

Sicherheit, Nachweisbarkeit und Dynamik in der Digitalisierung

Dr. Christian Weiser
Appaflex GmbH

Datenleck bei der Basler Polizei

Bussen Personendaten von Tausenden Verkehrssündern waren jahrelang frei zugänglich via Internet abrufbar.

VON SAMUEL HUFSCHMID

Die Basler Polizei hat mit ihrem Online-Bussenschalter 2015 Pionierarbeit geleistet. Nach Eingabe eines Codes kann die Busse fürs verbotene Parkieren direkt beglichen werden. Erhöht man die Bussen-Nummer an der richtigen Stelle jedoch um eins, ist die Chance gross, dass nicht die eigene, sondern die Busse eines wildfremden Menschen angezeigt wird. Inklusive dessen Vergehen, Name und Adresse. Lässt man ein Computerprogramm Tausende solcher Abfragen durchführen, ergibt sich ein eigentliches Whois-who-Verzeichnis der Basler Verkehrsünder. Mit dieser Tatsache konfrontiert, hat die Polizei die Personendaten am Montag vom Netz genommen.

«Dürfte nicht geschehen»

Polizeisprecher Martin Schütz sagt: «Bei der Einführung des Online-Bussenschalters haben die involvierten kantonalen Stellen eine Güterabwägung vorgenommen zwischen der Art von Daten und dem Schutzmechanismus auf der einen und der Benutzerfreundlichkeit auf der anderen Seite.» Dabei habe man sich bewusst für eine Methode



Ein Bussenzettel mit QR-Code. BS.CH

mit hoher Benutzerfreundlichkeit entschieden. Von einem Fehler will Schütz nicht sprechen - auch rückblickend nicht. Allerdings gibt er zu, dass es «nicht geschehen dürfe, dass Tausende Datensätze automatisiert eingelesen werden können».

Bernhard Frey Jäggi, Leiter Abteilung Verkehr, sagt: «Ursprünglich hatten wir bei der Bussen-Abfrage eine zusätzliche Sicherheitsstufe eingebaut, nämlich die Autonummer. Als wir aber auch Fussgängern und Velofahrern die Möglichkeit bieten wollten, ihre Ordnungsbussen online zu bezahlen, wurde die Autonummer weglassen.» Bei anderen Vergehen mit heikleren Daten, etwa Fahren in angetrunkenem Zustand oder Raserdelikten, sei eine Online-Abfrage grundsätzlich nicht möglich. «Die online einsehbaren Daten bei

Ordnungsbussen sind auch nicht mehr, als man auch bisher - ganz analog - mit grossem Aufwand hätte recherchieren können. Nämlich indem man einer Strasse entlanggeht und sich die Art der Busse sowie die Autonummer notiert und danach Halterabfragen tätigt.»

Technisch umgesetzt wurde der Online-Bussenschalter von den Zentralen Informatikdiensten. Deren Leiter, Thomas Berger, sagt: «Grundsätzlich ist das System sicher, das wurde bei der Einführung 2015 von externen Experten überprüft. Allerdings würde man mit dem heutigen Wissen für den Online-Bussenschalter eine zusätzliche Sicherheitsstufe dazwischenschalten. Dies wird nun nachgeholt.» Die Abwägung zwischen grösstmöglicher Datensicherheit und möglichst grosser Benutzerfreundlichkeit bleibe allerdings eine Gratwanderung.

Kritik vom Datenschützer

Mit den Recherchen dieser Zeitung konfrontiert, ist auch der kantonale Datenschutzbeauftragte aktiv geworden. «Dass zusätzlich zur Autonummer auch Namen und Adressen der Halter angezeigt werden und dass diese automatisiert abgefragt werden können, das geht nicht», sagt er. Weil die Polizei ihrerseits aber bereits gehandelt habe und die Personendaten nicht mehr angezeigt werden, sei eine Intervention nicht nötig gewesen. «Wir prüfen derzeit gemeinsam weitere Massnahmen, um maschinelle Abfragen zu verunmöglichen.»

Quelle:
Aargauer
Zeitung
20.03.19

Agenda

- Firmenvorstellung
- Herausforderungen und Zielkonflikte
- Compliance Manager
- Prozess-Sicherheit und Life-Cycle
- Nachweisbarkeit / Versionierung und Audit Trail für Reportings
- Digitalisierung von Prozessen
- Erfahrungsbericht



Startup mit 25 Jahren Berufserfahrung

Appaflex GmbH

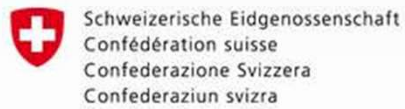
Im Technopark Aargau
Badenerstrasse 13
CH-5200 Brugg
Tel: +41 56 521 30 70
Mail: info@appaflex.ch



2015

25

Digitalisierung – aber sicher !



Eidgenössisches Departement für
auswärtige Angelegenheiten EDA



MITREVA



RÉPUBLIQUE
ET CANTON
DE GENÈVE

EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE



MIGROS



BASEL
LANDSCHAFT



LANDESVERWALTUNG
FÜRSTENTUM LIECHTENSTEIN



Kanton Zürich

solothurn

Anwendungselemente / Themengebiete:

Risk Management (RA + Simulationen)

Auftragsverwaltung

Umfragen (z.B. Kundenzufriedenheit)

Checklisten-Bearbeitung

Dokumentenablage

Beteiligungen/
Eigentumsanteile

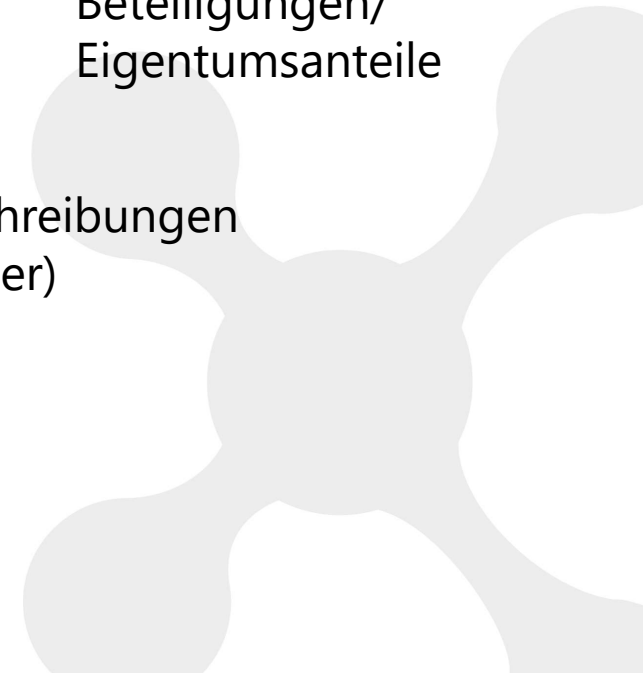
Ressourcenplanung

B2B-Ausschreibungen
(Mini-Tender)

Change Management
+ Request Ticketing

Reporting

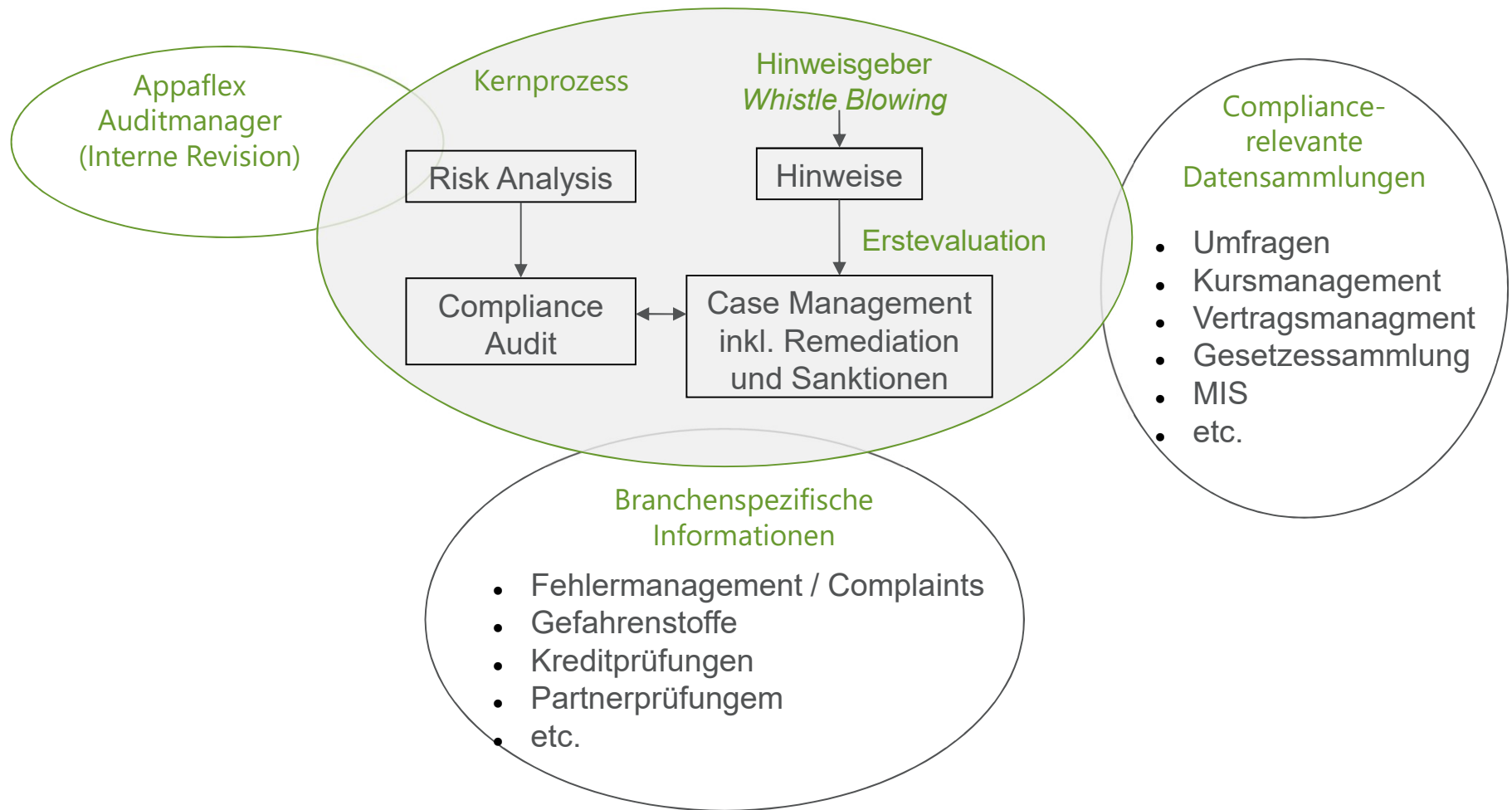
Portalfunktionalitäten



Herausforderungen / Zielkonflikt



Compliance Manager



Anwendung interaktives Meldesystem

Security:

- Hinweise *anonym* entgegennehmen
- Speicherung in einer speziell geschützten Datenbank



Usability:

Sichere Kommunikation
zwischen den Dialogpartnern



Hinweis - Neuer Eintrag

Speichern

Ihre Meldung Zusatzdokumente Angaben zur Person (freiwillig) Abschluss

Willkommen beim interaktiven Meldesystem

Bevor Sie fortfahren, beachten Sie bitte folgende Hinweis

- Ihre Meldung wird **streng vertraulich** behandelt.
- Sie können eine Meldung anonym abgeben, wenn Sie im dritten Schritt die Angaben zur Person leer lassen.
- Es haben nur Personen Zugang zu Ihrer Meldung, die für deren Bearbeitung verantwortlich sind und die Vertraulichkeitsvereinbarung unterschrieben haben.
- Falls es sich um eine Beschuldigung handelt, werden die Beschuldigten jedoch Zugang zu den Inhalten der Anschuldigung erhalten.
- Die Identität eines Meldenden wird nur dann offengelegt, wenn sich nachträglich herausstellt, dass Anschuldigung bewusst falsch erhoben wurden.
- Ihre Meldung wird in einer Datenbank gespeichert. Mit dem Click auf **Weiter** stimmen Sie der Speicherung explizit zu.

Inhalt der Meldung

Diese besteht aus einer **Kurzbeschreibung** - hier müssen Sie einen prägnanten Titel eingeben.

Die Kategorisierung können Sie uner bereits bestehenden wählen, bei Detailbeschreibung haben Sie Platz für weitergehende Informationen.

Nr. Ihrer Meldung

Kurzbeschreibung * → → → →

Auswahl der Kategorisierung

Kategorisierung

Detailbeschreibung

Hinweis

Speichern

Ihre Meldung Zusatzdokumente Angaben zur Person (freiwillig) Abschluss

Rückfragen

Dieses Meldesystem ermöglicht es, mit Ihnen - auch anonym - in Kontakt zu treten, z.B. falls weitere Details benötigt werden oder bei Unklarheiten. Die Zugangsdaten für Rückfragen erhalten Sie dabei im letzten Schritt, so dass Sie sich jederzeit online anmelden können. Falls Sie Ihre E-Mail-Adresse hinterlegen, werden Sie über eine neue Rückmeldung automatisch informiert.

Rückfragen erlaubt? * Ja Nein

Persönliche Angaben

Ihre Angaben sind freiwillig. Falls Sie anonym bleiben möchten, füllen Sie diese nicht aus.

Vorname / Nachname

Tel. Nr.

E-Mail

zurück

ABSCHLIESSEN

WEITER

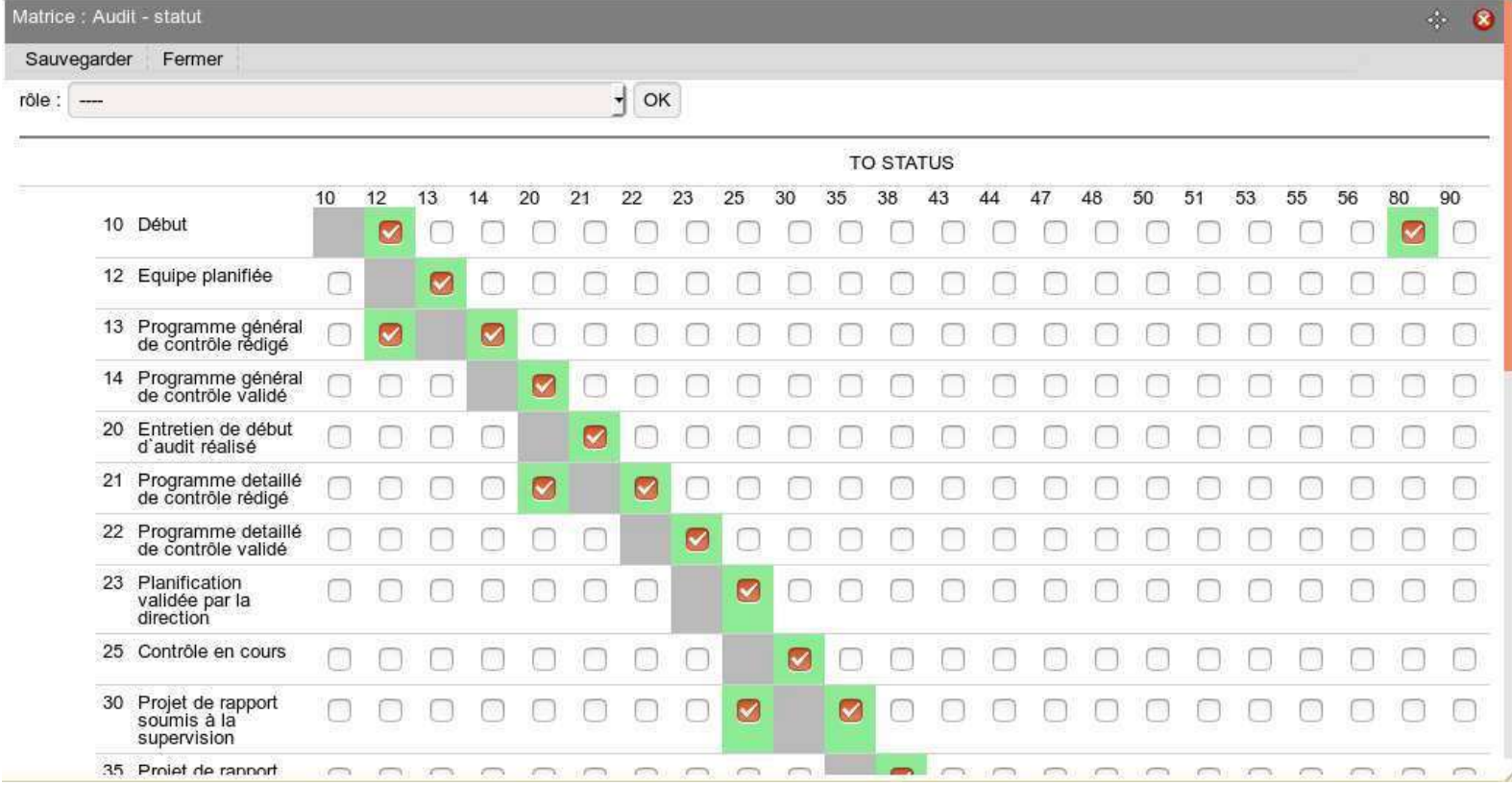
Prozess-Sicherheit und Life cycle:

- In der **Anwendung** : Korrekte Ausführung von Abläufen / Workflows
=> Sicherheit, dass Software konsistent ausgeführt wird
- In der **Technik** : Funktionierendes Change Management
=> Sicherheit, dass Software integer aktualisiert wird
- In der **Evolution**: Geordnete Weiterentwicklungen
=> Sicherheit, dass Software verlässlich ausgebaut wird
- In der **Datenverarbeitung** : Nachweisbarkeit / Versionierung
=> Sicherheit, dass Daten nachvollziehbar bewirtschaftet werden

Lösungsansatz von Appaflex: **Definieren statt Programmieren**



Appaflex : Prozess Management



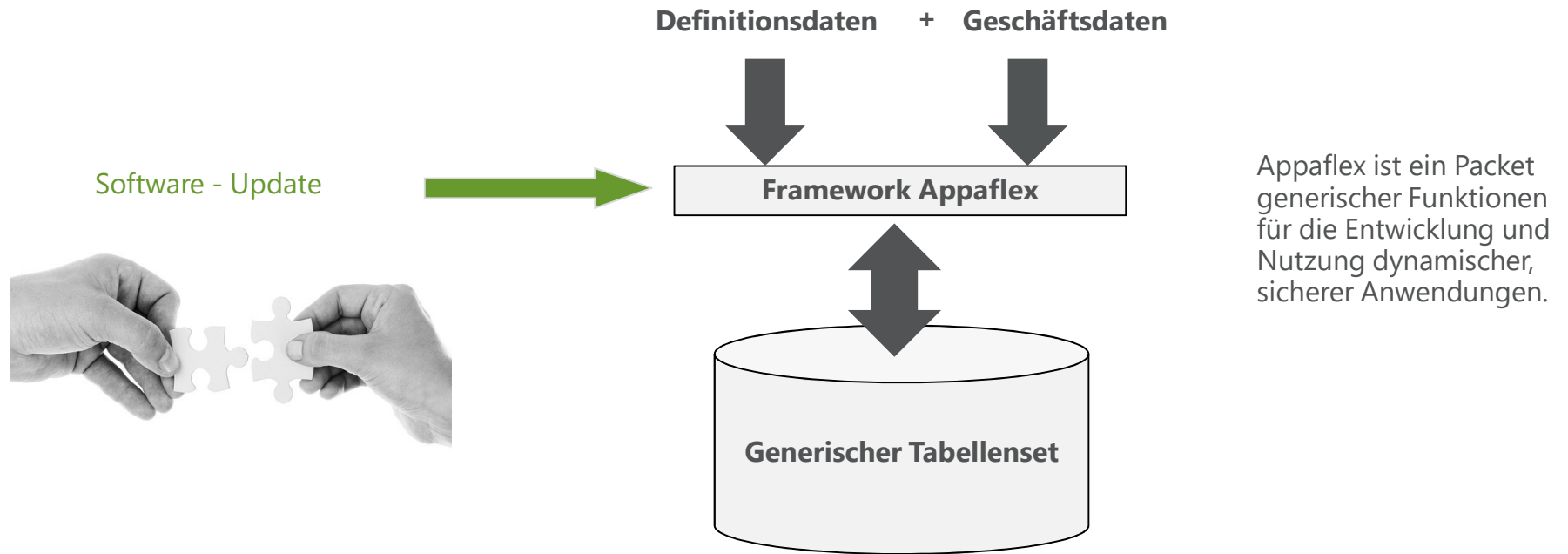
Appaflex : Sicherheit trotz Dynamik

The screenshot displays the Appaflex user interface. On the left is a form for 'Nutzvoll AG > Filialrevision'. On the right is a table with columns for ID, Attribut, Format, Subformat, and Sort Zoom. The table lists various attributes like 'Allgemein', 'Org ID', 'Organisation Name', etc., with their respective formats and sort orders.

A	ID	Attribut	Format	Subformat	Sort Zoom
▶	AMA@00900000003000000115	# Allgemein	Control	Title	a020
▶	AMA@00900000003000000000	Org ID	Text		a040
▶	AMA@00900000003000000001	Organisation Name	Text		a060
▶	AMA@00900000003000000446	Revisionsgruppe	Status		a065
▶	AMA@00900000003000000425	Auftragsserie ID	Text		a085
▶	AMA@00900000003000000149	Auftrag aus Risikoanalyse	Yesno	Dropdown	a090
▶	AMA@00900000003000000159	# Merkmale	Control	Subtitle	a100
▶	AMA@00900000003000000138	Auftrag ID	Counter		a120
▶	AMA@00900000003000000452	Auftrag ID (App)	Text		a130
▶	AMA@00900000003000000150	Auftragsstatus	Status	Workflow	a135
▶	AMA@00900000003000000144	Auftragstitel	Text		a140
▶	AMA@00900000003000000417	Geschäftsjahr	Text		a150
▶	AMA@00900000003000000160	Beginn	Datetime	Date	a160
▶	AMA@00900000003000000161	Ende	Datetime	Date	a180
▶	AMA@00900000003000000534	Archivdatum	Datetime	Date	a185
▶	AMA@00900000003000000664	# Textbausteine : Auftragsziele	Control	Formfill	a199
▶	AMA@00900000003000000173	Auftragsziele	Multiline		a200

Evolution mittels «Definieren statt Programmieren». Sicherheit (geprüfte Algorithmen) und Dynamik (Anpassungen an den Bedarf) sind kein Widerspruch!

Appaflex : Change Management



Appaflex ist ein Paket generischer Funktionen für die Entwicklung und Nutzung dynamischer, sicherer Anwendungen.

Appaflex : Nachweisbarkeit / Versionierung

Audit - Change log Filialrevision							
Close Format : No Panorama							
Overview							
A	Date	User	Action	Method	Options	Role	Reason
▶	28.08.2018 17:01:26	adminusr	User Admin	edit	Standard		Auditmanager
▶	28.08.2018 17:01:20	adminusr	User Admin	edit	Standard		Auditmanager
▶	17.07.2018 02:46:19	adminusr	User Admin	edit	Standard		Auditmanager
	17.05.2018 14:16:34	chweiser	Ch. Weiser	edit	Standard		Auditmanager
	17.05.2018 13:22:02	chweiser	Ch. Weiser	edit	Standard		Auditmanager
	17.05.2018 09:39:36	chweiser	Ch. Weiser	edit	Standard		Auditmanager
▶	17.05.2018 09:33:15	chweiser	Ch. Weiser	edit	Standard		Auditmanager
▶	17.05.2018 09:26:21	chweiser	Ch. Weiser	edit	Standard		Auditmanager
	24.01.2018 11:50:10	chweiser	Ch. Weiser	edit	RichtextEditor	CKEditor	Auditmanager
▶	05.09.2017 14:05:02	root	Root user	edit	Standard		Auditmanager
	04.05.2017 15:29:11	chweiser	Ch. Weiser	edit	Standard		Auditmanager
▶	04.05.2017 15:25:40	chweiser	Ch. Weiser	edit	Standard		Auditmanager
	03.04.2017 11:03:36	chweiser	Ch. Weiser	edit	Standard		Auditmanager
▶	02.03.2017 15:25:26	chweiser	Ch. Weiser	edit	Standard		Auditmanager

Wer hat = Benutzer
 Wann = Zeitpunkt
 Was = Inhalt
 Wie = Rolle
 Wodurch = Methode
 getan* ? = Aktion

= Sicherheit für Unternehmen und Mitarbeitende

* erstellt, geändert, gelöscht, vererbt, verschoben, wiederhergestellt, etc.

Digitalisierung von Prozessen (Integration)



Portale bieten ein hohes Potential für Effizienzverbesserung bei strengen Sicherheitsanforderungen.

Meist wird – gerade im B2B-Bereich - die doppelte Dynamik der Akteure unterschätzt.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössische Finanzkontrolle
EC+

Aktuell | Empfehlungen | ?

Logout

Umsetzungsmeldung

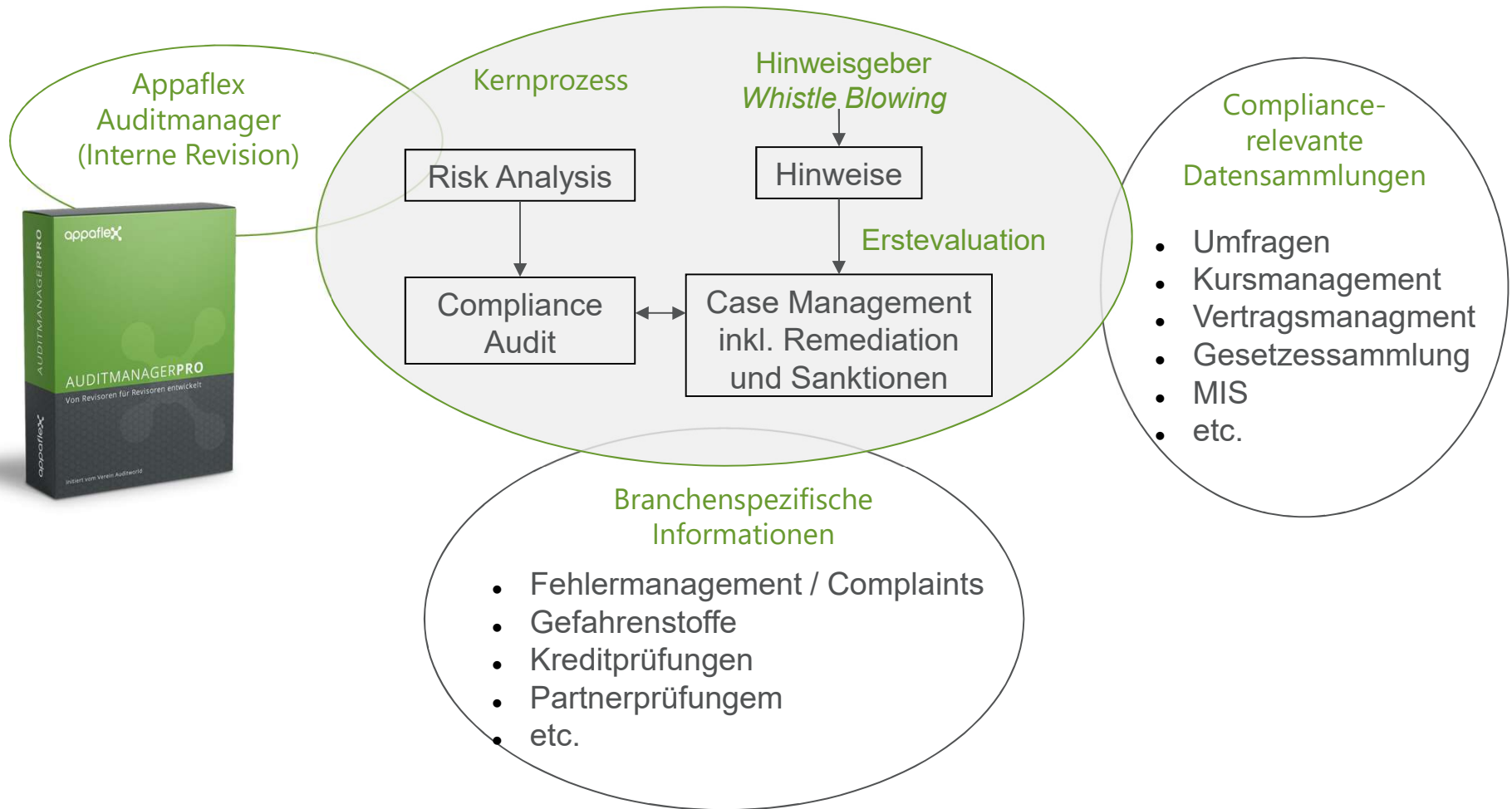
Speichern | Definiv setzen | Abbrechen

Empfehlung	Empfehlungstext	10	Evaluationsstufe	nicht evaluiert
Departement	8	UV/EX		
Art	010			
Prüfung	12277	Subventionsprüfung Aktionsplan Holz		
Empfehlungsnummer	11			
Empfehlungstext	Die EPK empfiehlt, die für den Aktionsplan Holz 2013 - 2017 vorgesehenen Subventionen um die in der Vorperiode eingetragenen Mittel für die Schweizerische Laubbäumeverwaltung, Waldentwicklung Holzbaustysteme und Sensibilisierung öffentliche Bauherren zu kürzen. Um wiederholenden Geben, ist insbesondere für die Datenprüfung und die Informations, sind soweit notwendig die bestandsaufwand im Budget des BAUFU und in der Regel um Dienstleistungsverträge und nicht um Subventionen handeln. Die Subvention APH ist aufzuheben.			
Aktuelle Nachricht	30.06.2016			
Stellungnahme	Beurteilungstext	Stellungnahme durch EPK akzeptiert		
Stellungnahmetext	Das BAUFU hat die Wirkung des Aktionsplan Holz I durch eine externe Firma evaluieren lassen und kommt zu anderen Schlussfolgerungen (siehe auch Bericht, Kap. 5). Entgegen der Zielsetzung ist zu kurz, um abschliessende Beurteilungen vornehmen zu können. Zielsetzung: Der Impact wurde von einem Fachgremium als hoch eingestuft. Gemäss der Wirkung des Aktionsplan Holz muss sich in weiterer Linie in der Erhebung aller Antragsverfahren, bei der Holzproduktion, und nicht in der Erhebung der (Produktionskosten) über v.a. ein Bereich Laubbäume/Erhebung kann der APH erste Schritte schreiben, welche eine detaillierte Prüfung nicht möglich gewesen wären. Hingegen ist die Analyse der EPK bezüglich der schwer bewertbaren Rahmenbedingungen (Waldentwicklung) korrekt. Das BAUFU wird dies bei der Neuausarbeitung des APH Holz I berücksichtigen. Das BAUFU achtet sehr auf, nach der Hälfte der Laufzeit des APH I zusammen mit der EPK eine gemeinsame Evaluation durchzuführen, aufgrund dieser Resultate über den			
Umgesetzt bis	31.12.2015			
Zuständigkeit Umsetzung	MUR / WAB / Rolf Manser			
Stellungnahmetext	Beurteilungstext	Umsetzungsmeldung erstattet		
Meldung zur Umsetzung	Dies ausstellen			
Nachricht beitragen / Umsetzungsmeldung	Inhaltsangabe			

Dies ist eine Pro-A Empfehlung: Was ist Ihre derzeitige Einschätzung bezüglich der Inanspruchnahme?

auf Kurs / nicht getriggert getriggert / nicht möglich (Kommentar zwingend)

Anwendungsgebiete im Compliance Umfeld



Erfahrungsbericht : Baloïse Holding AG

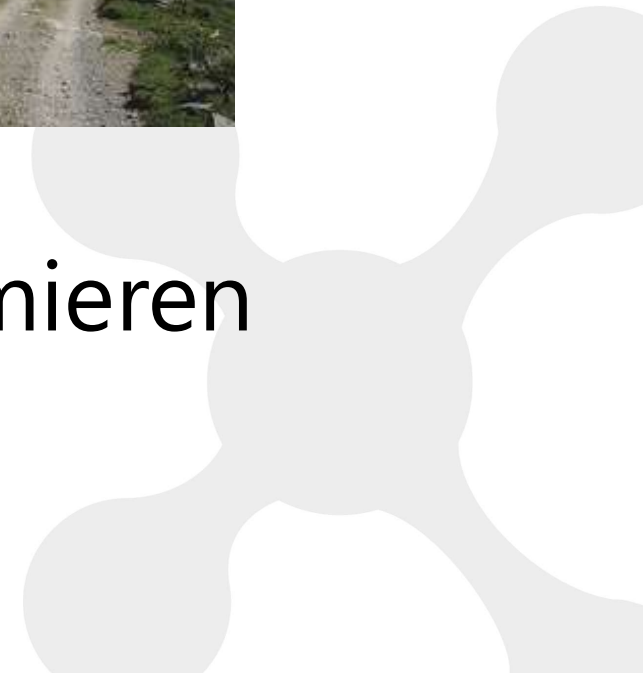
Hr. André Mäder
Head of IT Audit
Group Internal Audit



Security UND Dynamik



Definieren statt Programmieren



Interesse geweckt?



Gutschein für einen 1-stündigen Workshop

Erleben Sie live, wie schnell und einfach sich Ihre Geschäftsanwendung mit Appaflex definieren lässt.

Nehmen Sie mit uns Kontakt auf, um einen Termin zu vereinbaren:

Tel: +41 56 521 30 70

E-Mail: info@appaflex.ch

Appaflex GmbH
Im Technopark Brugg
Badenerstrasse 13
CH-5200 Brugg
www.appaflex.ch