



Forschungsprojekt: Geschäftsprozess-Sicherheit
zur Verstärkung des Einsatzes von eBusiness-Standards

Mittelstand-
Digital

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

GESINE - Geschäftsprozess- Sicherheit für KMU in der Cloud

Open Identity Summit
2013-09-09 – 2013-09-11
Kloster Banz, Germany

Prof. Dr. Torsten Eymann, Universität Bayreuth
Philipp Vogler, BF/M Bayreuth





Das Projekt GESINE ist Teil der Förderinitiative „**eStandards: Geschäftsprozesse standardisieren, Erfolg sichern**“, die im Rahmen des Förderschwerpunkts „Mittelstand-Digital – IKT-Anwendungen in der Wirtschaft“ vom Bundesministerium für Wirtschaft und Technologie (BMWi) gefördert wird.

Der Förderschwerpunkt unterstützt gezielt kleine und mittlere Unternehmen (KMU) sowie das Handwerk bei der Entwicklung und Nutzung moderner Informations- und Kommunikationstechnologien (IKT).

„**Mittelstand-Digital**“ setzt sich zusammen aus den Förderinitiativen „eKompetenz-Netzwerk für Unternehmen“ mit 38 eBusiness-Lotsen, „eStandards: Geschäftsprozesse standardisieren, Erfolg sichern“ mit derzeit 11 Förderprojekten und „Einfach intuitiv – Usability für den Mittelstand“ mit zurzeit 10 Förderprojekten.

Weitere Informationen finden Sie unter **www.mittelstand-digital.de**.

Motivation des Projektes

- Geschäftsprozessautomatisierung ermöglicht flexible Anpassung und Veränderung, aber:
 - Eintrittshürden sind für die Nutzung von BPM durch KMU in jetziger Ausprägung zu hoch
- Fehlende Sicherheitsgarantien sind dabei größtes Hindernis für den Einsatz von BPM in KMU:
 - Bedenken bzgl. Sicherheit, Compliance und Governance existierender eStandards können durch automatisierte Zertifizierung in GESINE überwunden werden

Ziele des Projektes GESINE

- Unterstützung von KMU bei der sicheren Einführung von eBusiness-Standards und BPM:
 - Beratungs- und Lernkonzept (Projektpartner IHK@hoc)
- Automatisierte Zertifizierung von Geschäftsprozessen bzgl. der Einhaltung von Sicherheits-, Compliance- und Governanceanforderungen
 - Automatische Überführung von Geschäftsprozessmodellen (BPMN, BPEL) in formal fundierte Petri Netz Modelle
 - Annotation der Petri Netze mit security-relevanter Information
 - Automatisierte Analyse von Daten- und Informationsflüssen

Arbeitspakete und Projektpartner von GESINE

Festlegung
typischer
Anwendungsfälle

Weiterentwicklung
einer BPM-
Software
ARISTAFLOW

Entwurf eines
Beratungs- und
Lehrkonzeptes

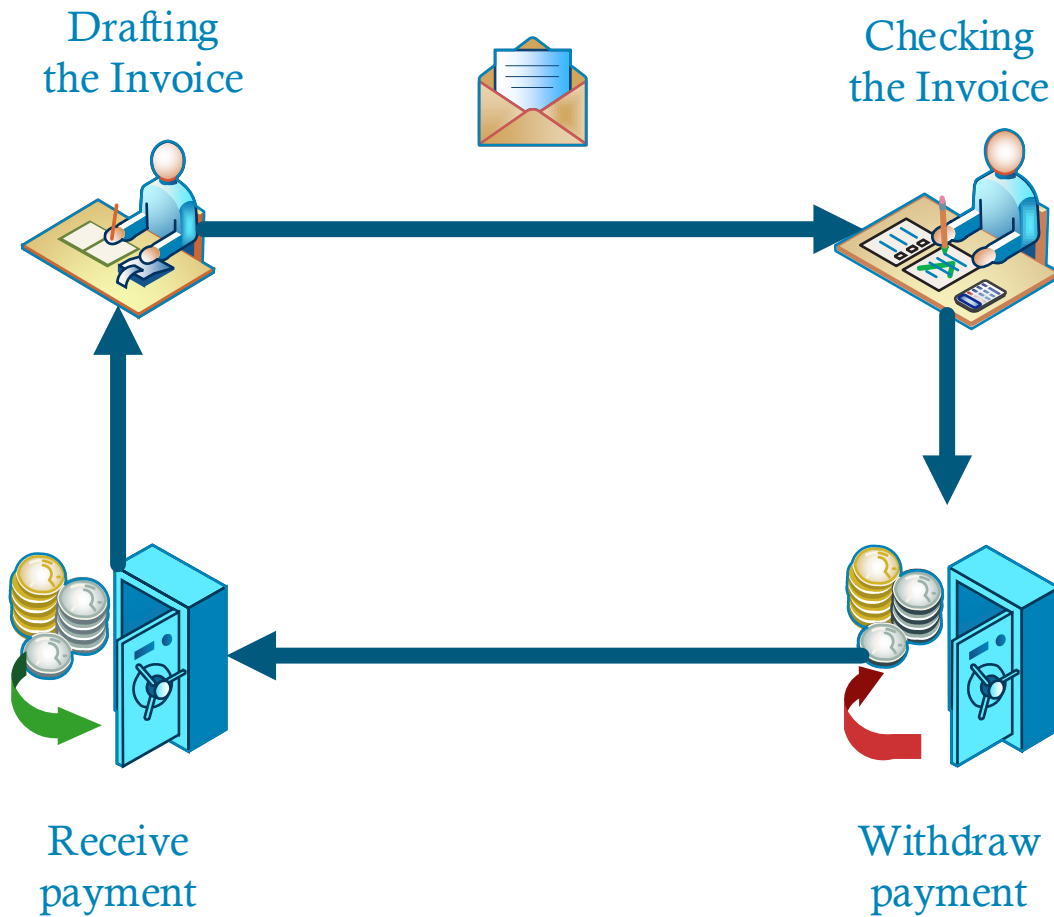


Automatisierte
Zertifizierung

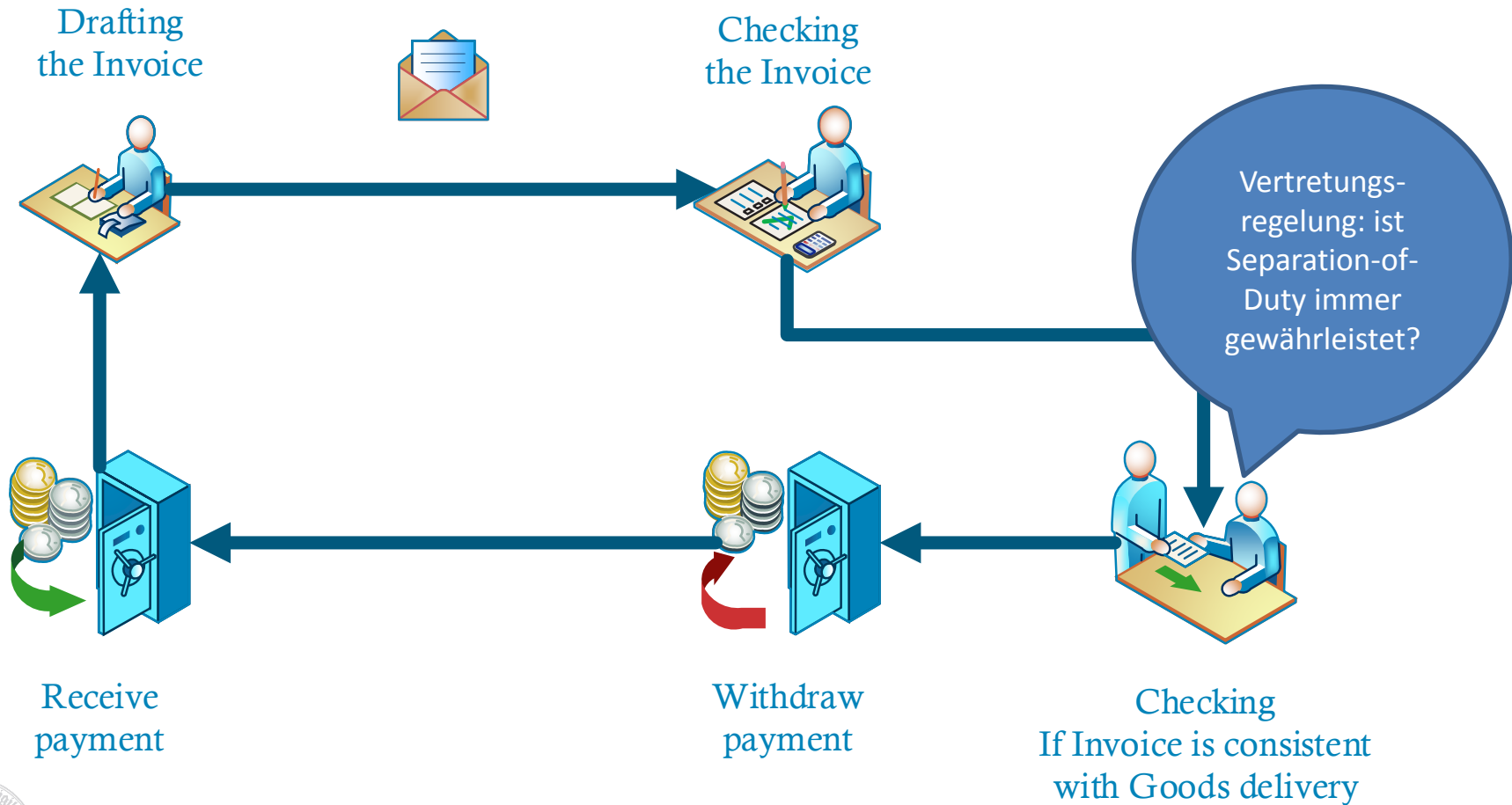
Empirische
Umfragen zu
Anforderungen
und Akzeptanz



Fallstudie: E-Invoicing / E-Rechnung



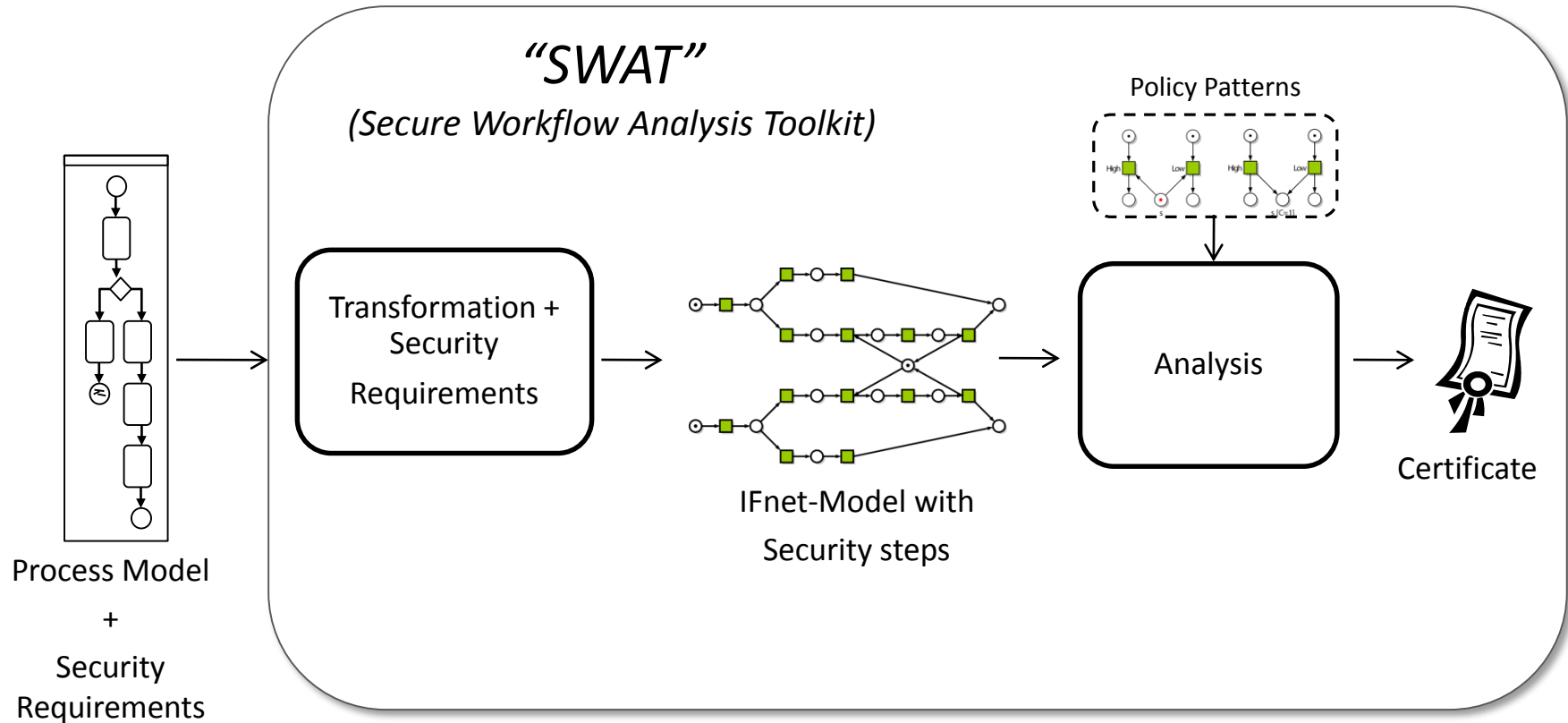
Fallstudie: E-Invoicing / E-Rechnung



Anforderungen an technische Lösung

- Grundprinzipien:
 - Aufgabenteilung (Separation-of-Duty): Aufgaben müssen von unterschiedlichen Personen durchgeführt werden (Bsp. Rechnungsprüfung)
 - Vier-Augen-Prinzip: Prüfaufgabe muss gleichzeitig durchgeführt werden
 - Need-to-Know: Daten sind unmittelbar für Durchführung der Aufgabe nötig
 - Vertraulichkeit: Daten dürfen nicht über Prüfaufgabe hinaus verwendet werden
- **In BPM-Software abbildbar?**

Technische Umsetzung



Standards: BPMN, BPEL, etc.

Arbeitspakete und Projektpartner von GESINE

Festlegung
typischer
Anwendungsfälle

Weiterentwicklung
einer BPM-
Software
ARISTAFLOW

Entwurf eines
Beratungs- und
Lehrkonzeptes



Automatisierte
Zertifizierung

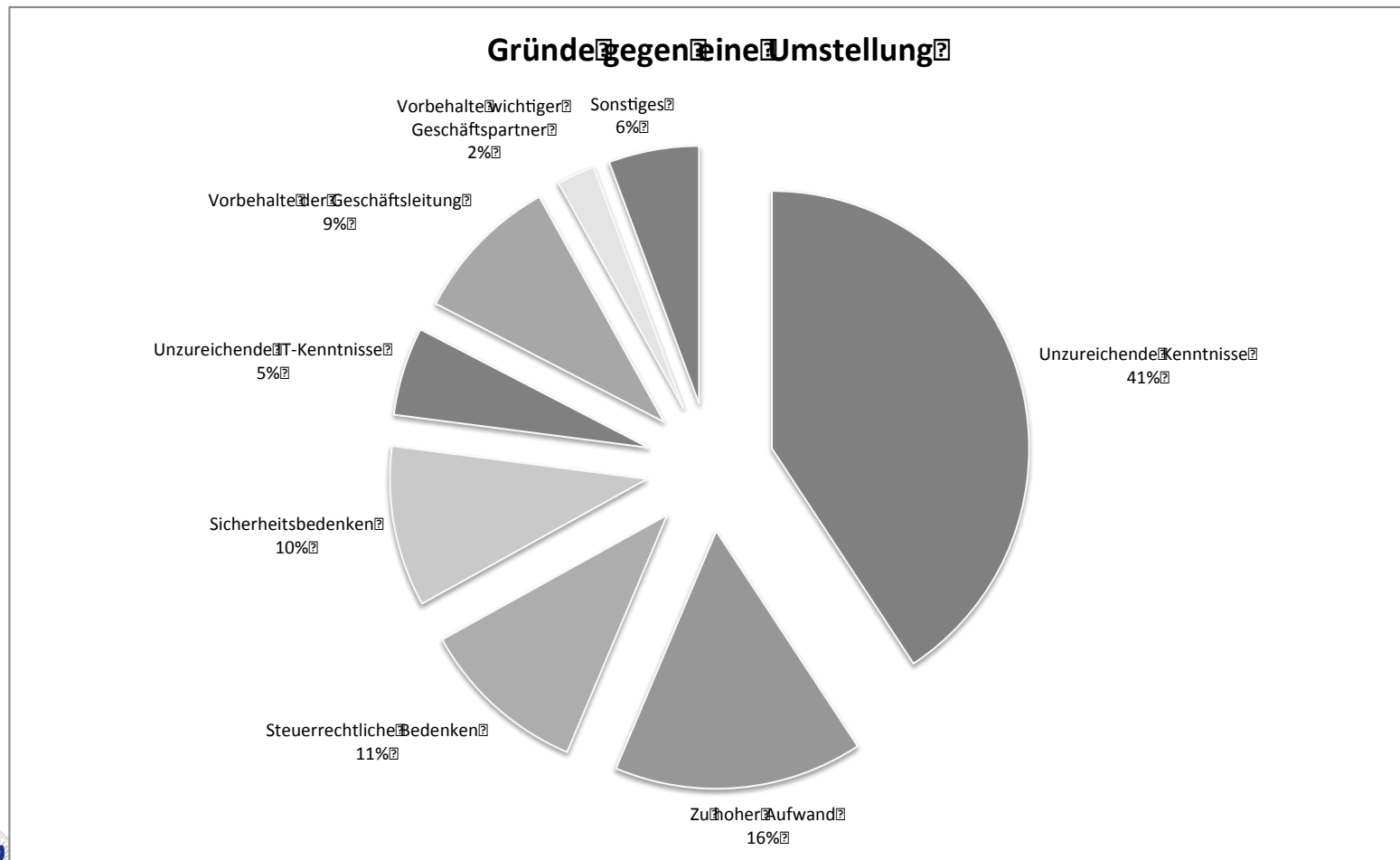
Empirische
Umfragen zu
Anforderungen
und Akzeptanz



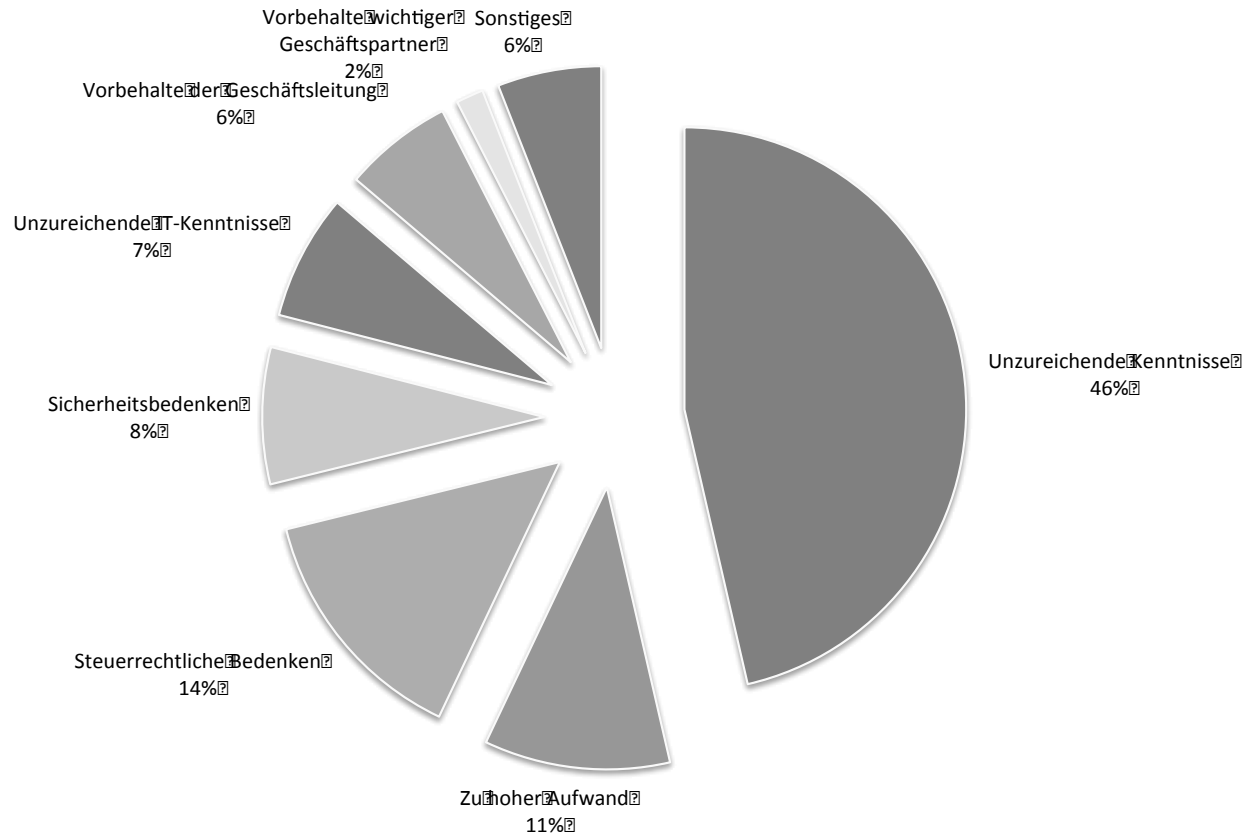


- **Ist Sicherheit überhaupt das dringendste Problem?**

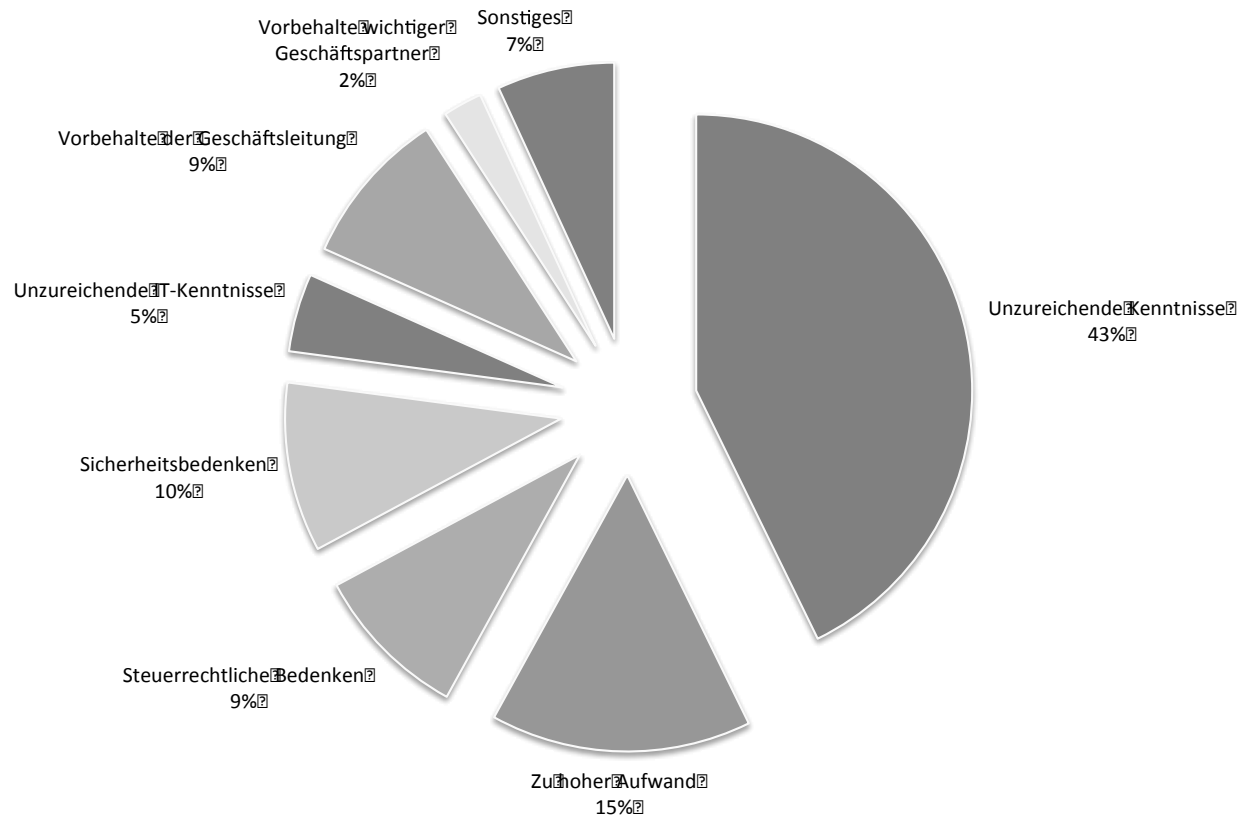
Ergebnisse einer Umfrage in Mittelstand-Digital



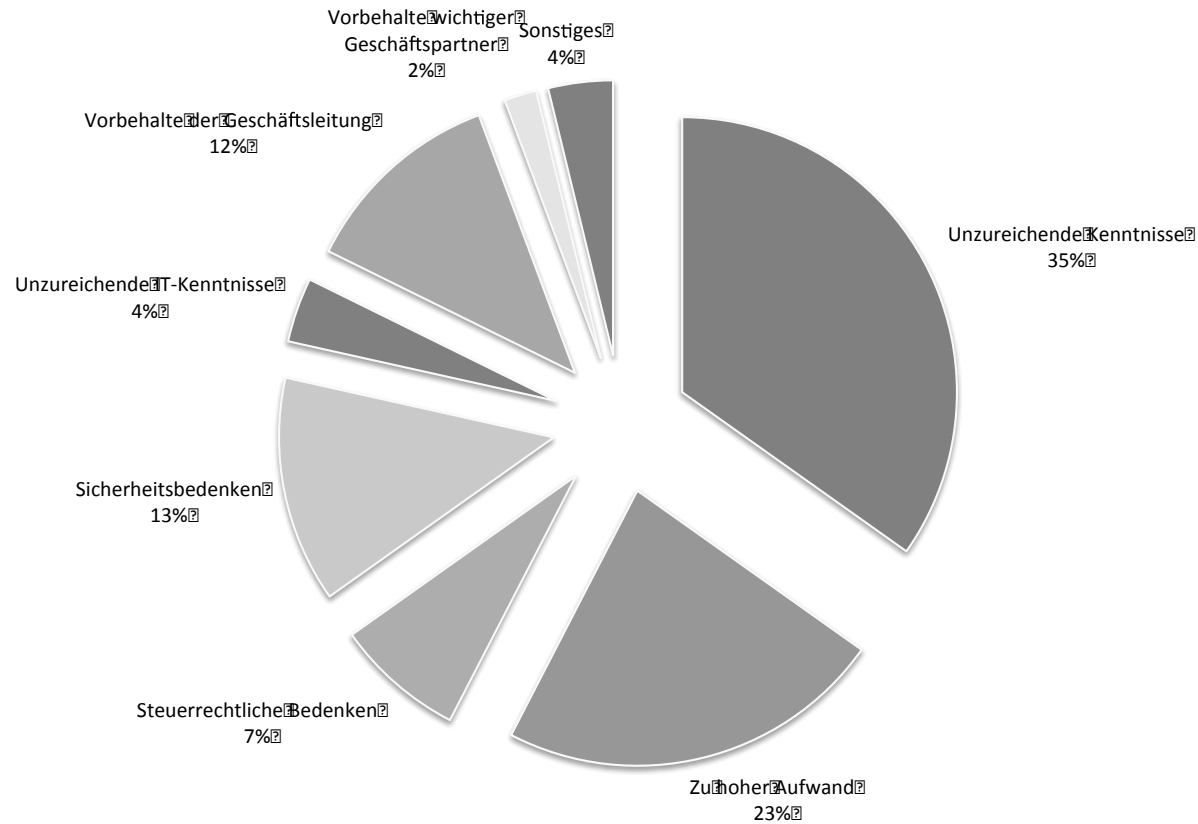
Gründe gegen eine Umstellung für Unternehmen bis 5 MA



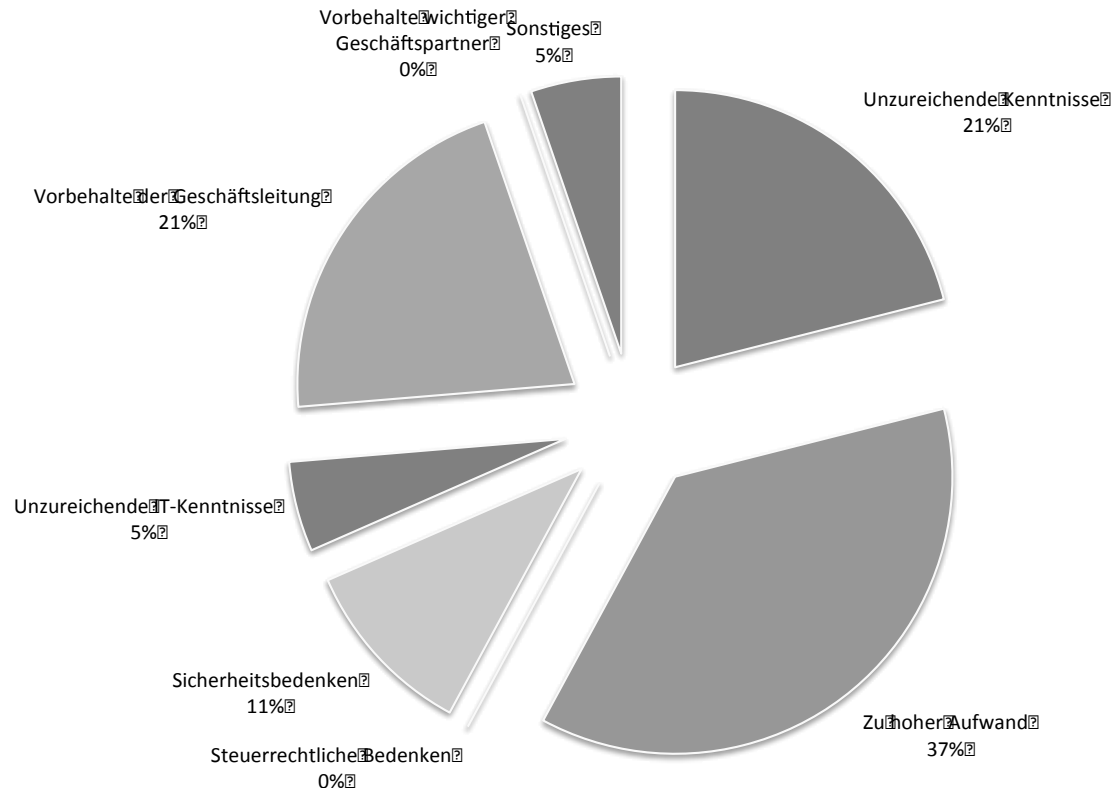
Gründe gegen eine Umstellung für Unternehmen bis 10 MA



Gründe gegen eine Umstellung für Unternehmen mit 10-50 MA



Gründe gegen eine Umstellung für Unternehmen mit 50-250 MA



Zusammensetzung der Stichprobe

Anzahl der Rückläufer: 762

Clusterung nach Unternehmensgröße:		Clusterung nach Rechnungsanzahl:	
Mitarbeiteranzahl	n	Rechnungen pro Jahr	n
Bis 5	232	Bis 100	150
5-10	104	101-1000	161
11-50	156	Über 1000	76
51-250	20	Keine Angaben	375
251-500	4		
Über 500	5		
Keine Angaben	241		
Gesamt	762	Gesamt	762

Ernüchterndes Fazit

- Sicherheitsbedenken sind ein hintergründiges Problem (nur 10% Nennungen)
- Unzureichende Kenntnisse / IT-Kenntnisse nehmen als Problem mit zunehmender Unternehmensgröße ab
- Aufwandsbedenken / Bedenken der Geschäftsleitung nehmen als Problem mit zunehmender Unternehmensgröße zu
- Folgerung: kein Problem des Nicht-Könnens, ein Problem des Nicht-Wollens
 - „Return on Security Investment“ wird nicht deutlich



GESINE: Umsetzung durch Aristaflow



Loan Origination Business Process

Loan Request Formular

Personal Information

Name:	<input type="text" value="Mustermann"/>	First Name:	<input type="text" value="Max"/>
Address:	<input type="text" value="Musterstraße 28"/>		
City:	<input type="text" value="Berlin"/>	State / Zip:	<input type="text" value="12345 Berlin"/>
Email:	<input type="text" value="max@mustermann.de"/>	Day of Birth:	<input type="text" value="05.05.1970"/>
Social Security Number:	<input type="text" value="12345-DP554-P"/>		

Loan Request

Amount:	<input type="text" value="12345"/>	Target Date	<input type="text" value="20.01.2013"/>
Purpose	<input type="text" value="Ich möchte eine Wohnung anzahlen."/>		



Loan Origination Business Process

Customer Identification

Customer Identity Information

Name: First Name: ID:

SSN:

Status:

The identity of the customer has been confirmed.

The local public authorities have verified the personal information (Name, Address).
It has also been assured that the customer is not involved in any criminal issue
or any other event of public interest that would prevent him from being able to receive a
loan.

[Request Identity Check](#)



Loan Origination Business Process

Check Internal Rating

Customer Credit Report Information

Name: First Name: ID:

The following information has been retrieved through the customers credit report.

Payment history (35% contribution to credit score):

Debt (30% contribution to credit score):

Length of credit history (15% contribution to credit score):

Account diversity (10% contribution to credit score):

New credit applications (10% contribution to credit score):

Final Customer Credit Score: Points, based on the FICO score.

Based on the Credit Rating Score the customer is not worthy a credit. Please verify the internal credit information and make a final decision.

☐ Credit worthy ☒ Not Credit worthy, but can apply for a credit in the future



Loan Origination Business Process

Open Account



Request Summary

Name: First Name: ID:

The bank supervisor has approved the loan request. Please confirm all of the following data and checks have been provided:

- ☒ Complete customer data
- ☒ Correct identity confirmation
- ☒ Customer passed internal credit check
- ☒ Customer passed external credit check

By completing this activity you confirm all requirements have been met. An account for the customer will be created with the respective loan amount.


The invoicing process



The invoicing process

Firefox
GESINE Plattform
192.168.42.116:8080/aristainvoice/

Logout | Info | Einstellungen

 Mittelstand-Digital
Usability
eStandards
eKompetenz-Netzwerk

Home
Arbeitsbereich
Rechnungsarchiv
Administration

Meine Aufgaben Rechnung erfassen

Status: Rechnung muss erfasst werden.

Rechnungsinformation

Kreditor:

Erfasst am: 10.04.2013

Rechnungsnummer: 0

Belegnummer: 12345

Belegdatum: 10.04.2013

Fällig am: 10.04.2013

☒ Skonto möglich

Skonto bis: 10.04.2013

Rechnungsbetrag (EUR): 0,00

Historie Anlagen

AUFGABE	BEARBEITER	ZEITPUNKT

Anmerkungen:

Sachliche Prüfung an:

☐ Rechnung reklamieren

Wählen Sie die Rechnungsdatei aus:

NO_OCR OCR

Meine Firma, Musterstraße 1, 01234 Musterhausen
Kundenfirma: Josef Meier
Kundenstraße 2
01234 Kundenhausen

Datum: 10.03.2006
Rechnungsnummer: R0001
Kundennummer: 00001

Rechnung Nr. R0001

Sehr geehrter Herr Meier,
vielen Dank für Ihren Auftrag. Für die erbrachten Leistungen stelle ich Ihnen in Rechnung:

Pos.	Beschreibung	Menge	Einheit	Einzelpreis	Betrag
1	Anfahrt <20km	2	Anfahrt(en)	10,00	20,00
2	Beratungsgespräch	1	Gespräche	25,00	25,00
3	Musterleistung	9	Stunde(n)	35,00	315,00
Total EUR					360,00

Bitte überweisen Sie den Betrag bis zum 24.03.2006 auf das unten angegebene Konto.

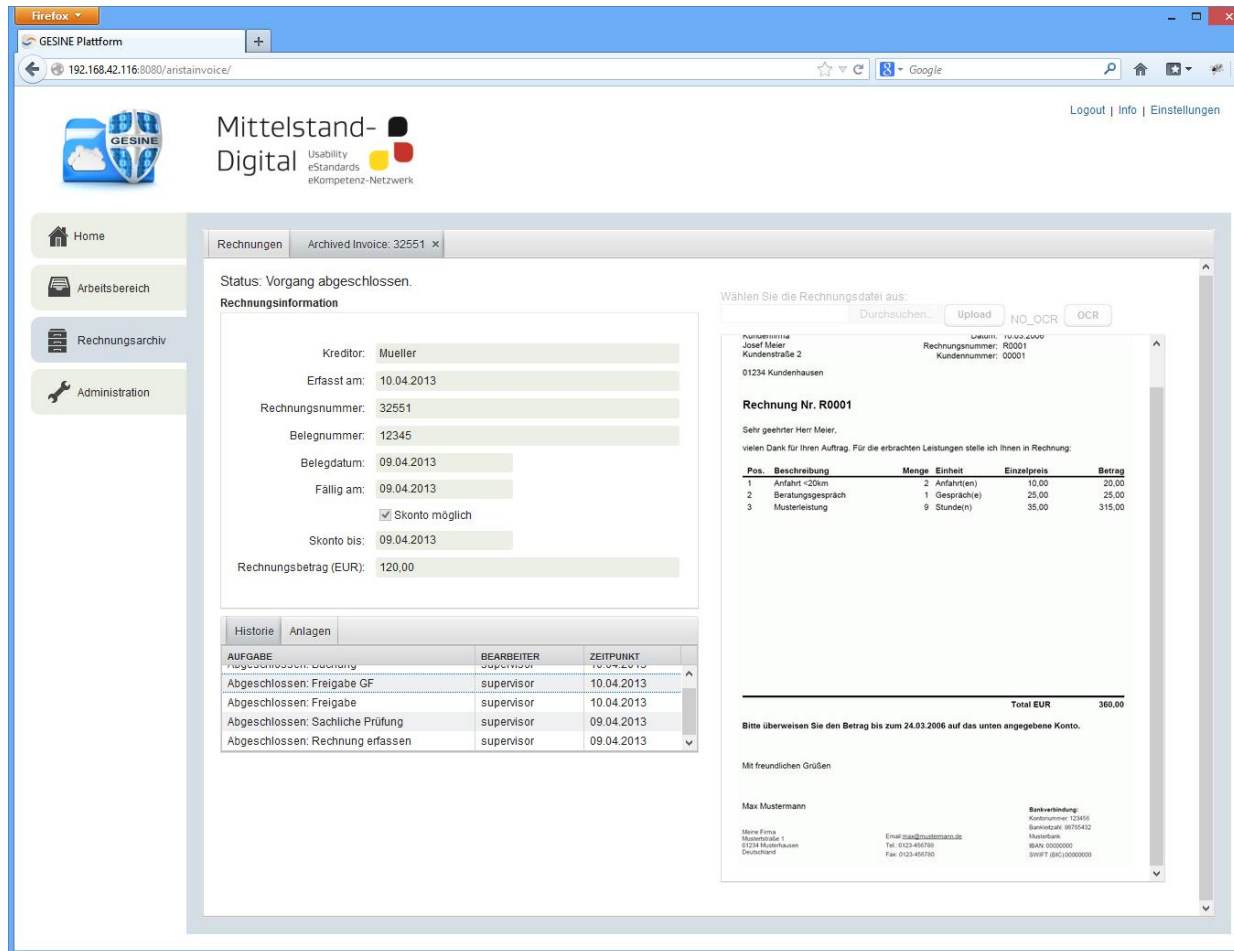
Mit freundlichen Grüßen

Max Mustermann

Bankverbindung:
Kontonummer: 123456
Bankleitzahl: 98765432
Musterbank

Meine Firma, Musterstraße 1
E-Mail: max@mustermann.de

The invoicing process



The screenshot shows the GESINE Plattform web interface in a Firefox browser. The address bar shows the URL 192.168.42.116:8080/aristainvoice/. The interface includes a navigation menu on the left with options: Home, Arbeitsbereich, Rechnungsarchiv, and Administration. The main content area displays the status 'Vorgang abgeschlossen.' and 'Rechnungsinformation' for an archived invoice (32551). The information includes: Kreditor: Mueller, Erfasst am: 10.04.2013, Rechnungsnummer: 32551, Belegnummer: 12345, Belegdatum: 09.04.2013, Fällig am: 09.04.2013, Skonto möglich (checked), Skonto bis: 09.04.2013, and Rechnungsbetrag (EUR): 120,00. Below this is a table with columns: AUFGABE, BEARBEITER, and ZEITPUNKT. The table lists tasks such as 'Abgeschlossen: Buchung', 'Abgeschlossen: Freigabe GF', 'Abgeschlossen: Freigabe', 'Abgeschlossen: Sachliche Prüfung', and 'Abgeschlossen: Rechnung erfassen', all performed by 'supervisor' on '10.04.2013'. On the right, there is a section for 'Rechnung Nr. R0001' with a table of items: Pos., Beschreibung, Menge, Einheit, Einzelpreis, and Betrag. The items are: 1. Anfahrt <20km (2 Anfahrten) at 10,00 each (Total 20,00); 2. Beratungsgespräch (1 Gespräch(e)) at 25,00; 3. Musterleistung (9 Stunde(n)) at 35,00 each (Total 315,00). The total amount is 360,00 EUR. The interface also includes a 'Rechnungen' tab and an 'Archived Invoice: 32551' tab.



Forschungsprojekt: Geschäftsprozess-Sicherheit
zur Verstärkung des Einsatzes von eBusiness-Standards

Mittelstand-
Digital

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

GESINE - Geschäftsprozess- Sicherheit für KMU in der Cloud

Open Identity Summit
2013-09-09 – 2013-09-11
Kloster Banz, Germany

Prof. Dr. Torsten Eymann,
Universität Bayreuth

