ARBEITSANWEISUNG
ASSESSMENT-MANAGEMENT TKB

Inhalt

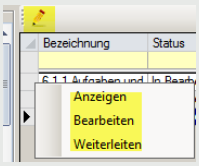
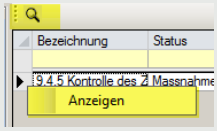
1 Ausgangslage

Im Assessment-Management-Tool der TKB werden die Assessments der Informationssicherheit verwaltet. Die Assessment definiert die Informationssicherheit aufgrund von gesetzlichen und regulatorischen Vorgaben. Die Durchführung der Assessments erfolgt durch Mitarbeitende der Informationssicherheit sowie durch Abteilungsleiter der IT und auch ausserhalb der IT. Prüfungen, Feststellungen und Massnahmen werden im Tool nachvollziehbar dokumentiert.

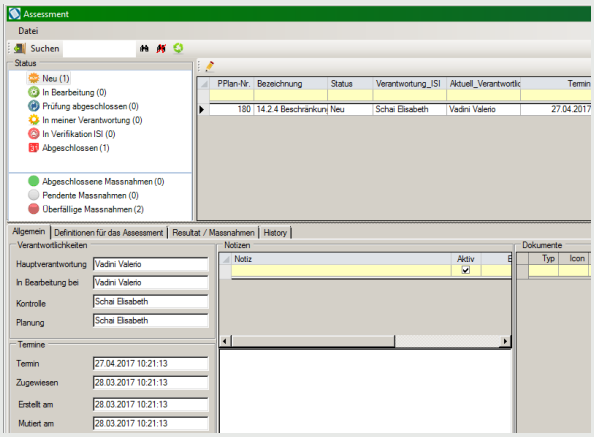
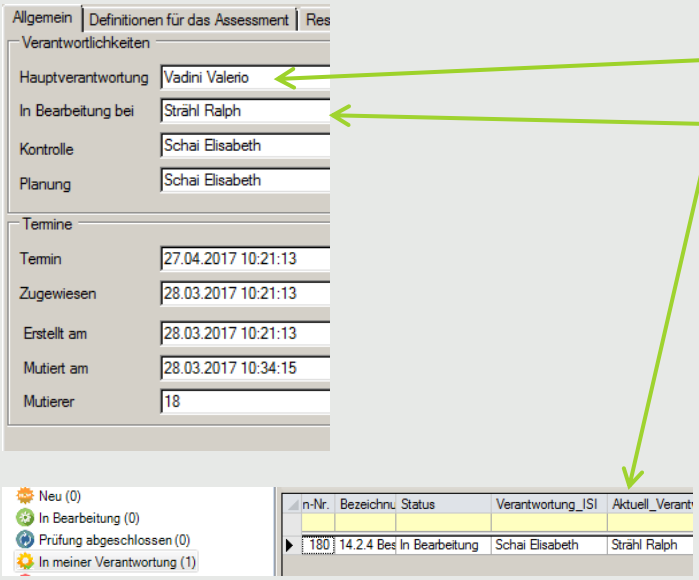
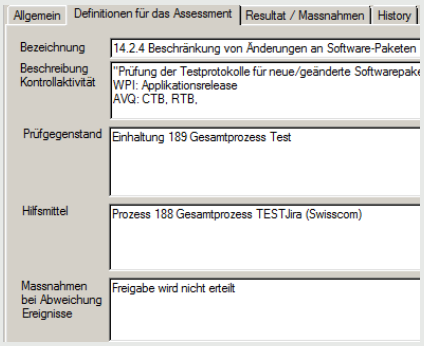
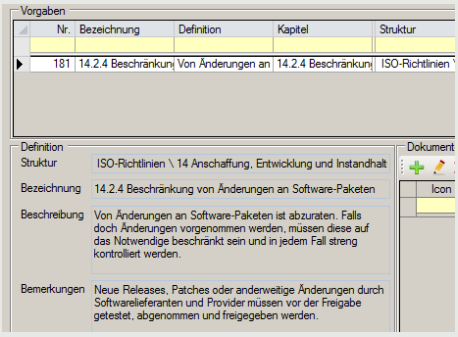
2 Anmeldung im Tool

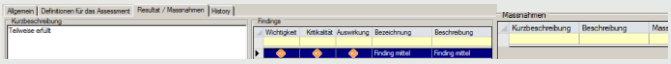
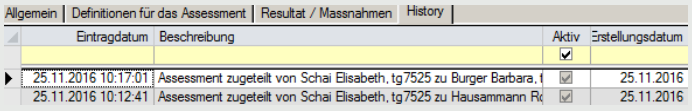
Nr.	Abbildung	Beschreibung
1.	Assessment-Management starten	Anmeldung auf Prod-Umgebung
2.	Berechtigungsstufen	Unterschiedlich für Informationssicherheit und Assessment-Verantwortliche

3 Allgemeine Bearbeitungshinweise

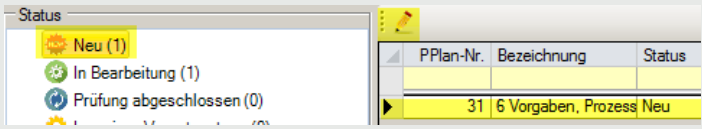
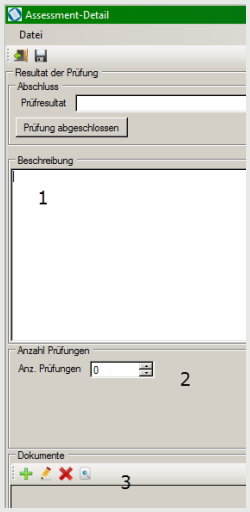
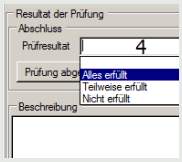
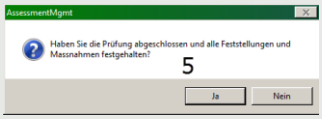
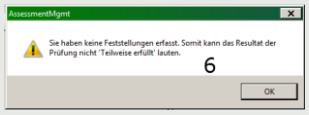
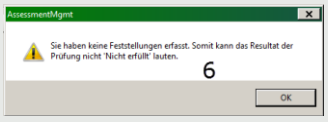
Nr.	Abbildung	Beschreibung
3.		Element (Feststellung, Massnahmen, Dokumente) - zufügen - bearbeiten - löschen - anzeigen
4.		Markiertes Element kann angezeigt, bearbeitet oder weitergleitet werden
5.		Nur Anzeige möglich, z:B. weil Assessment bereits abgeschlossen ist

4 Assessment-Übersicht Allgemein

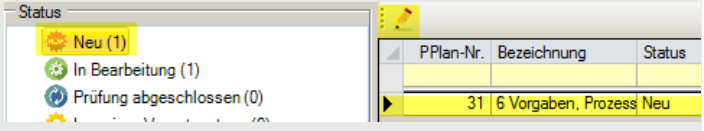
Nr.	Abbildung	Beschreibung
6.		**Assessment** Übersicht über alle verantworteten Assessements - Bearbeitungsstati - Verantwortungen - Definitionen zum Assessment - erfasste Resultate und Massnahmen - History
7.		**Allgemein** Hauptverantwortung: Bleibt immer beim Assessmentverantwortlichen, auch wenn Assessment zur Bearbeitung weitergegeben wird. Kontrolle/Planung zeigt die Verantwortlichkeit innerhalb der Informationssicherheit an.
8.		**Definitionen für das Assessment** - Beschreibung der Kontrollaktivität - Prüfgegenstand - Hilfsmittel - Massnahmen bei Abweichung
9.		**Vorgaben** Zeigt die regulatorischen oder gesetzlichen Vorgaben des Assessments an - ISO-Richlinien - FINMA-Vorgaben - Vorgaben Datenschutzgesetz - weitere möglich inkl. deren genauen Bezeichnung und Beschreibung

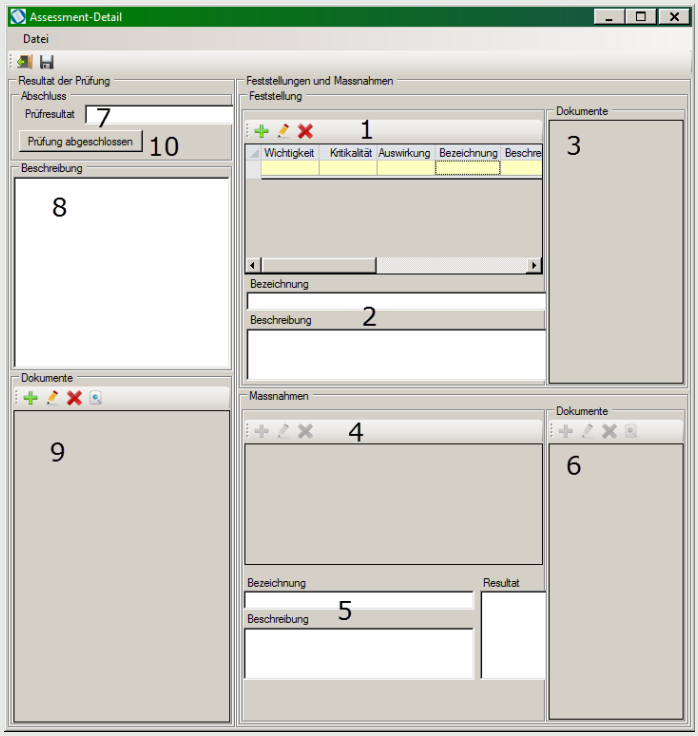
Nr.	Abbildung	Beschreibung
10.		**Resultat/Massnahmen** Die erfassten Einträge werden angezeigt.
11.		**History** Nachverfolgung neue Zuteilung Assessements

5 Assessments / Prüfungen durchführen ohne Feststellung

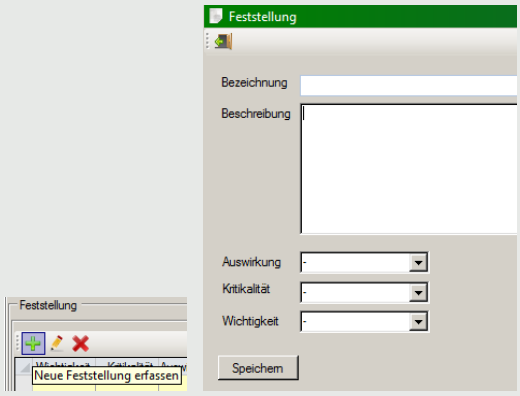
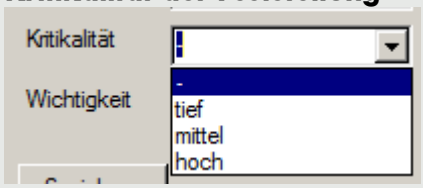
Nr.	Abbildung	Beschreibung
12.		**Assessment durchführen** „Neu" anwählen und Assessment-Detail mit  Prüfschritt bearbeiten oder mit Doppelklick öffnen
13.	    	**Assessments ohne Feststellung** Prüfung durchführen 1 Prüfresultat beschreiben 2 Anzahl Prüfungen, wenn mehrere Kontrollen ohne Feststellung durchgeführt wurden, z.B. tägliche oder monatliche Kontrollen 3 Dokumente zufügen, die beschreiben wie Prüfung durchgeführt wurde Prüfung abschliessen 4 „Alles erfüllt" auswählen Prüfung abgeschlossen wählen 5 Mit Ja Bestätigen, nach dem Abschluss kann an den Einträgen nichts mehr geändert werden. 6 Assessments ohne Feststellung müssen mit „Alles erfüllt" abgeschlossen werden, es ergeben sich Warnmeldungen.

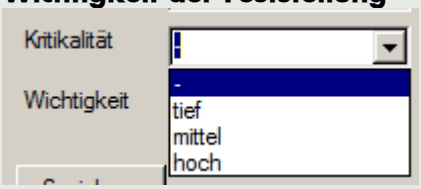
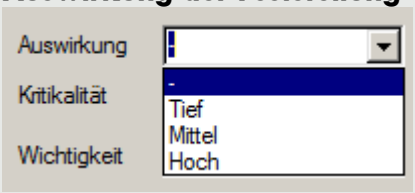
6 Assessments / Prüfungen durchführen mit Feststellungen

Nr.	Abbildung	Beschreibung
14.		**Assessment durchführen** „Neu" anwählen und Assessment-Detail mit  Prüfschritt bearbeiten oder mit Doppelklick öffnen

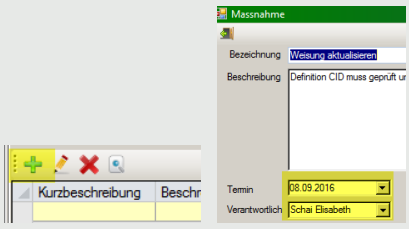
Nr.	Abbildung	Beschreibung
15.		**Assessment-Detail – Übersicht** **Feststellung** 1 Dokumentieren gemäss Kap. 7 2 Bezeichnung und Beschreibung wird übernommen 3 Dokumente zu Feststellung zufügen **Massnahmen** 4 beschreiben gemäss Kap.8 5 Bezeichnung und Beschreibung wird übernommen 6 Dokumente zu Massnahmen zufügen **Resultat der Prüfung** 7 Prüfresultat gemäss Kap. 9 8 Prüfresultat beschreiben 9 Dokumente zu Prüfung zufügen, falls dies noch notwendig sein sollte. 10 Prüfung abschliessen

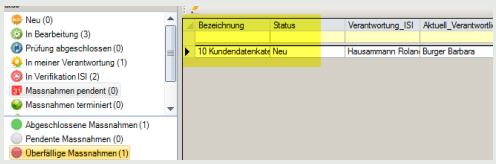
7 Feststellung erfassen

Nr.	Abbildung	Beschreibung
16.		Bezeichnung: Kurzbeschreibung der Feststellung Beschreibung: ausführliche Beschreibung wenn kein zusätzliches Dokument vorliegt Kritikalität, Wichtigkeit und Auswirkung der Feststellung differenziert bestimmen
17.	**Kritikalität der Feststellung** 	**-**  Keine Kritikalität **Tief**  Die Feststellung ist nicht kritisch. z.B. Iconberechtigung nicht entfernt, in Applikation wurde Berechtigung gelöscht **Mittel**  Die Feststellung betr. einzelne Dateien z.B. Daten mit CIDs sind allgemein einsehbar **Hoch**  Es handelt sich um eine Feststellung in einer geschäftskritischen Applikation, mit

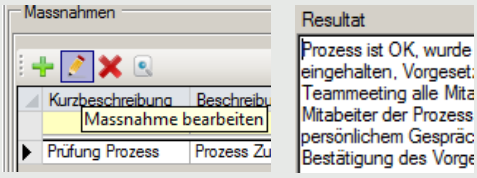
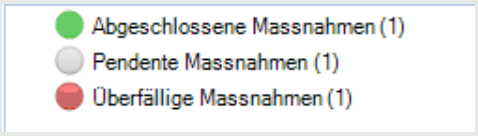
Nr.	Abbildung	Beschreibung
		einer hohen Bedrohungsstufe oder Cybervorfall
18.	**Wichtigkeit der Feststellung** 	- Wichtigkeit null **Tief** Die Feststellung ist nicht sehr wichtig. z.B. Korrektur einer Bezeichnung notwendig **Mittel** Schaden könnte fahrlässig entstehen (z.B. Notfalluser wurde nicht zurückgesetzt) **Hoch** Feststellung hat grosse Auswirkungen auf wichtige Geschäftsprozesse, z.B. E-Banking
19.	**Auswirkung der Feststellung** 	- Keine Auswirkung **Tief** kleine Auswirkungen auf Sicherheit (z.B. Unklarheiten/Fragen in Provider-Reports) **Mittel** Informationssicherheit beeinträchtigt, (z.B. Benutzer hat falsche Berechtigungen) **Hoch** Informationssicherheit gefährdet (z.B. Datenverlust möglich, Risiko von Reputationsschaden)
20.	**Gesamtbeurteilung**	Beurteilung der Wichtigkeit und Kritikalität ergibt die Auswirkung. Ist die Auswirkung **hoch** muss die Informationssicherheit unmittelbar informiert werden. Bei Auswirkung **mittel** und **hoch** müssen Massnahmen definiert werden.

8 Massnahme erfassen

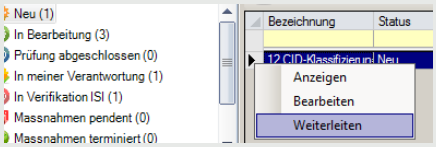
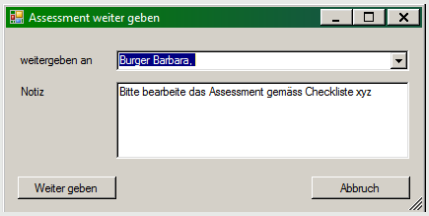
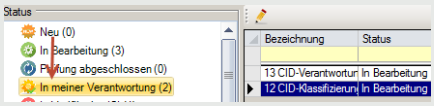
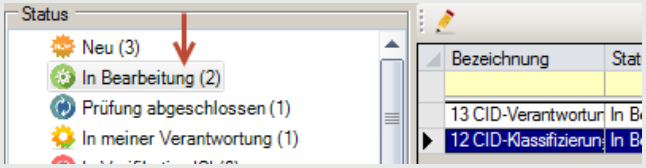
Nr.	Abbildung	Beschreibung
21.		**Massnahmen erfassen** Massnahme definieren, terminieren und zuordnen. Sie kann selbst durchgeführt werden oder zur Durchführung weitergegeben werden.

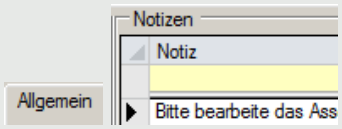
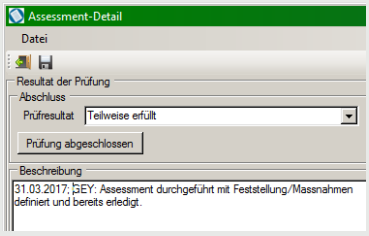
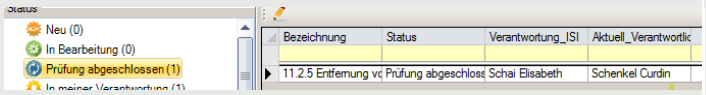
Nr.	Abbildung	Beschreibung
22.	Guten Tag Ihnen wurde vom Assessment "12.4.4 Zeitsynchronisation" die Massnahme "Massnahme 1" zur Bearbeitung zugewiesen. Bearbeiten Sie dieses bitte im Assessment-Management-Tool. (Assessment-Management starten)	Bei der Weiterleitung der Massnahme wird Mail ausgelöst.
23.		Massnahme wird bei zugewiesenem Benutzer als pendent oder überfällig angezeigt und kann durchgeführt werden gemäss Kapitel 9, Massnahmen durchführen.

9 Massnahmen durchführen

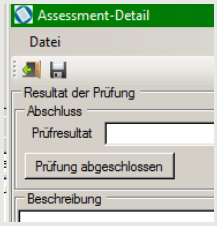
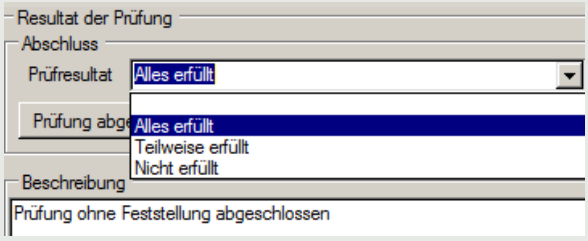
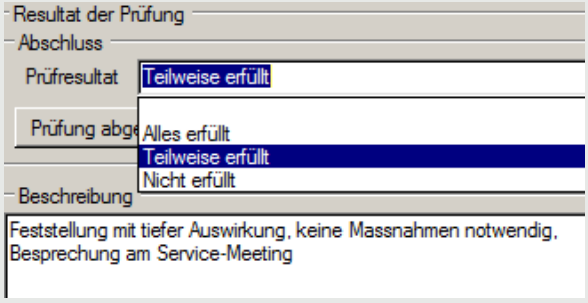
Nr.	Abbildung	Beschreibung
24.		Massnahme durchführen und Resultat im neu geöffneten Fenster beschreiben. **Dokumente**, die Erledigung der Massnahme bestätigen, zufügen, bei **Mittel** und **Hoch gewichteten** Feststellungen zwingend notwendig.
25.		Status-Anzeige: abgeschlossene Massnahmen

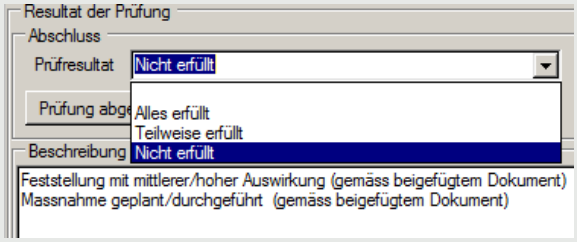
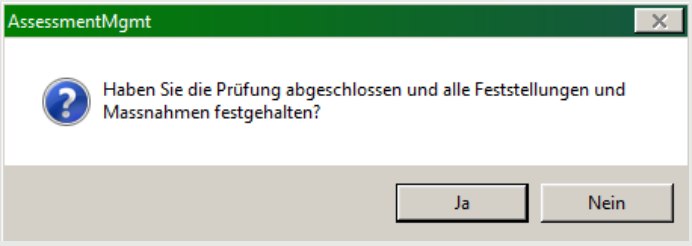
10 Assessments weiterleiten

Nr.	Abbildung	Beschreibung
26.	  	Ein Assessment kann einem Mitarbeitenden, Abteilungsleiter oder Vorgesetzten zur Bearbeitung weitergeleitet werden. Bearbeiter auswählen weitergeben. Bearbeiter wird mit Mail avisiert **Hauptverantwortung** für Assessment **bleibt** beim Assessmentempfänger Statusänderung wird angezeigt
27.		Mitarbeiter sieht zugewiesenes Assessment im Status „In Bearbeitung“ inkl. der entsprechenden Notiz Assessment bearbeiten gem. Kap. 5 bis 9.

Nr.	Abbildung	Beschreibung
		
28.	 	Prüfung/Assessment abschliessen gem. Kap. 11, zusätzlich kurze Bemerkung erfassen Hauptverantwortlicher erhält Mail, dass Mitarbeiter Assessment abgeschlossen hat und er die Prüfung vornehmen kann.
29.		Anzeige beim Hauptverantwortlichen In „Prüfung Abgeschlossen“. Er muss Assessment noch endgültig abschliessen gem. Kap. 11.

11 Prüfung abschliessen

Nr.	Abbildung	Beschreibung
30.		Wenn das Assessment (Prüfung) komplett abgeschlossen ist, schliesst der Verantwortliche die Prüfung ab. Nach dem Abschluss sind keine Änderungen mehr möglich.
31.		**Abschluss** Keine Feststellung=Prüfresultat =Alles erfüllt **Beschreibung** z.B. Prüfung ohne Feststellung abgeschlossen, konkret beschreiben was, wann und wie geprüft wurde, keine Massnahmen notwendig
32.		**Abschluss** Prüfresultat = Feststellung „tief“ teilweise erfüllt (min. eine Feststellung muss erfasst werden) **Beschreibung** Konkrete Beschreibung der Feststellung „tief“, wenn ergänzende Dokumente vorhanden sind, reicht Kurzbeschreibung, üblicherweise keine Massnahmen erforderlich

Nr.	Abbildung	Beschreibung
33.		**Abschluss** Feststellung mittel/hoch = nicht erfüllt immer Massnahmen notwendig
34.		Prüfung oder Verifikation(wenn Assessment weitergegeben wurde) durch Assessmentverantwortlichen abschliessen. Assessment kann nachher nicht mehr bearbeitet werden. Massnahmen müssen noch nicht erledigt, jedoch definiert sein. Sie bleiben in Verantwortung des Besitzers des Assessments.