Konzeptentwicklung
Akkreditierte Software Prüfstelle

Durchgeführt an der	Naturwissenschaftlichen Fakultät der Universität Salzburg Fachbereich Computerwissenschaften
Betreuer	Uni.-Prof. Dipl.-Ing. Dr. Wolfgang Pree
Autoren	Josef Maier Thomas Pfeiffenberger
Datum	Jänner 2008

Inhalt

- Einleitung
- Grundlagen der Akkreditierung
- Spezialisierung im Softwarebereich
- Kostennutzen Rechnung
- Zusammenfassung

Einleitung

Einleitung
- Problemstellung
- Lösungsansatz

Grundlagen der Akkreditierung

Spezialisierung im Softwarebereich

Kostennutzen Rechnung

Zusammenfassung

- Leitfaden für die Akkreditierung von Prüflaboratorien.
- Spezialisierung im Bereich Softwaretests und Softwarequalitätsmanagement.
- Umsetzung des Akkreditierungsverfahren, Beschränkung auf Österreich.
- Konzeptentwicklung kann teilweise auch für andere Branchen verwendet werden.

Problemstellung

Einleitung
- **Problemstellung**
- Lösungsansatz

Grundlagen der Akkreditierung

Spezialisierung im Softwarebereich

Kostennutzen Rechnung

Zusammenfassung

In welchen Bereichen kann fehlerhafte Software Probleme verursachen?

- Kosten
- Anwendung
- Garantie
- Gewährleistung
- Produkthaftung
- Schadensersatz
- Sicherheit
- Risiko

Lösungsansatz

Einleitung
- Problemstellung
- **Lösungsansatz**

Grundlagen der Akkreditierung

Spezialisierung im Softwarebereich

Kostennutzen Rechnung

Zusammenfassung

- Einsatz von bestehenden Normen und Standards in den Bereichen:
  - Qualitätsmanagement
  - Verfahrensanweisungen
  - Prüfverfahren
- Akkreditierung der Prüfstelle:
  - Ordnungsgemäße Umsetzung der Prüfverfahren
- Unterstützung bei der Auswahl geeigneter Ansätze und Verfahren im Softwarebereich:
  - Spezial Standards und Normen

Grundlagen der Akkreditierung

Einleitung

Grundlagen der Akkreditierung

- Anforderungen an das Qualitäts-managementsystem
- Anforderungen an die Kompetenz von Prüf- und Kalibier-laboratorien

Spezialisierung im Softwarebereich

Kostennutzen Rechnung

Zusammenfassung

Prüf- und Kalibrierlaboratorien müssen ein Managementsysteme betreiben, technisch kompetent und fähig sein, um fachlich fundierte Ergebnisse zu erzielen!

- Qualitätsmanagementsystem
  (nicht zwingend erforderlich)
  - ISO 9000
  - ISO 9001
  - ISO 9004

- Anforderungen an Prüf- und Kalibrierlaboratorien
  - ISO/IEC 17025

Anforderungen an das Qualitätsmanagementsystem

Einleitung

Grundlagen der Akkreditierung

- **Anforderungen an das Qualitäts-managementsystem**
- Anforderungen an die Kompetenz von Prüf- und Kalibier-laboratorien

Spezialisierung im Softwarebereich

Kostennutzen Rechnung

Zusammenfassung

Grundsätze des Qualitätsmanagementsystems

1. Qualität muss erzeugt werden, sie kann nicht erprüft werden.
2. Qualität bezieht sich immer auf Produkte und auf Prozesse.
3. Qualitätsverantwortung ist untrennbar mit Sach-, Termin- und Kostenverantwortung.
4. Das Qualitätswesen erbringt Dienstleistungen und ist verantwortlich für die Ermittlung der Qualität.
5. Das Qualitätswesen muss einen unabhängigen Berichterstattungspfad haben.
6. Die Mitarbeiter müssen über die Qualität ihrer Arbeit informiert werden.

Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien

Einleitung

Grundlagen der Akkreditierung

- Anforderungen an das Qualitäts-managementsystem
- **Anforderungen an die Kompetenz von Prüf- und Kalibier-laboratorien**

Spezialisierung im Softwarebereich

Kostennutzen Rechnung

Zusammenfassung

- Die ISO/IEC 17025 definiert die allgemeinen Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien, mit zwei Schwerpunkten:
  - Anforderungen an das Managementsystem
  - Technische Anforderungen
- Sie ist auf alle Organisationen, die Prüfungen und/oder Kalibrierungen durchführen, anwendbar.
- Diese Organisation können sein:
  - Anbieter (first party)
  - Anwender (second party)
  - Unabhängige Dritte (third party)

Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien

Einleitung

Grundlagen der Akkreditierung

- Anforderungen an das Qualitäts-managementsystem
- **Anforderungen an die Kompetenz von Prüf- und Kalibier-laboratorien**

Spezialisierung im Softwarebereich

Kostennutzen Rechnung

Zusammenfassung

Technische Anforderungen

- Personal und Räumlichkeiten
- Prüf- und Kalibrierverfahren
- Mess- und Prüfeinrichtungen
- Sicherung der Qualität von Prüf- und Kalibrierergebnissen
- Ergebnisberichte

Spezialisierung im Softwarebereich

Einleitung
Grundlagen der Akkreditierung
Spezialisierung im Softwarebereich
- **Qualitätsmerkmale für Softwareprodukte**
- Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme
- IT Sicherheitsverfahren und Evaluationskriterien

Kostennutzen Rechnung
Zusammenfassung

- ISO/IEC 9126
  - Software engineering - Product quality
- IEC 61 508
  - Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbar elektronischer Systeme
- ISO 15 408
  - Common Criteria CC

ISO/IEC 9126

Einleitung
Grundlagen der Akkreditierung
Spezialisierung im Softwarebereich
- **Qualitätsmerkmale für Softwareprodukte**
- Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme
- IT Sicherheitsverfahren und Evaluationskriterien

Kostennutzen Rechnung
Zusammenfassung

Softwarequalität

Gesamtheit der Merkmale und Merkmalswerte eines Software-Produkts, die sich auf dessen Eignung beziehen, festgelegte oder vorausgesetzte Erfordernisse zu erfüllen

ISO/IEC 9126

Einleitung
Grundlagen der Akkreditierung
Spezialisierung im Softwarebereich
- **Qualitätsmerkmale für Softwareprodukte**
- Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme
- IT Sicherheitsverfahren und Evaluationskriterien

Kostennutzen Rechnung
Zusammenfassung

Aufgaben

- Sicherung der Produktqualität
- Nicht der Prozessqualität
- 6 Qualitätsmerkmale/Software-Qualitätsattributen
- Qualitätsmaße
  - numerisch oder symbolisch
  - für die Bewertung von Qualitätsattributen

ISO/IEC 9126

Einleitung
Grundlagen der Akkreditierung
Spezialisierung im Softwarebereich
- **Qualitätsmerkmale für Softwareprodukte**
- Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme
- IT Sicherheitsverfahren und Evaluationskriterien

Kostennutzen Rechnung
Zusammenfassung

Qualitätsmerkmale

- Functionality / Funktionalität:
  - Korrektheit, Angemessenheit, Interoperabilität, Konformität, Sicherheit
- Reliability / Zuverlässigkeit:
  - Reife, Fehlertoleranz, Wiederherstellbarkeit
- Usability / Benutzbarkeit:
  - Verständlichkeit, Bedienbarkeit, Erlernbarkeit, Robustheit

ISO/IEC 9126

Einleitung
Grundlagen der Akkreditierung
Spezialisierung im Softwarebereich
- **Qualitätsmerkmale für Softwareprodukte**
- Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme
- IT Sicherheitsverfahren und Evaluationskriterien

Kostennutzen Rechnung
Zusammenfassung

Qualitätsmerkmale

- Efficiency / Effizienz:
  - Wirtschaftlichkeit, Zeitverhalten, Verbrauchsverhalten
- Maintainability / Wartungsfreundlichkeit:
  - Analysierbarkeit, Änderbarkeit, Stabilität, Testbarkeit
- Portability / Übertragbarkeit:
  - Anpassbarkeit, Installierbarkeit, Konformität, Austauschbarkeit

ISO/IEC 9126

Einleitung
Grundlagen der Akkreditierung
Spezialisierung im Softwarebereich
- **Qualitätsmerkmale für Softwareprodukte**
- Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme
- IT Sicherheitsverfahren und Evaluationskriterien

Kostennutzen Rechnung
Zusammenfassung

Weitere Qualitätsmerkmale

- Wiederverwendbarkeit – Reuseability
  - (Wartungsfreundlichkeit, Übertragbarkeit)
- Kosten

Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme

Einleitung

Grundlagen der Akkreditierung

Spezialisierung im Softwarebereich

- Qualitätsmerkmale für Softwareprodukte
- **Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme**
- IT Sicherheitsverfahren und Evaluationskriterien

Kostennutzen Rechnung

Zusammenfassung

- ISO/IEC 61 508
- Funktionale Sicherheit
  - Sicherheitsfunktion auf Anforderung
  - Ständige Ausführung der Sicherheitsfunktion
- Sicherheitsgrundnorm
  - IEC 61 513 Anforderungen für sicherheitsrelevante Systeme in einem Kernkraftwerk
  - DIN EN 50 129 Anforderungen für Eisenbahn-Signalanlagen
- Funktionale Sicherheit ist gegeben,
  - wenn jede spezifizierte Sicherheitsfunktion ausgeführt wird
  - wenn der geforderte Erfüllungsgrad der Sicherheitsfunktion erreicht wird.

Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme

Einleitung

Grundlagen der Akkreditierung

Spezialisierung im Softwarebereich

- Qualitätsmerkmale für Softwareprodukte
- **Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme**
- IT Sicherheitsverfahren und Evaluationskriterien

Kostennutzen Rechnung

Zusammenfassung

Ziel ISO/IEC 61 508

- Wahrscheinlichkeit des Auftretens eines gefahrbringendens Ereignisses zu verringern
- Im Falle des Auftretens eines gefahrbringendens Ereignisses die schädigenden Auswirkungen zu verringern

→ Risikominderung

Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme

Einleitung

Grundlagen der Akkreditierung

Spezialisierung im Softwarebereich

- Qualitätsmerkmale für Softwareprodukte
- **Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme**
- IT Sicherheitsverfahren und Evaluationskriterien

Kostennutzen Rechnung

Zusammenfassung

Ziel ISO/IEC 61 508

- Risikographen
  - Risikodefinition und -bewertung nach detaillierten Versagenswahrscheinlichkeiten
- Sicherheitsfunktionen
  - Festlegung und Umsetzung der Maßnahmen zur Restrisikominimierung
- Sicherheitsintegrationslevel (SIL1 – SIL4)
  - Ausfallwahrscheinlichkeit einer Sicherheitsfunktion

Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme

Einleitung

Grundlagen der Akkreditierung

Spezialisierung im Softwarebereich

- Qualitätsmerkmale für Softwareprodukte
- **Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme**
- IT Sicherheitsverfahren und Evaluationskriterien

Kostennutzen Rechnung

Zusammenfassung

Ziel ISO/IEC 61 508

- Fehlervermeidung (systematische Fehler)
  Fehlerbeherrschung (zufällige Fehler)
  - Wiederkehrende Prüfung der korrekten Einhaltung der Sicherheitsfunktionen
- Sicherheitslebenszyclus
  - Berücksichtigung von Entwicklung und Fertigung

Sicherheitsintegritätslevel

Einleitung
Grundlagen der Akkreditierung
Spezialisierung im Softwarebereich
- Qualitätsmerkmale für Softwareprodukte
- **Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme**
- IT Sicherheitsverfahren und Evaluationskriterien

Kostennutzen Rechnung
Zusammenfassung

SIL 1 – SIL4

- Höhere Levels abhängig von
  - der Wahrscheinlichkeit eines gefahrbringendens Ereignisses
  - der Größe der Auswirkungen eines gefahrbringendens Ereignisses
- Erreichen des Levels durch
  - mittlere Ausfallswahrscheinlichkeit bei Aktivierung
  - mittlerer Ausfallswahrscheinlichkeit pro Stunde

Sicherheitslebenszyklus

Einleitung
Grundlagen der Akkreditierung
Spezialisierung im Softwarebereich
- Qualitätsmerkmale für Softwareprodukte
- **Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme**
- IT Sicherheitsverfahren und Evaluationskriterien

Kostennutzen Rechnung
Zusammenfassung

- Konzept
- Definition des gesamten Anwendungsbereiches
- Gefährdungs- und Risikoanalyse
- Gesamte Sicherheitsanforderungen
- …
- Sicherheitsgesamtvalidierung
- Gesamtbetrieb, gesamte Instandhaltung und Reparatur
- …
- Außerbetriebnahme oder Ausmusterung

Was sind Common Criteria (CC)

Einleitung
Grundlagen der Akkreditierung
Spezialisierung im Softwarebereich
- Qualitätsmerkmale für Softwareprodukte
- Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme
- **IT Sicherheitsverfahren und Evaluationskriterien**

Kostennutzen Rechnung
Zusammenfassung

- Internationaler Standard zur Bewertung der Sicherheit eines IT- Systemen
- Technisch abstrakte Sprache
- Katalog mit vordefinierten Anforderungen
  - Funktionale Sicherheitsanforderungen
  - Anforderungen an die Vertrauenswürdigkeit

Ziele Common Criteria (CC)

Einleitung
Grundlagen der Akkreditierung
Spezialisierung im Softwarebereich
- Qualitätsmerkmale für Softwareprodukte
- Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme
- **IT Sicherheitsverfahren und Evaluationskriterien**

Kostennutzen Rechnung
Zusammenfassung

Nachweis der Sicherheitseigenschaften

- Neutrale und vertrauenswürdige Prüfung und Bewertung
- Beseitigung von Schwachstellen

Zielgruppen Common Criteria (CC)

Einleitung
Grundlagen der Akkreditierung
Spezialisierung im Softwarebereich
- Qualitätsmerkmale für Softwareprodukte
- Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme
- **IT Sicherheitsverfahren und Evaluationskriterien**

Kostennutzen Rechnung
Zusammenfassung

- Entwickler:
  Bereitet das System auf eine Evaluierung vor.
- Evaluatoren:
  Bewerten mit Hilfe der CC die Sicherheitsfunktionen des Systems.
- Anwender:
  Erwartet, dass das System nach der erfolgreichen Evaluierung seinen Sicherheitsanforderungen entspricht.

Teile der Common Criteria

Einleitung
Grundlagen der Akkreditierung
Spezialisierung im Softwarebereich
- Qualitätsmerkmale für Softwareprodukte
- Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme
- **IT Sicherheitsverfahren und Evaluationskriterien**

Kostennutzen Rechnung
Zusammenfassung

- Schutzprofil / Protection Profile
- Sicherheitsvorgaben / Security Target
- Evaluierungsgegenstand / Target of Evaluation
- Vertrauenswürdigkeitsstufen / Evaluation Assurance Level (EALs)

Common Criteria (CC) ISO/IEC 15 408

Einleitung

Grundlagen der Akkreditierung

Spezialisierung im Softwarebereich

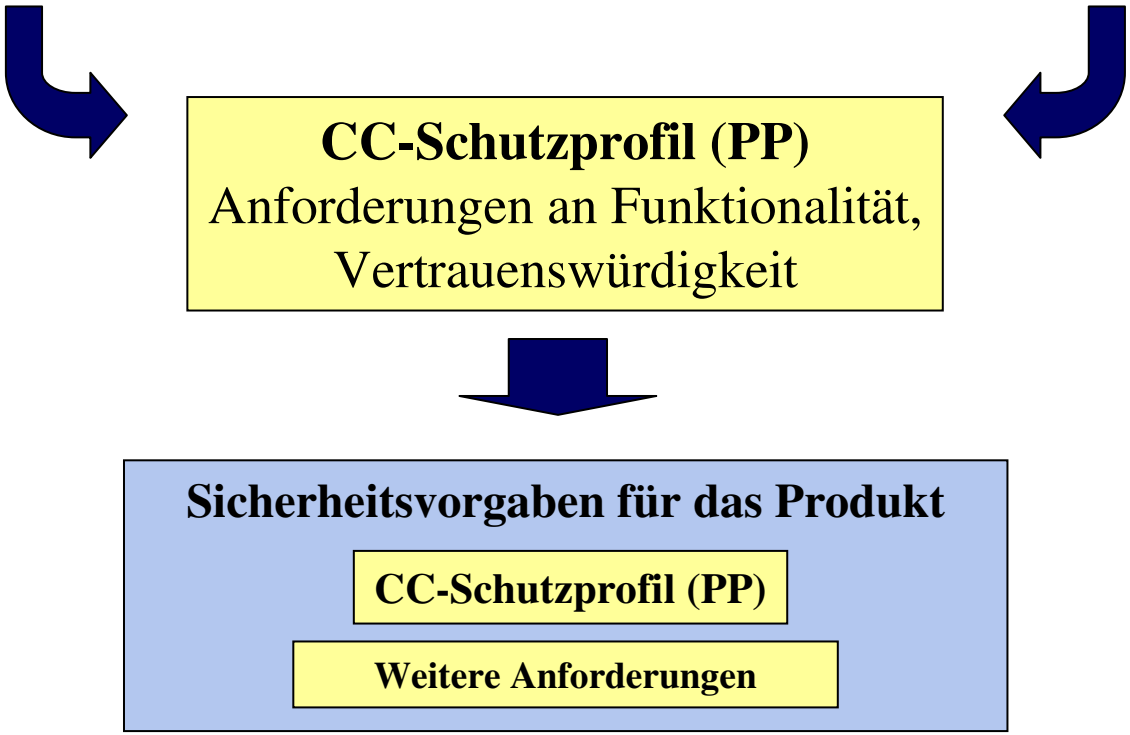
- Qualitätsmerkmale für Softwareprodukte
- Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme
- **IT Sicherheitsverfahren und Evaluationskriterien**

Kostennutzen Rechnung

Zusammenfassung

- Bedrohungsanalyse
- Sicherheitsziele
- Funktionale Anforderungen an einen Produkttyp

- Anforderungen an Vertrauenswürdigkeit (Prüfstufe - EAL)



Common Criteria (CC) ISO/IEC 15 408

Einleitung

Grundlagen der Akkreditierung

Spezialisierung im Softwarebereich

- Qualitätsmerkmale für Softwareprodukte
- Funktionale Sicherheit sicherheitsbezogener E/E/PES Systeme
- **IT Sicherheitsverfahren und Evaluationskriterien**

Kostennutzen Rechnung

Zusammenfassung

- Internationale Vergleichbarkeit von IT-Produkten Qualitätsnachweis
- Anerkennung und Vertrauen
- Vergleichbarkeit der Evaluierung
- Technologie unabhängig

- Common Criteria V3.1 Release2
  - Seit 2007

Kostennutzen Rechnung

Einleitung

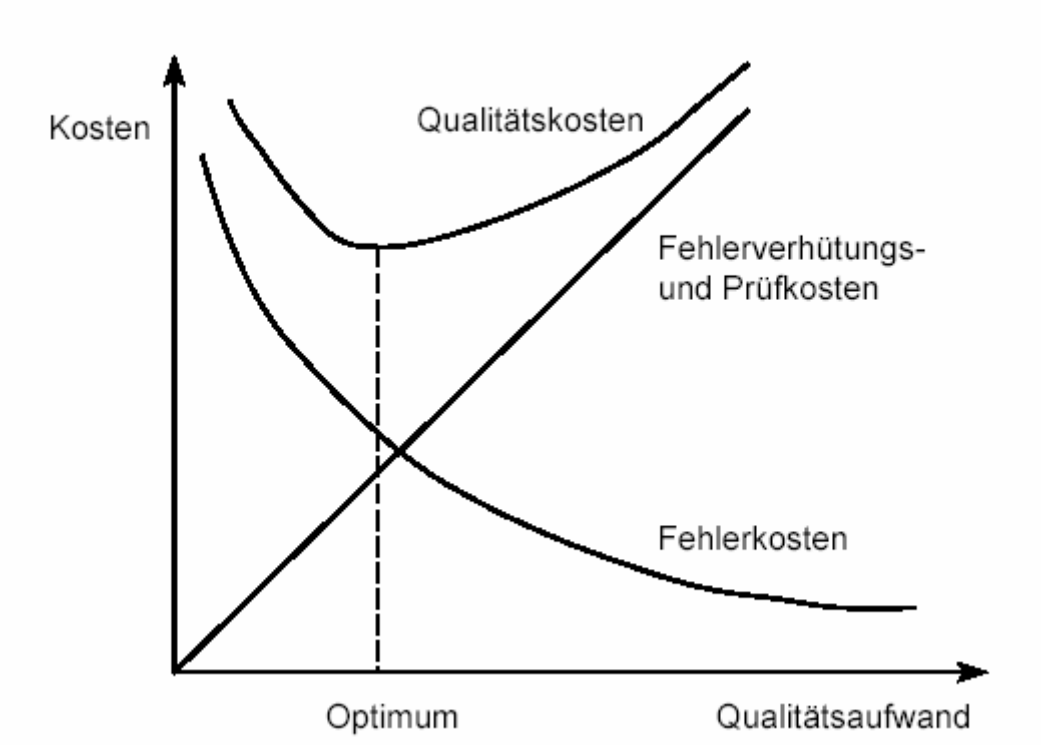
Grundlagen der Akkreditierung

Spezialisierung im Softwarebereich

Kostennutzen Rechnung

- Externe Kosten
- Interne Kosten
- Betriebs-wirtschaftlicher Effekt

Zusammenfassung



Externe Kosten

Einleitung

Grundlagen der Akkreditierung

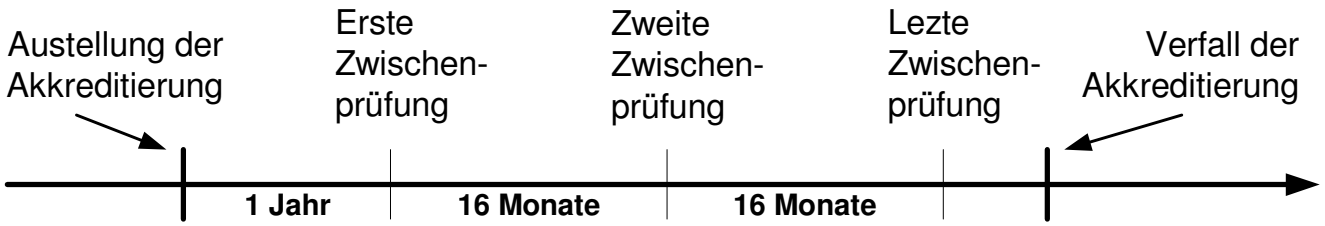
Spezialisierung im Softwarebereich

Kostennutzen Rechnung

- **Externe Kosten**
- Interne Kosten
- Betriebs-wirtschaftlicher Effekt

Zusammenfassung

Einmaliger Verwaltungsaufwand (5-Jahreszyklus)	€ 5.595,-
Für jedes Prüf- und Kalibrierverfahren	€ 36,-
Sachverständige (Überprüfung der Verfahren im Unternehmen)	€ 4.400,-



Interne Kosten

Einleitung

Grundlagen der Akkreditierung

Spezialisierung im Softwarebereich

Kostennutzen Rechnung

- Externe Kosten
- **Interne Kosten**
- Betriebs-wirtschaftlicher Effekt

Zusammenfassung

Aufbau des Qualitätsmanagementsystem und aller benötigter Verfahren. (ca. 1 Mannjahr)	€ 73.000,-
Betreuung des Qualitätsmanagementsystem pro Jahr	€14.600,-
Laufende Validierungen und Kalibrierungen der Mess- und Prüfmitteln (keine Erfahrungswerte im Softwarereich)	-
Mess- und Prüfmitteln müssen dem aktuellen Standard entsprechen (keine Erfahrungswerte im Softwarereich)	-
Personalschulungen pro Mitarbeiter	€ 5.000,-

Betriebswirtschaftlicher Effekt

Einleitung
Grundlagen der Akkreditierung
Spezialisierung im Softwarebereich
Kostennutzen Rechnung
- Externe Kosten
- Interne Kosten
- **Betriebs-wirtschaftlicher Effekt**
Zusammenfassung

Vorteile:

- Erweiterung des Portfolio
- Wettbewerbsvorteil
- Informationsvorsprung

Nachteile:

- Kosten
- Flexibilität

Zusammenfassung

Einleitung
Grundlagen der Akkreditierung
Spezialisierung im Softwarebereich
Kostennutzen Rechnung
Zusammenfassung

- Nachweis der korrekten Implementierung und der Qualität von IT-Produkten und der Wirksamkeit von Sicherheitsfunktion
- Verbesserung der Qualität und Sicherheit von IT-Produkten
- Neutrale, vertrauenswürdige Prüfung und Bewertung
- Erfüllung der Richtlinien und Normen

Danke für Ihre Aufmerksamkeit