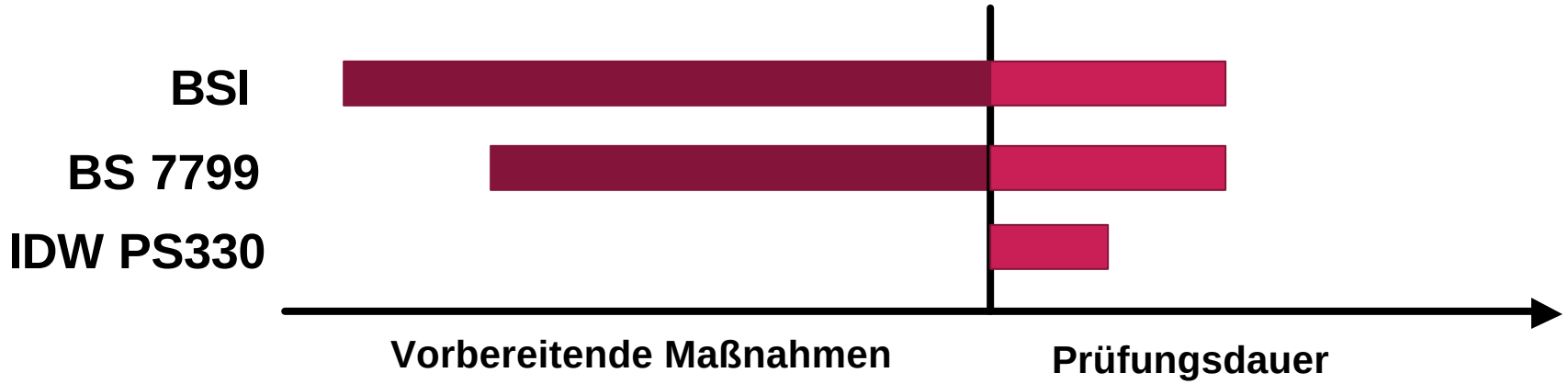
Genügt das IT-System (Dokumentationslage!) in den Augen des Prüfers den Anforderungen des Unternehmens (Größe, Markt, etc.)?

- **Prüfung der Wirksamkeit**

Sind die dokumentierten bzw. geplanten Maßnahmen wirksam umgesetzt und werden sie gelebt?

Aufwand für vergleichbare Prüfungen

- \+ kein Vorbereitung der IT für die Zertifizierung notwendig
- \+ geringer Zeitaufwand = geringe Kosten
- \+ gute Verwendbarkeit als „Lagebericht“ der IT-Sicherheit
- \- Qualität der Prüfung in hohem Maß abhängig von der Qualität des Prüfers
- \- Direkte Vergleichbarkeit (ohne Einsicht in die Prüfungsunterlagen) schwierig



Prüfungsumfeld

- **Prüfung wird nicht immer von den WPs selbst sondern von Spezialisten erledigt (Verwendung der Arbeit eines anderen Prüfers nach IDW PS 320)**
- **Buchhaltungssoftware selbst wird vom Programmhersteller meist bei einem Wirtschaftsprüfer zertifiziert (Korrekte Funktionsweise nach IDW PS 880)**
- **Oft kombiniert mit den Vorbereitungen auf die elektronische Buchprüfung**

Einordnung vergleichbarer Prüfungen

	IDW PS330	BSI	BS 7799
Zertifizierung	Zertifiziert durch Wirtschaftsprüfer (WP)	Grundschutzzertifikat BSI	BS-7799-Zertifikat durch akkred. Unternehmen
Abhängigkeit v. Prüfer	Hoch	Kaum	Mittel
„Schwerpunkt“ der Prüfung	Rechnungslegungs-relevante IT-Systeme	Definierter IT-Verbund (meist gesamte IT)	IT-Organisation
Zielpublikum	Prüfungspflichtige Unternehmen (auch KMU!)	Behörden, Institute, auch Wirtschaft	größere Firmen mit definierter Org.
Herkunft	Aus der Sicht WP / Juristen /Geschäftsleitung	Von IT-Fachleuten für IT-Fachleute	Qualitätssicherung, betriebliche Unternehmensorg.

Vielen Dank für die Aufmerksamkeit !

.consulting .solutions .partnership

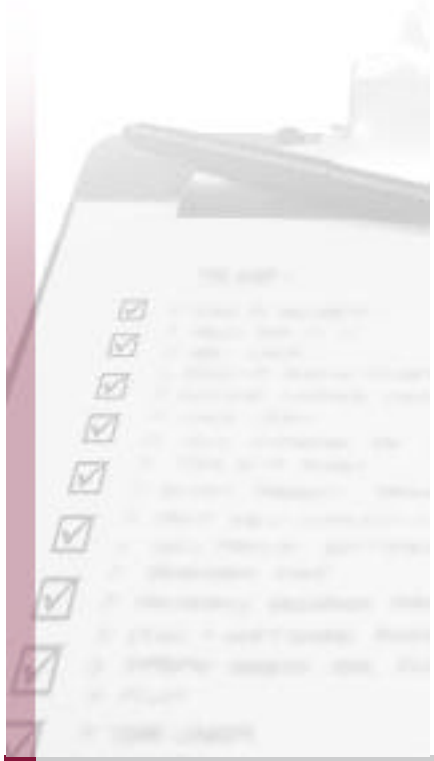
IDW PS 330 contra BSI GSHB und BS7799 am Beispiel mittelständischer Unternehmen

.consulting .solutions .partnership

Florian Oelmaier, msg systems ag

Agenda

1. Vorstellung
2. Hintergründe
3. Prüfungsstandard
4. Zusammenfassung
5. Fragen / Diskussion



Überblick msg systems ag

.consulting .solutions .partnership

Als produktbasiertes Lösungs- und Service-Haus agieren wir unter den Top 25 der IT-Berater und Systemintegratoren in Deutschland.

Kerngeschäft:	**Branchenspezifische Gesamtlösungen** (Beratung, Anwendung, Systemintegration)
Gründung:	**1980**
Geschäftssitz:	**Ismaning / München**
Vorstand:	**Hans Zehetmaier (Vorsitzender)** **Karl-Martin Klein** **Pius Pflügler** **Volker Reichenbach**
Mitarbeiter:	**> 2000**

Standorte

.consulting .solutions .partnership

Leistungsspektrum

Kompetenz zur Beratung und Durchführung sämtlicher Projekte im Bereich der IT Sicherheit mit langjährigem Schwerpunkt im Bereich Applikationssicherheit.

Leistungsspektrum

- Full-Service für Business-Lösungen
- Individuelle Anwendungsentwicklung
- SAP-Beratung und -Entwicklung

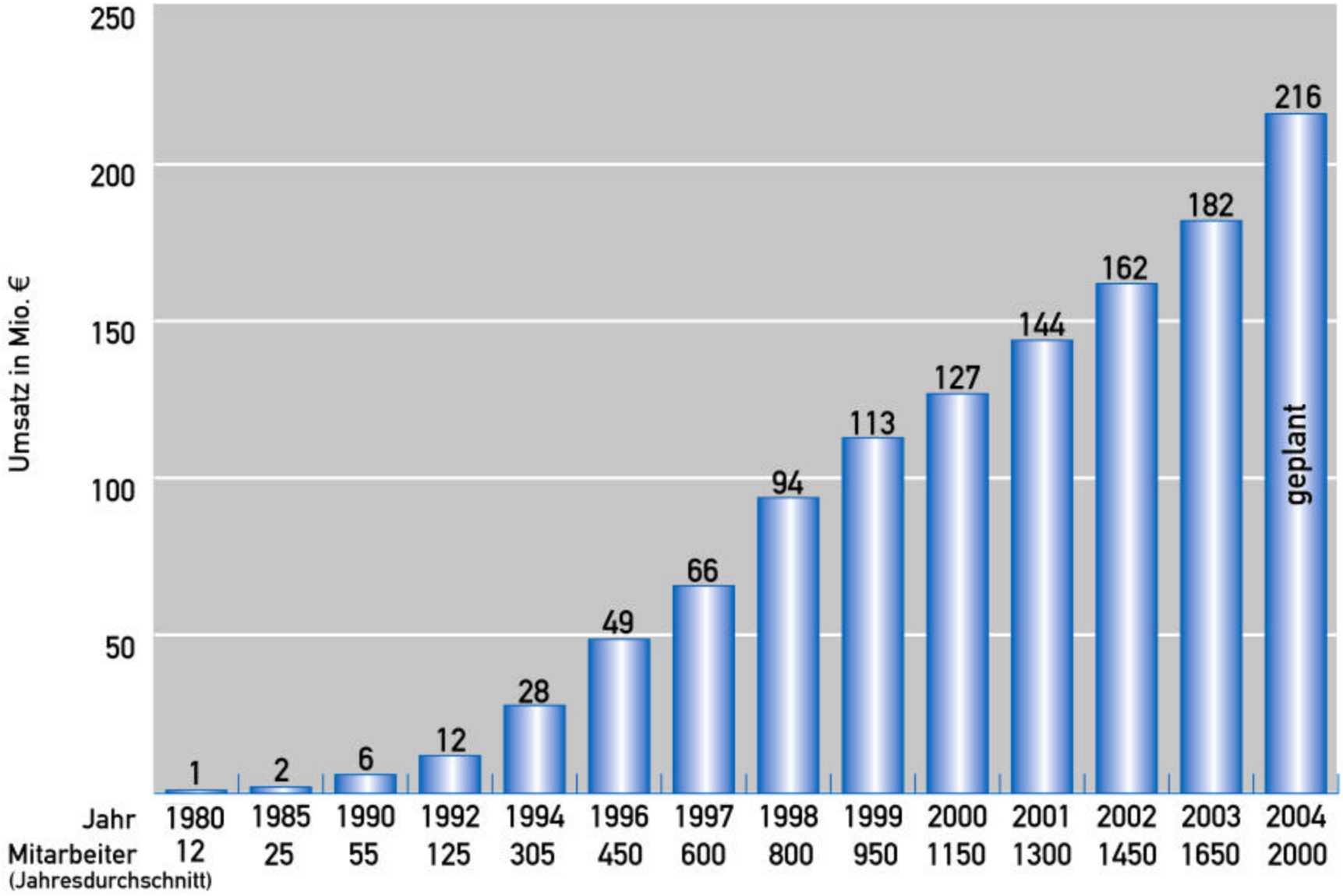
Branchenlösungen

- Versicherungen
- Finanzdienstleistungen
- Gesundheitswesen

Seit 1996 nach DIN EN ISO 9001 zertifiziert

Umsatz- und Mitarbeiterentwicklung

.consulting .solutions .partnership



Branchen und Kunden (Auszug)

.consulting .solutions .partnership

Versicherungen

- ADAC-Versicherung
- Allstate, USA
- Allianz
- AMB Generali
- AOK
- Aspecta
- AXA
- Basler Versicherungen,CH
- Bayer. Beamten Vers.
- Folksam
- Gerling
- Gothaer Rück
- Hannover Rück
- Helvetia Patria, CH
- HUK Coburg
- Münchener Rück
- NÜRNBERGER Vers.
- Quelle Versicherungen
- Sparkassenversicherung
- UNIQA
- Versicherungskammer Bayern
- Wiener Städtische, A
- Winterthur, CH
- Zurich Fin. Services, CH

Finanzdienstleistungen

- Bankgesellschaft Berlin
- Bayerische Landesbank
- BHW
- BMW Financial Services
- Commerzbank
- Deutsche Bank
- DZ BANK
- Dresdner Bank
- Deutsche Börse Systems
- Finanz IT
- HELABA
- HSBC Trinkaus & Burkhardt
- HSH Nordbank
- IZB SOFT
- Bayerische Landesbausparkasse (LBS)
- Sparkassen Informatik
- Bausparkasse Schwäbisch Hall
- Stadtsparkasse Köln
- VW Financial Services
- WestLB

Gesundheitswesen

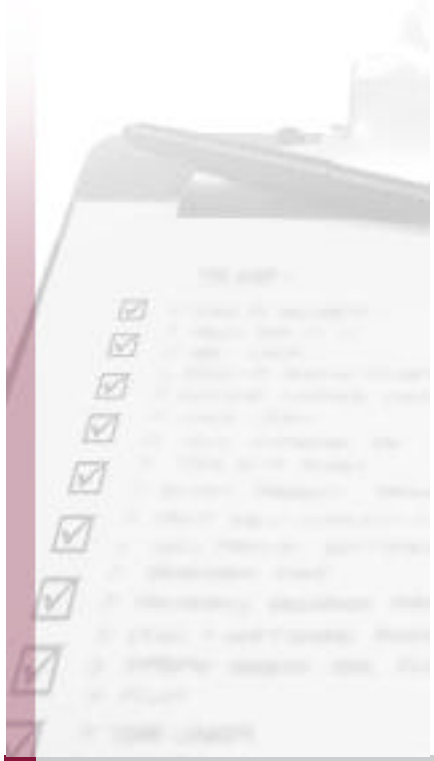
- Allianz PKV
- BARMER Ersatzkasse
- Bau Berufsgenossenschaft Rheinland/Westf.
- BKK Allianz
- BKK Berlin
- BKK futur
- Bundesinnungskrankenkasse Gesundheit(BIG)
- Deutsche Krankenversicherung (DKV)
- DRG-Institut (IneK gGmbH)
- Hanseatische KK
- IKK-Bundesverband
- IKK Sachsen-Anhalt
- Johanniter-Krankenhaus Bonn
- Kaiserswerther Diakonie
- Kliniken d. Landesverbandes Rheinland
- PKV Verband
- SIGNAL Krankenvers.
- Techniker Krankenkasse

Industrie/Behörden/Touristik

- AUDI AG
- BMW AG
- Brunata
- Bundeswehr/-Marine
- Deutsche Telekom
- E.ON
- Europ. Patentamt
- GASAG
- Gebühreneinzugszentrale (GEZ)
- Hoffmann Werkzeuge
- Messer Griesheim
- PREMIERE
- Renault Nissan Deutschland
- Rolls Royce Deutschland
- TUI
- VW AG
- Wacker-Chemie

Agenda

1. Vorstellung
2. Hintergründe
3. Prüfungsstandard
4. Zusammenfassung
5. Fragen / Diskussion



Warum prüfen Wirtschaftsprüfer IT-Systeme?

Erfahrungen aus Enron, Worldcom & Co.

- **Steuerumgehung**
- **Intransparenz**
- **Bereicherung**
- **Kontrollverlust**

=> Vertrauensverlust in die Wirtchaft

Warum prüfen Wirtschaftsprüfer IT-Systeme?

Gesetzlicher Auftrag:

- **Der Jahresabschluss eines Unternehmens hat unter Beachtung der Grundsätze ordnungsgemäßer Buchführung ein den tatsächlichen Verhältnissen entsprechendes Bild der Vermögens-, Finanz- und Ertragslage zu vermitteln (§264 HGB)**
- **Ein Wirtschaftsprüfer hat seine Prüfung so anzulegen, dass Unrichtigkeiten und Verstöße gegen diese Pflicht erkannt werden (§§ 317 HGB)**

Warum prüfen Wirtschaftsprüfer IT-Systeme?

IT-Systeme können dabei nicht außen vor bleiben:

- **Controlling und Verwaltung sind essentiell vom IT-Einsatz abhängig**
- **IT ist in fast allen Unternehmen ein wichtiger Produktionsfaktor**
- **Gesetzliche Vorschriften, die die Prüfung von Risiken auch durch IT-Einsatz vorschreiben (KontraG)**
- **(Basel II)**

Warum prüfen Wirtschaftsprüfer IT-Systeme?

- **Forderung des internationalen Dachverbands IFAC (International Federation of Accountants)**
- **Nationale Umsetzung des internationalen Auditing Standards ISA 401**
- **Institut der Wirtschaftsprüfer empfiehlt die Aufnahme einer Prüfung nach PS330 in den Prüfungsplan (keine jährliche Wiederholung!)**

Wann ist ein Unternehmen prüfungspflichtig?

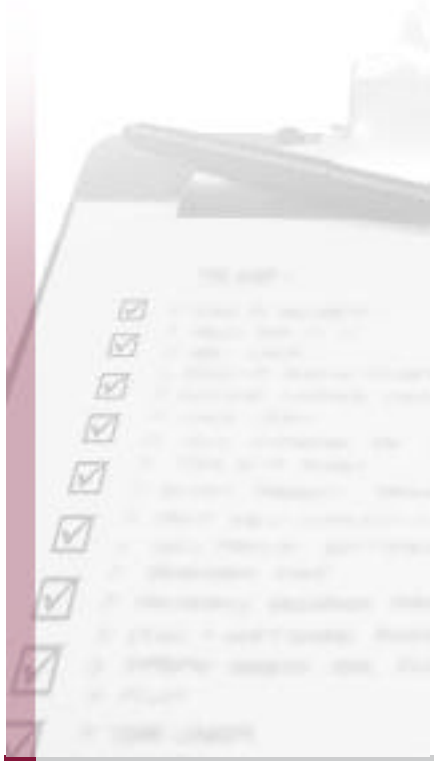
- **Jedes Unternehmen kann seinen Abschluss freiwillig prüfen lassen**
- **Prüfungspflichtig sind mittelgroße und große Kapitalgesellschaften nach HGB, d.h. wenn 2 der drei Kriterien erfüllt bzw. überschritten sind besteht Prüfungspflicht (die Beträge gelten ab dem Wirtschaftsjahr 2004):**
  - 4.015 TEUR Bilanzsumme nach Abzug eines auf der Aktivseite ausgewiesenen Fehlbetrags
  - 8.030 TEUR Umsatzerlöse in den zwölf Monaten vor Abschlussstichtag
  - Im Jahresdurchschnitt fünfzig Arbeitnehmer

Vorteile der Prüfungen für Unternehmen

- Notwendig für einen uneingeschränkten Bestätigungsvermerk im Abschluss
- Wirtschaftlichen Schaden vermeiden (Haftung des WP!)
- Persönliche Haftung durch IT-Leiter und Geschäftsführer „abwenden“
  (OLG Hamm: positive Vertragsverletzung aus seinem Arbeitsvertrag bei angestelltem IT-Leiter wegen Nicht-Einhaltung der Sicherheitspolicy => persönlich finanziell verantwortlich)
- Gesetzliche Vorgaben erfüllen
- Außendarstellung gegenüber z.B. der Kreditwirtschaft (Basel II?)

Agenda

1. Vorstellung
2. Hintergründe
3. Prüfungsstandard
4. Zusammenfassung
5. Fragen / Diskussion

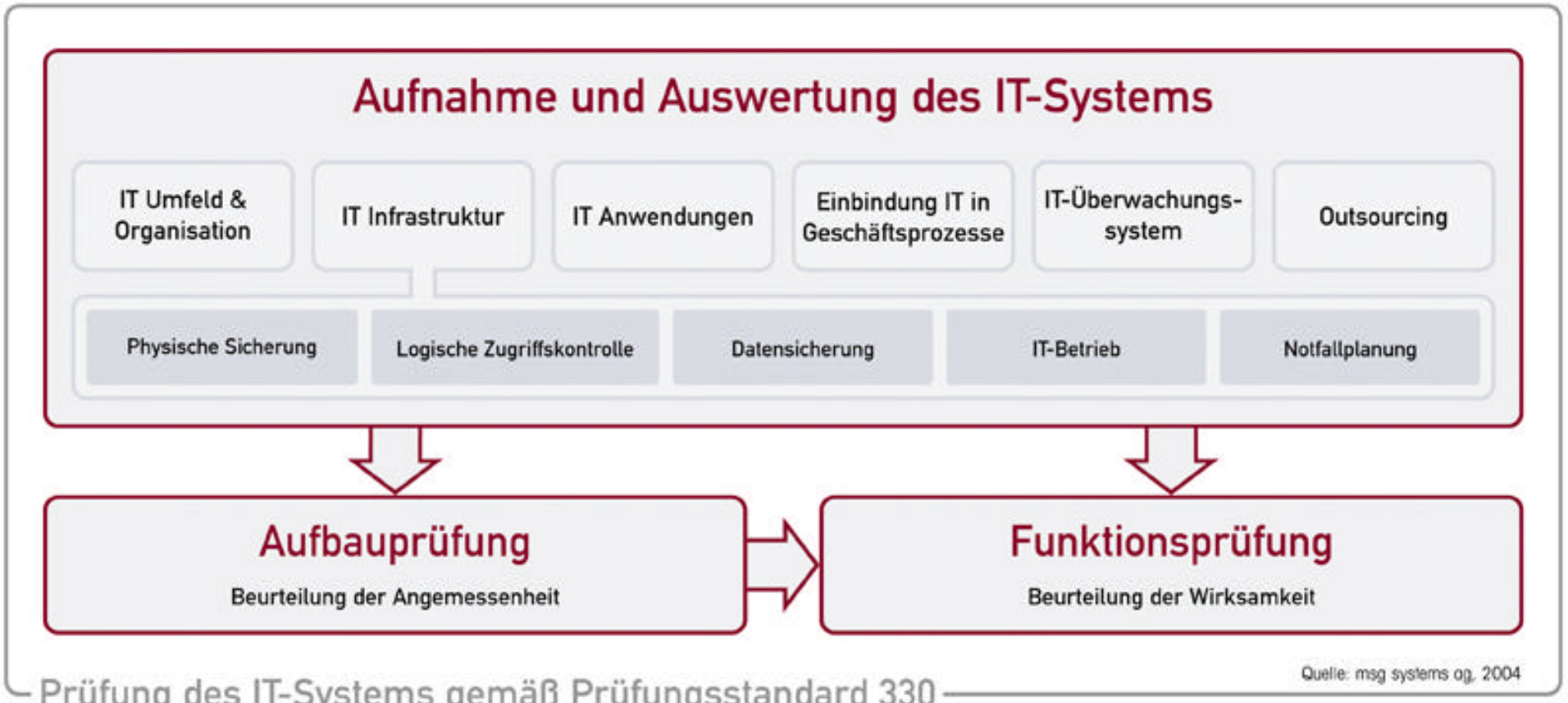


Prüfungsumfang ist eingeschränkt auf IT-Systeme die dazu dienen, Daten zu verarbeiten die direkt oder indirekt „rechnungslegungs-relevant“ sind, d.h. für:

- **Buchführung**
- **Jahresabschluss**
- **Lagebericht**

D.h. in Prosa: alle IT-Systeme, durch deren Gefährdung dem Unternehmen oder dessen Eigentümern ein wirtschaftlicher Schaden entstehen könnte.

IDW PS-330 Prüfungsumfang



Prüfung des IT-Systems gemäß Prüfungsstandard 330

IDW PS330 Prüfungskriterien

- **Vollständigkeit**
- **Richtigkeit**
- **Zeitgerechtigkeit**
- **Ordnung**
- **Nachvollziehbarkeit**
- **Unveränderlichbarkeit**

Die „üblichen“ IT-Sicherheitsziele werden dementsprechend als „nur“ Voraussetzung behandelt:

- **Authentizität**
- **Autorisierung**
- **Vertraulichkeit**
- **Verbindlichkeit**
- **Integrität**
- **Verfügbarkeit.**

IDW PS330 Risikoindikatoren

- **Abhängigkeit**
- **Änderungen**
- **Know-How und Ressourcen**
- **Geschäftliche Ausrichtung**

Anzuwenden auf Unternehmens- und Prüffeldebene.

Keine „statische“ Prüfung, sondern:

- **Prüfung der Angemessenheit**

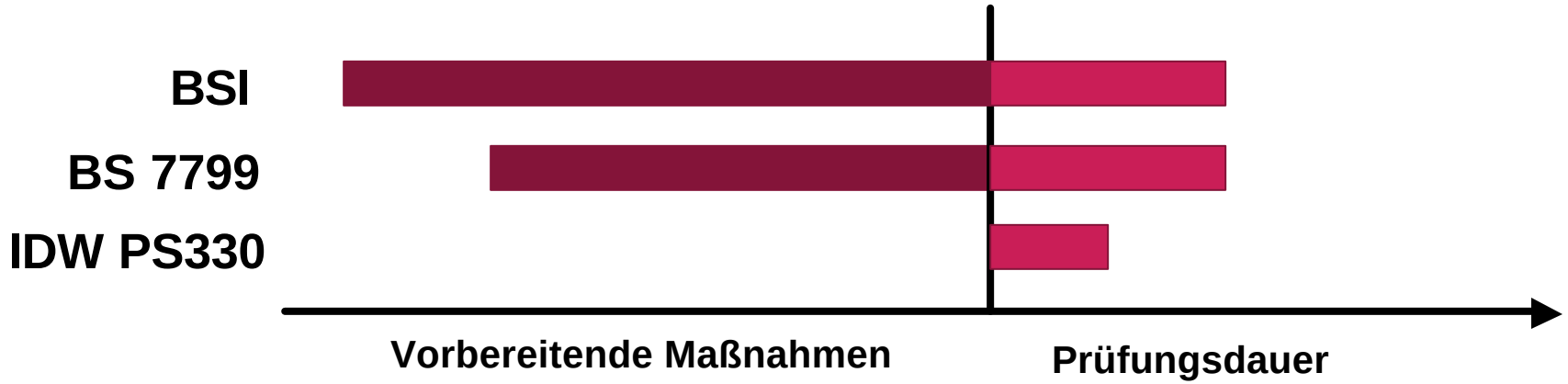
Genügt das IT-System (Dokumentationslage!) in den Augen des Prüfers den Anforderungen des Unternehmens (Größe, Markt, etc.)?

- **Prüfung der Wirksamkeit**

Sind die dokumentierten bzw. geplanten Maßnahmen wirksam umgesetzt und werden sie gelebt?

Aufwand für vergleichbare Prüfungen

- \+ kein Vorbereitung der IT für die Zertifizierung notwendig
- \+ geringer Zeitaufwand = geringe Kosten
- \+ gute Verwendbarkeit als „Lagebericht“ der IT-Sicherheit
- \- Qualität der Prüfung in hohem Maß abhängig von der Qualität des Prüfers
- \- Direkte Vergleichbarkeit (ohne Einsicht in die Prüfungsunterlagen) schwierig



Prüfungsumfeld

- **Prüfung wird nicht immer von den WPs selbst sondern von Spezialisten erledigt (Verwendung der Arbeit eines anderen Prüfers nach IDW PS 320)**
- **Buchhaltungssoftware selbst wird vom Programmhersteller meist bei einem Wirtschaftsprüfer zertifiziert (Korrekte Funktionsweise nach IDW PS 880)**
- **Oft kombiniert mit den Vorbereitungen auf die elektronische Buchprüfung**

Einordnung vergleichbarer Prüfungen

	IDW PS330	BSI	BS 7799
Zertifizierung	Zertifiziert durch Wirtschaftsprüfer (WP)	Grundschutzzertifikat BSI	BS-7799-Zertifikat durch akkred. Unternehmen
Abhängigkeit v. Prüfer	Hoch	Kaum	Mittel
„Schwerpunkt“ der Prüfung	Rechnungslegungs-relevante IT-Systeme	Definierter IT-Verbund (meist gesamte IT)	IT-Organisation
Zielpublikum	Prüfungspflichtige Unternehmen (auch KMU!)	Behörden, Institute, auch Wirtschaft	größere Firmen mit definierter Org.
Herkunft	Aus der Sicht WP / Juristen /Geschäftsleitung	Von IT-Fachleuten für IT-Fachleute	Qualitätssicherung, betriebliche Unternehmensorg.

Vielen Dank für die Aufmerksamkeit !

.consulting .solutions .partnership