# ISO/IEC 17024:2003

## Leitlinien, Umsetzung, Bedeutung


/donabauer/
IT MANAGEMENT & RESOURCES

© 2004 zeitform Internet Dienste OHG Fraunhoferstraße 5 64283 Darmstadt Tel: 06151-155637 Fax: 06151-155634 E-Mail: zeitform@zeitform.de http://www.zeitform.de

# Vorstellung


/donabauer/
IT MANAGEMENT & RESOURCES

# zeitform /donabauer/projektbüro

- Der Dienstleister für nationale und internationale Industrie- und Forschungsprojekte
- Ressourcenbeschaffung und Ressourcenentwicklung
- Entwicklung der strategischen und operativen Marketinginstrumente
- Verteilte, webbasierte Projekt-Tools
- Projekt-Kommunikation
- Projekt-Koordination
- Projekt-Controlling

 Fraunhoferstraße 5 64283 Darmstadt Tel: 06151-155637 Fax: 06151-155634 E-Mail: zeitform@zeitform.de http://www.zeitform.de

# Key Note


/donabauer/
IT MANAGEMENT & RESOURCES

# Bildung vs. Qualifizierung

- Bildung dient der umfassenden Entwicklung der Persönlichkeit
- Bildung ist eher „Input orientiert“
- Bildungsabschlüsse folgen dem Senioritätsprinzip
- Schulische Primär-Bildung, Ausbildung, Studium

- Qualifizierung dient der Aneignung von Fachkompetenz
- Qualifizierung ist eher „Output orientiert“
- Qualifizierungsabschlüsse folgen dem Aktualitätsprinzip
- Betriebliche und außerbetriebliche Qualifizierung

# Forderungen nach einem Kompetenz-nachweis in der Informationssicherheit

- Gefordert wird die eindeutige Identifikation und Zuordnung Ressource/Aufgabe
- Das notwendige Wissen für die jeweilige Aufgabe
- In einigen Fällen die Dokumentation des an einen Mitarbeiter gebundenen Wissens
- Und die Dokumentation der Maßnahmen zum Erhalt dieses Wissens

# Anforderungen an einen Kompetenznachweis

- Egalitär
- Elitär
- Allgemeingültig
- Transparent
- Unabhängig
- Aktuell
- Kompetent
- Qualitätsgeprüft

# Begriffsdefinition

# Normen und Standards


/donabauer/
IT MANAGEMENT & RESOURCES

# Begriffsdefinition Normen und Standards

- Ein Standard ist eine Beschreibung der Art und Weise, etwas einheitlich herzustellen oder durchzuführen
- Normen sind nur solche Standards, die durch nationale oder Internationale Normierungsorganisationen veröffentlicht wurden
- Nationale DIN (Deutsches Institut für Normung), Internationale ISO (International Organization for Standardization), u.w.
- Sie beinhalten die unabhängige Zertifizierung einer Methode, eines Produktes, einer Organisation oder einer Person

# Begriffsdefinition Normen und Standards

- Zu den Normen existieren oft „Umsetzungs-Standards“
- Die Existenz kann von der Norm vorgeschrieben sein, sie sind jedoch selbst nicht Bestandteil der Norm
- ITIL / ISO 20000, ISMS / ISO 27001, CISSP/ ISO 17024
- Normen und Zertifizierungen sind aus Sicht der Unternehmen Prüfungsinstrumente der Qualität
- Primäres Ziel der Norm ist die internationale Vergleichbarkeit
- Sie bewirken für die Unternehmen eine Marktöffnung oder eine Marktschließung

# ISO/IEC 17024:2003

- Die ISO 17024 ist eine Norm zur Akkreditierung von Personalzertifizierungsstellen
- Akkreditierung ist die unabhängige Bestätigung durch Dritte, dass die Zertifizierungsstelle bestimmte Konformitätbewertungen durchführen kann
- Historisch entstanden aus der Zertifizierung der Berufsgruppe der Gutachter und Sachverständigen (EU-Zertifiziert)

# ISO/IEC 17024:2003

# Struktur und Inhalt


/donabauer/
IT MANAGEMENT & RESOURCES

# Anforderungen an die Zertifizierungsstelle

- 4.1.1 Die grundsätzlichen Regelungen und Verfahren der Zertifizierungsstelle und deren Anwendung müssen … für alle Kandidaten gleichermaßen fair und gerecht sein
- 4.1.2 Die Zertifizierungsstelle muss die Leitlinien und die Verfahren für die Erteilung, Aufrechterhaltung, Erneuerung, Erweiterung, Einschränkung des Geltungsbereichs der gewünschten Zertifizierung und Aussetzung oder Entzug der Zertifizierung definieren.

# Organisatorische Struktur

- 4.2.1 Die Zertifizierungsstelle muss so strukturiert sein, dass die interessierten Kreise Vertrauen in ihre Kompetenz, Unparteilichkeit und Integrität haben können.
- Rechtliche, organisatorische und finanzielle Unabhängigkeit gegenüber allen anderen Akteuren und Organisationen des Systems
- Schulungsverbot und Dienstleistungsbeschränkung
- Beschwerdeverfahren
- Qualifizierungsnachweis der Mitarbeiter

# Entwicklung und Aufrechterhaltung eines Zertifizierungsprogrammes

- 4.3.1 Die Zertifizierungsstelle muss Methoden und Abläufe für die Bewertung der Kompetenz der Kandidaten definieren.
- Bewertung und Validierung durch Dritte
- Veröffentlichungspflicht
- Normenkonformität
- Neutralität auch im Falle einer anerkannten Schulung als Voraussetzung
- Erfassung statistischer Daten und jährliche Bewertung

# Managementsystem

- 4.4.1 Die Zertifizierungsstelle muss ein dokumentiertes Managementsystem betreiben…
- Dokumentiertes Managementsystem nach ISO 9001
- Umfassend für die gesamte Organisation
- Interne Audits
- Verbesserung, Korrektur- und Vorbeugemaßnahmen

# Unterauftragsvergabe

- Vertragspflicht
- Vertraulichkeitsregel
- Verantwortung für die Zertifizierung ist nicht übertragbar
- Kompetenznachweis
- Nachweis der Unparteilichkeit

# Vertraulichkeit, Aufzeichnungen Sicherheit

- Regelung zur Vertraulichkeit
- Zur ordnungsgemäßen Aufzeichnung, der Lagerung und Vernichtung von Aufzeichnungen
- Sicherheitsregelungen

# Anforderung an die Prüfer

- 5.2.1 Die Prüfer müssen die Anforderungen der Zertifizierungsstelle erfüllen, die auf den anzuwendenden Kompetenznormen und anderen relevanten Dokumenten basieren
- Fachlich Kompetent
- Kompetenz in Prüfungsverfahren
- Unparteiisch
- Sozial geeignet

# Zertifizierungsprozess und Zertifizierungsentscheidung

- Veröffentlichungs- und Aushändigungspflicht über Zertifizierungsverfahren und Preise
- Vertragspflicht
- Evaluationspflicht der Voraussetzungen des Kandidaten
- Dokumentationspflicht
- Personelle Trennung von Ausbildung, Prüfung und Zertifizierung
- Zertifikatspflicht

# Überwachung und Rezertifizierung

- Aktive Überwachung der zertifizierten Person
- Verfahren zur Aufrechterhaltung der Zertifizierung
- Rezertifizierungszwang
- Definition der Häufigkeit und der Inhalte der Rezertifizierung

# Benutzung der Zertifikate und Logos

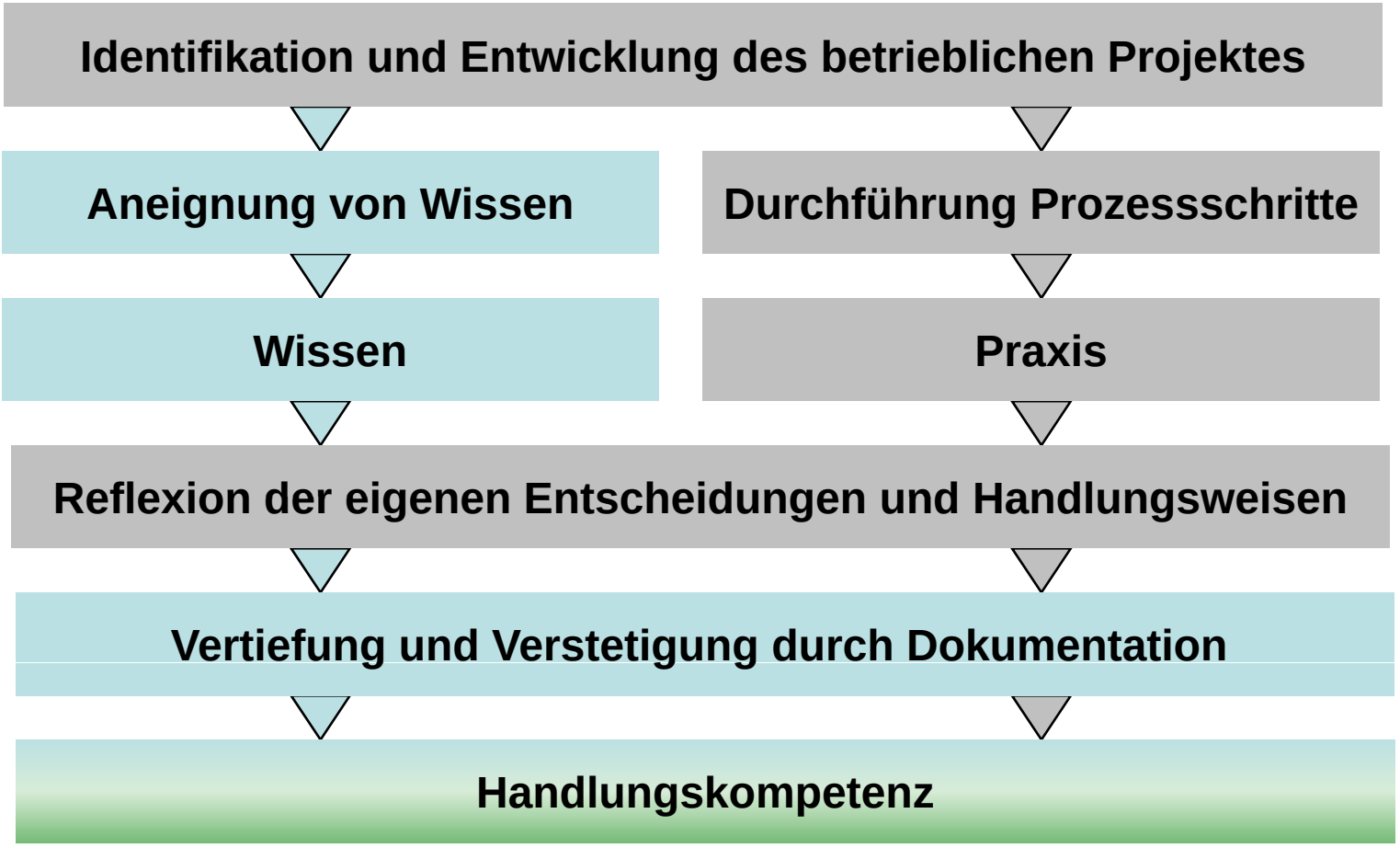
- Umfassende Zeichenordnung
- Verwendungsverbot nach Aussetzung oder Verlust der Zertifizierung
- Definition und Umsetzung von Repressionsmaßnahmen bis hin zur Ergreifung rechtlicher Schritte

# ISO/IEC 17024:2003

# Umsetzung


/donabauer/
IT MANAGEMENT & RESOURCES

# Beispiel Qualifizierungsmethode AITTS

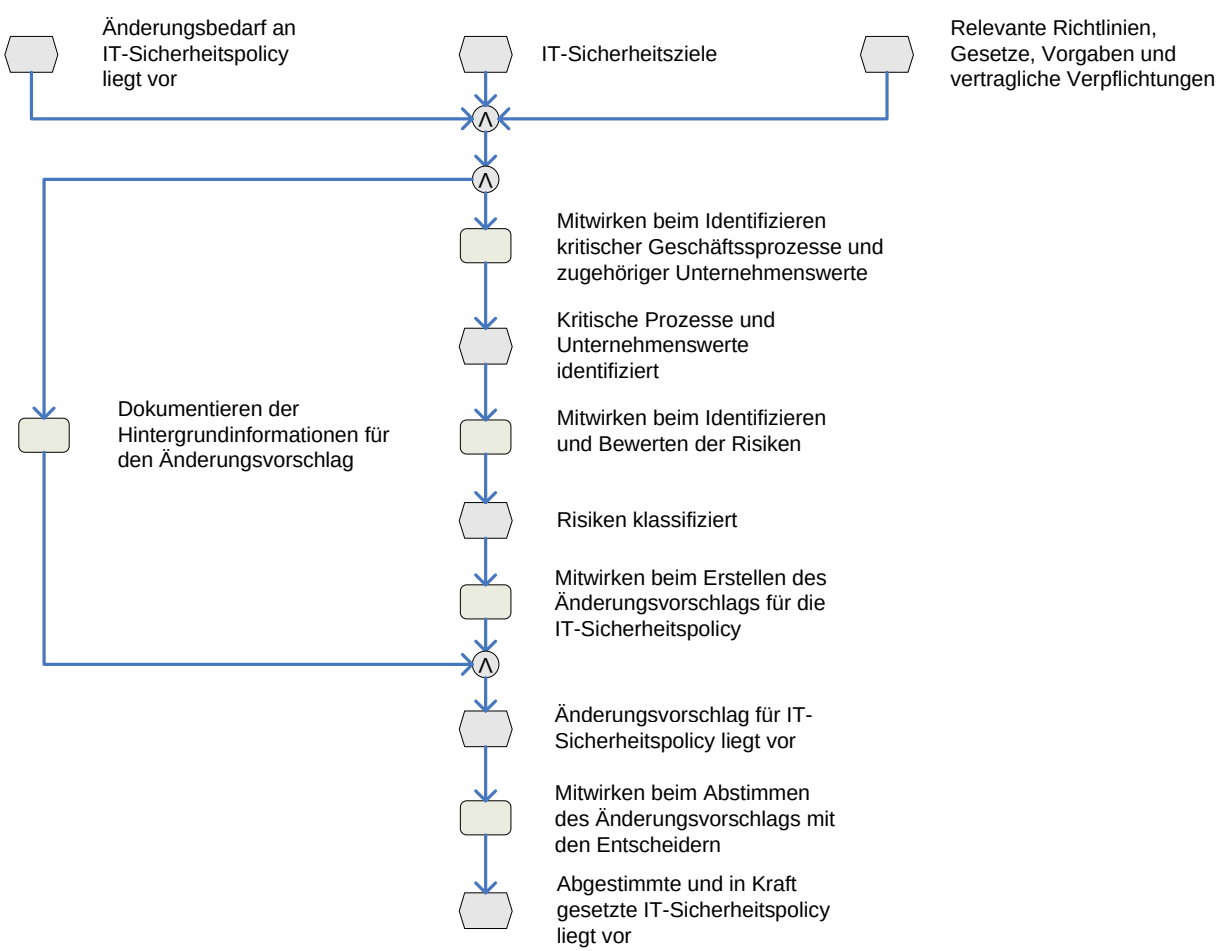



Quelle: Eigene Darstellung

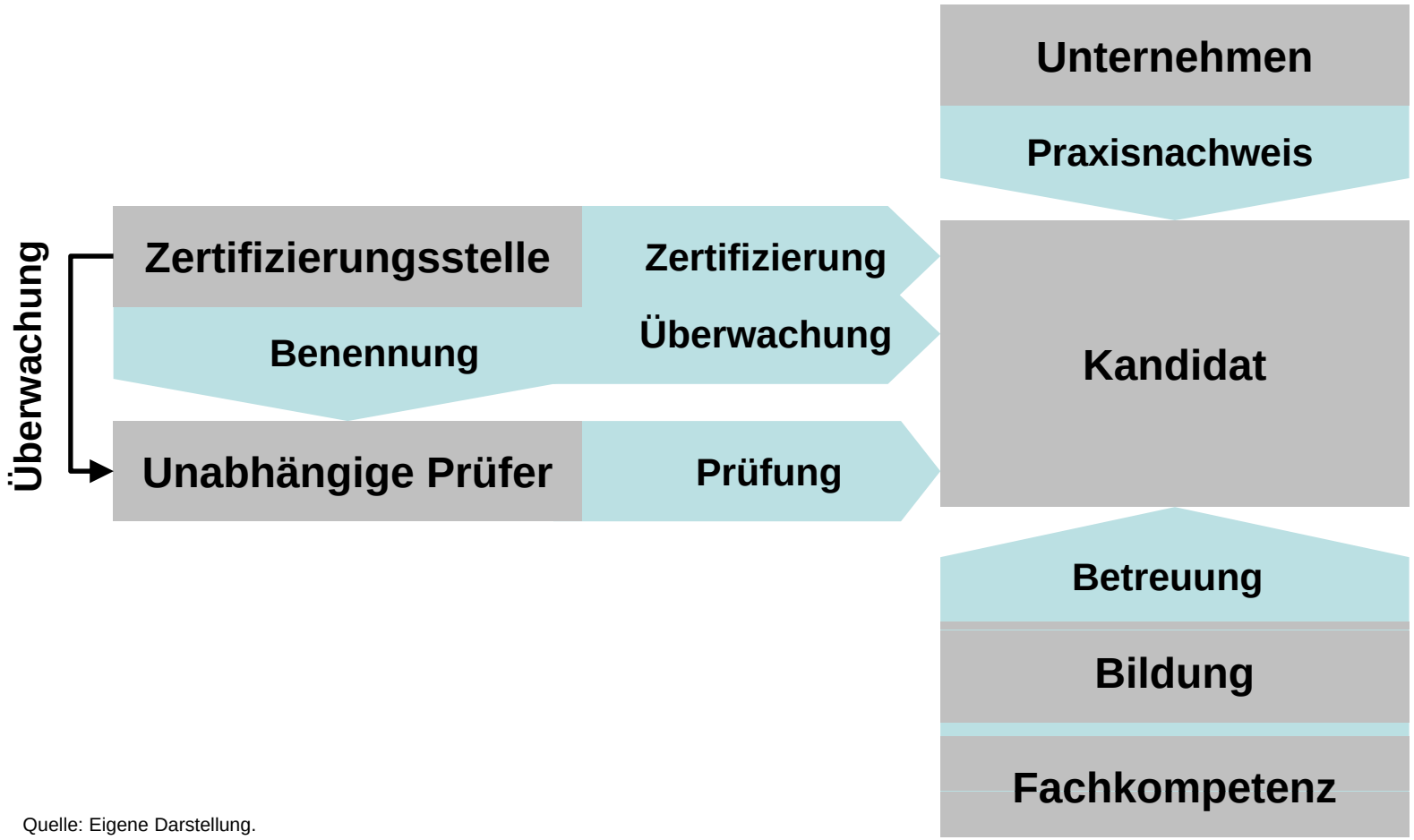
# Beispiel Programminhalt IT Security Coordinator

- Definition des Informationssicherheits-Projektes
- Durchführung vorgegebener Prozessschritte
- Fachliche Begleitung durch erfahrenen Berater zwingend vorgeschrieben
- Durchführung von Reflexionsgesprächen
- Aneignung vorgegebener Handlungskompetenzen
- Umfangreiche Dokumentation (-sprüfung)
- Einstündiges mündliches Fachgespräch

# Beispiel Qualifizierungsprofil IT SECO

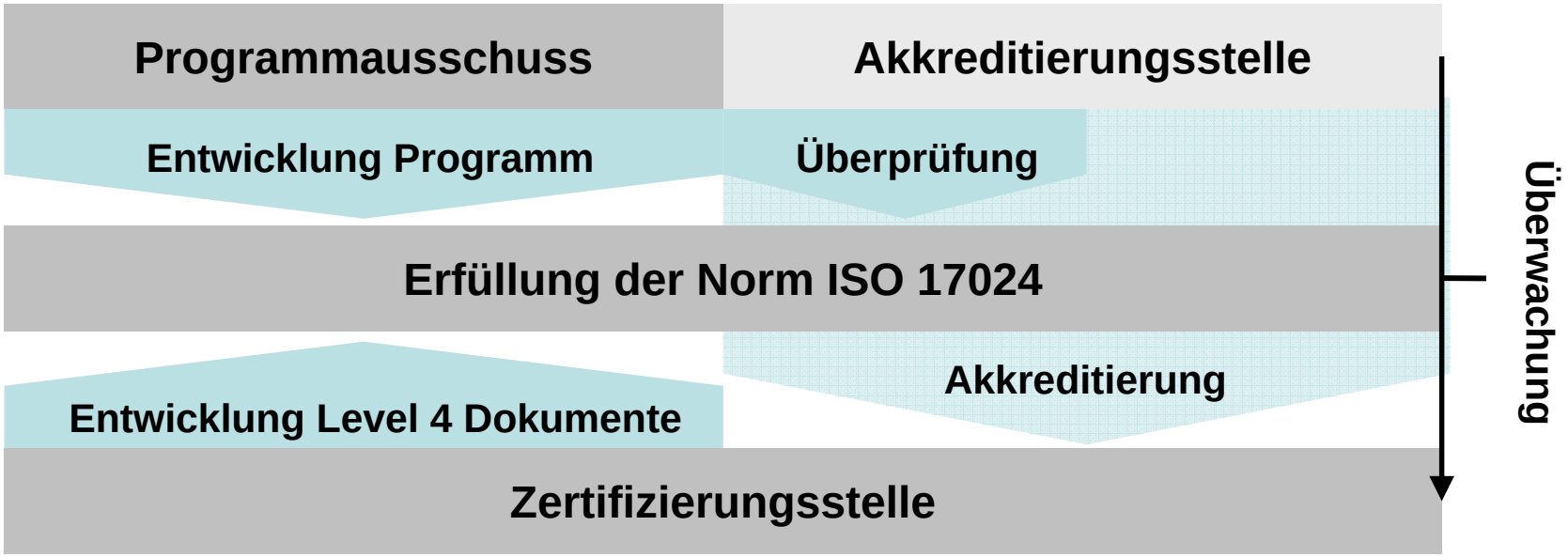


# Akteure der Zertifizierung




Quelle: Eigene Darstellung.

# Akteure der Akkreditierung




Quelle: Eigene Darstellung

# Beispiel Ablauf Akkreditierung

- Programmausschuss entwickelt „Bildungsprogramm“ – Level 2 (Beschreibung) und Level 3 Dokumente (Anwendungsbeispiele)
- Zukünftige Zertifizierungsstelle entwickelt Ausführungsdokumente – Level 4 Dokumente (z.B. Bildungsvereinbarung, Prüfungsordnung, Prüfervertrag, etc.)
- Zukünftige Zertifizierungsstelle entwickelt normenkonforme Organisation, Personalressourcen und Managementsystem
- Empfehlung: Internes Audit mit Beratungsanteil
- Akkreditierungsaudit Stage 1 und Stage 2

# ISO/IEC 17024:2003

# Bedeutung


/donabauer/
IT MANAGEMENT & RESOURCES

# Bedeutung

- Erfüllt alle Forderungen an einen Qualifizierungsnachweis
- Insbesondere Qualität, Unabhängigkeit, Transparenz, Vergleichbarkeit, Aktualität
- Zertifizierung nach ISO 17024 der mit der IT- und Informationssicherheit betrauten Mitarbeiter senkt das operationelle Risiko
- Im nationalen und internationalen Wettbewerb der Qualifizierungsprodukte werden sich mittelfristig jene mit ISO 17024 Zertifikat durchsetzen

# Kontaktinformationen

Bernd Donabauer
zeitform Internet Dienste OHG
Fraunhoferstraße 5
64283 Darmstadt
Tel: 06151-155637
Fax: 06151-155634
E-Mail: zeitform@zeitform.de
http://www.zeitform.de

Donabauer, Bernd: ISO/IEC 17024:2003. Leitlinien, Umsetzung, Bedeutung. Kommentierte Fassung. GI Fachgruppe SECMGT, 17.10.2008. Veröffentlicht unter www.it-mare.com/sources/171008_vortrag_secmgt.pdf, Stand 17.10.2008.