

# ARBEITSANWEISUNG

## ASSESSMENT-MANAGEMENT TKB

### Inhalt

1	Ausgangslage	1
2	Anmeldung im Tool	1
3	Allgemeine Bearbeitungshinweise	1
4	Assessment-Übersicht Allgemein	2
5	Assessments / Prüfungen durchführen ohne Feststellung	3
6	Assessments / Prüfungen durchführen mit Feststellungen	3
7	Feststellung erfassen	4
8	Massnahme erfassen	5
9	Massnahmen durchführen	6
10	Assessments weiterleiten	6
11	Prüfung abschliessen	7

### 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

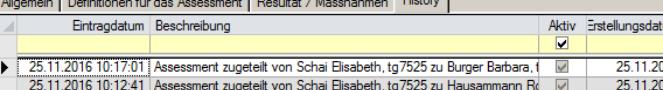
Nr.	Abbildung	Beschreibung
1.	<a href="#">Assessment-Management starten</a>	Anmeldung auf Prod-Umgebung
2.	Berechtigungsstufen	Unterschiedlich für Informationssicherheit und Assessment-Verantwortliche

### 3 Allgemeine Bearbeitungshinweise

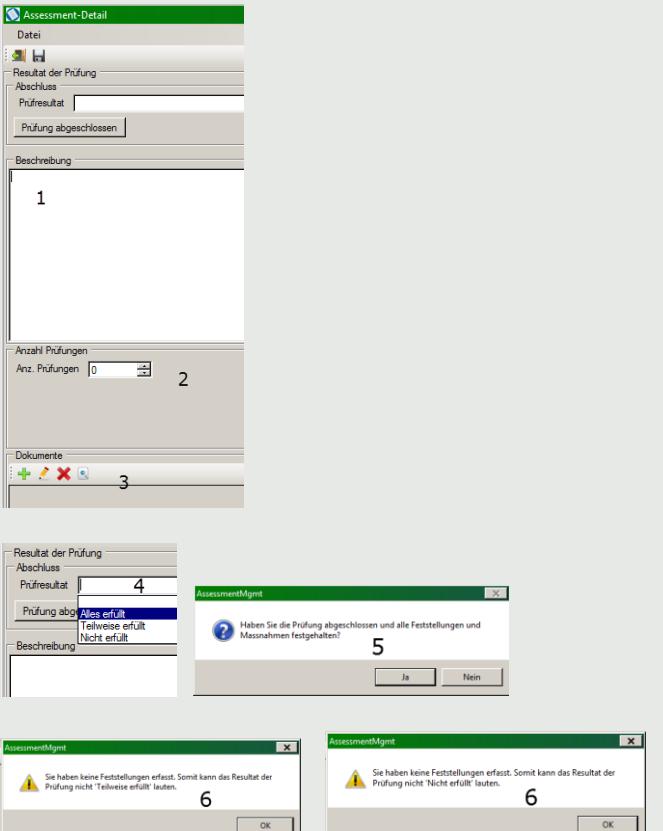
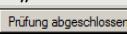
Nr.	Abbildung	Beschreibung
3.		Element (Feststellung, Massnahmen, Dokumente) - zufügen - bearbeiten - löschen - anzeigen
4.		Markiertes Element kann angezeigt, bearbeitet oder weitergeleitet werden
5.		Nur Anzeige möglich, z.B. weil Assessment bereits abgeschlossen ist

## 4 Assessment-Übersicht Allgemein

Nr.	Abbildung	Beschreibung
6.	<p>The screenshot shows the main interface of the Assessment Management system. On the left, there's a sidebar with navigation icons and a status bar. The main area has tabs: 'Allgemein', 'Definitionen für das Assessment', 'Resultat / Massnahmen', and 'History'. Below these tabs, there are sections for 'Verantwortlichkeiten' (Responsibilities) and 'Termine' (Deadlines). A small table at the bottom shows a single row with ID 180, description '14.2.4 Beschränkung', status 'Neu', responsible 'Schai Elisabeth', and due date '27.04.2017'.</p>	<b>Assessment</b> Übersicht über alle verantworteten Assessments - Bearbeitungsstati - Verantwortungen - Definitionen zum Assessment - erfasste Resultate und Massnahmen - History
7.	<p>This screenshot shows the 'General' tab of an assessment entry. It includes fields for 'Hauptverantwortung' (Main Responsibility), 'In Bearbeitung bei' (In Progress by), 'Kontrolle' (Control), 'Planung' (Planning), 'Termine' (Deadlines), and 'Zugewiesen' (Assigned). Below the form is a small table with one row showing ID 180, description '14.2.4 Beschränkung', status 'In Bearbeitung', responsible 'Schai Elisabeth', and progress 'Strähl Ralph'.</p>	<b>Allgemein</b> Hauptverantwortung: Bleibt immer beim Assessmentverantwortlichen, auch wenn Assessment zur Bearbeitung weitergegeben wird. Kontrolle/Planung zeigt die Verantwortlichkeit innerhalb der Informationssicherheit an.
8.	<p>This screenshot shows the 'Definitionen für das Assessment' tab. It contains sections for 'Bezeichnung' (Description), 'Beschreibung Kontrollaktivität' (Description Control Activity), 'Prüfgegenstand' (Subject of Audit), 'Hilfsmittel' (Tools), and 'Massnahmen bei Abweichung Ereignisse' (Measures in Case of Deviations Events). The 'Beschreibung Kontrollaktivität' section shows a detailed audit description.</p>	<b>Definitionen für das Assessment</b> - Beschreibung der Kontrollaktivität - Prüfgegenstand - Hilfsmittel - Massnahmen bei Abweichung
9.	<p>This screenshot shows the 'Vorgaben' tab. It contains sections for 'Vorgaben' (Requirements) and 'Bemerkungen' (Remarks). The 'Vorgaben' section lists requirements like 'ISO-Richtlinien \ 14 Anschaffung, Entwicklung und Instandhaltung' and 'FINMA-Vorgaben'. The 'Bemerkungen' section provides additional notes about software changes.</p>	<b>Vorgaben</b> Zeigt die regulatorischen oder gesetzlichen Vorgaben des Assessments an - ISO-Richtlinien - FINMA-Vorgaben - Vorgaben Datenschutzgesetz - weitere möglich inkl. deren genauen Bezeichnung und Beschreibung

Nr.	Abbildung	Beschreibung
10.		<b>Resultat/Massnahmen</b> Die erfassten Einträge werden angezeigt.
11.		<b>History</b> Nachverfolgung neue Zuteilung Assessments

## 5 Assessments / Prüfungen durchführen ohne Feststellung

Nr.	Abbildung	Beschreibung
12.		<b>Assessment durchführen</b> „Neu“ anwählen und Assessment-Detail mit  Prüfschritt bearbeiten oder mit Doppelklick öffnen
13.		<b>Assessments ohne Feststellung</b> 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  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.

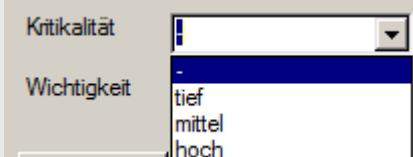
## 6 Assessments / Prüfungen durchführen mit Feststellungen

Nr.	Abbildung	Beschreibung
14.		<b>Assessment durchführen</b> „Neu“ anwählen und Assessment-Detail mit  Prüfschritt bearbeiten oder mit Doppelklick öffnen

Nr.	Abbildung	Beschreibung
15.		<p><b>Assessment-Detail – Übersicht</b></p> <p><b>Feststellung</b></p> <ol style="list-style-type: none"> <li>1 Dokumentieren gemäss Kap. 7</li> <li>2 Bezeichnung und Beschreibung wird übernommen</li> <li>3 Dokumente zu Feststellung zufügen</li> </ol> <p><b>Massnahmen</b></p> <ol style="list-style-type: none"> <li>4 beschreiben gemäss Kap.8</li> <li>5 Bezeichnung und Beschreibung wird übernommen</li> <li>6 Dokumente zu Massnahmen zufügen</li> </ol> <p><b>Resultat der Prüfung</b></p> <ol style="list-style-type: none"> <li>7 Prüfresultat gemäss Kap. 9</li> <li>8 Prüfresultat beschreiben</li> <li>9 Dokumente zu Prüfung zufügen, falls dies noch notwendig sein sollte.</li> <li>10 Prüfung abschliessen</li> </ol>

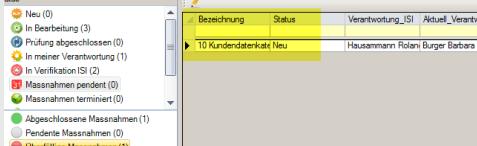
## 7 Feststellung erfassen

Nr.	Abbildung	Beschreibung
16.		<p>Bezeichnung: Kurzbeschreibung der Feststellung      Beschreibung: ausführliche Beschreibung wenn kein zusätzliches Dokument vorliegt</p> <p>Auswirkung, Kritikalität und Wichtigkeit der Feststellung differenziert bestimmen</p>
17.		<ul style="list-style-type: none"> <li>-  Keine Kritikalität</li> <li><b>Tief</b>  Die Feststellung ist nicht kritisch. z.B. Iconberechtigung nicht entfernt, in Applikation wurde Berechtigung gelöscht</li> <li><b>Mittel</b>  Die Feststellung betr. einzelne Dateien z.B. Daten mit CIDs sind allgemein einsehbar</li> <li><b>Hoch</b>  Es handelt sich um eine Feststellung in einer geschäftskritischen Applikation, mit</li> </ul>

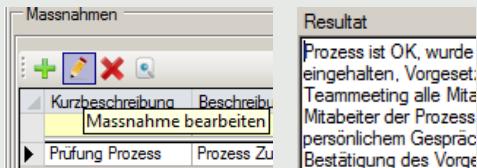
Nr.	Abbildung	Beschreibung
		einer hohen Bedrohungsstufe oder Cybervorfall
18.	<b>Wichtigkeit der Feststellung</b> 	<ul style="list-style-type: none"> <li>-  Wichtigkeit null</li> <li><b>Tief</b>  Die Feststellung ist nicht sehr wichtig. z.B. Korrektur einer Bezeichnung notwendig</li> <li><b>Mittel</b>  Schaden könnte fahrlässig entstehen (z.B. Notfalluser wurde nicht zurückgesetzt)</li> <li><b>Hoch</b>  Feststellung hat grosse Auswirkungen auf wichtige Geschäftsprozesse, z.B. E-Banking</li> </ul>
19.	<b>Auswirkung der Feststellung</b> 	<ul style="list-style-type: none"> <li>-  Keine Auswirkung</li> <li><b>Tief</b>  kleine Auswirkungen auf Sicherheit (z.B. Unklarheiten/Fragen in Provider-Reports)</li> <li><b>Mittel</b>  Informationssicherheit beeinträchtigt, (z.B. Benutzer hat falsche Berechtigungen)</li> <li><b>Hoch</b>  Informationssicherheit gefährdet (z.B. Datenverlust möglich, Risiko von Reputationsschaden)</li> </ul>
20.	<b>Gesamtbeurteilung</b>	<p>Beurteilung der Wichtigkeit und Kritikalität ergibt die Auswirkung.</p> <p>Ist die Auswirkung <b>hoch</b> muss die Informationssicherheit unmittelbar informiert werden.</p> <p>Bei Auswirkung <b>mittel</b> und <b>hoch</b> müssen Massnahmen definiert werden.</p>

## 8 Massnahme erfassen

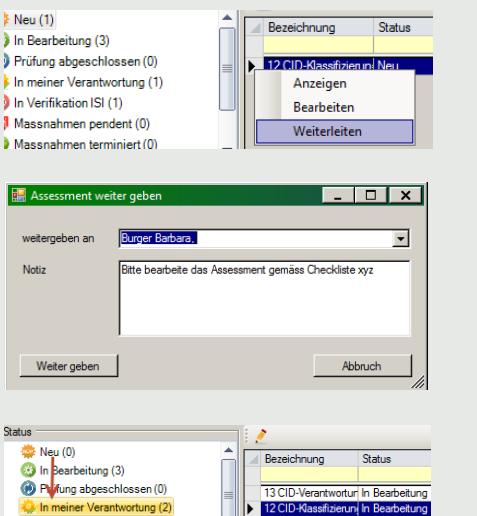
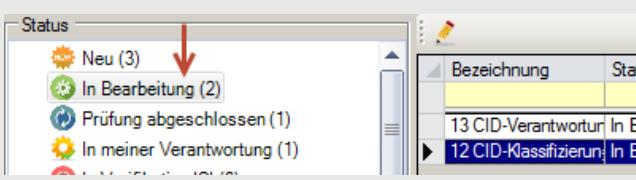
Nr.	Abbildung	Beschreibung
21.		<p><b>Massnahmen erfassen</b></p> <p>Massnahme definieren, terminieren und zuordnen.</p> <p>Sie kann selbst durchgeführt werden oder zur Durchführung weitergegeben werden.</p>

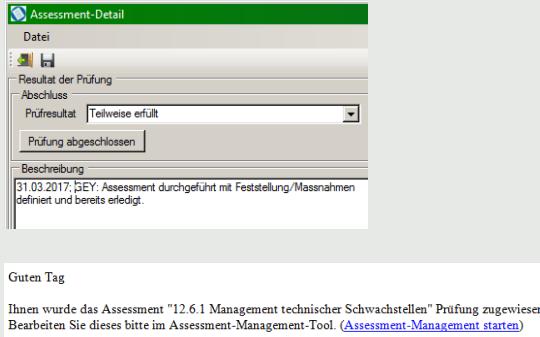
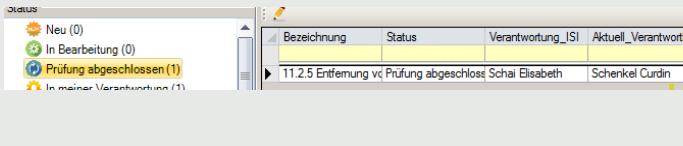
Nr.	Abbildung	Beschreibung
22.	Guten Tag Ihnen wurde vom Assessment "12.4.4 Zeitsynchronisation" die Massnahme "Massnahme 1" zur Bearbeitung zugewiesen. Bearbeiten Sie dieses bitte im Assessment-Management-Tool. ( <a href="#">Assessment-Management starten</a> )	Bei der Weiterleitung der Massnahme wird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

## 9 Massnahmen durchführen

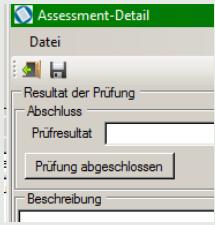
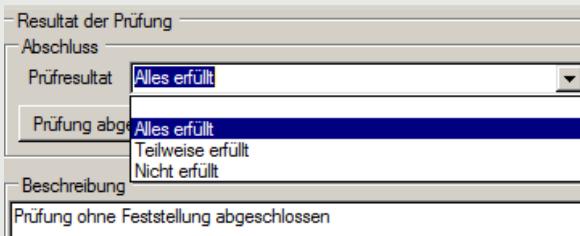
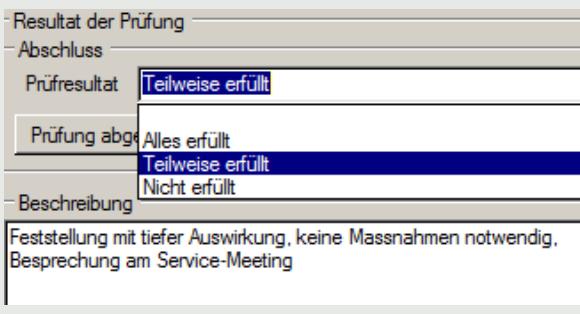
Nr.	Abbildung	Beschreibung
24.		Massnahme durchführen und Resultat im neu geöffneten Fenster beschreiben. <b>Dokumente</b> , die Erledigung der Massnahme bestätigen, zufügen, bei <b>Mittel</b> und <b>Hoch gewichteten</b> Feststellungen zwingend notwendig.
25.		Status-Anzeige: abgeschlossene Massnahmen

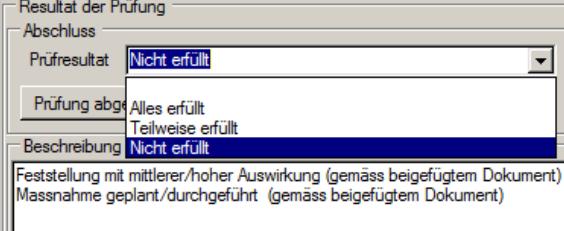
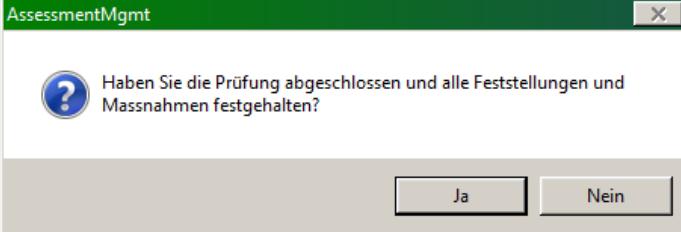
## 10 Assessments weiterleiten

Nr.	Abbildung	Beschreibung
26.		Ein Assessment kann einem Mitarbeitenden, Abteilungsleiter oder Vorgesetzten zur Bearbeitung weitergeleitet werden.  Bearbeiter auswählen weitergeben.  Bearbeiter wird mit Mail avisiert  <b>Hauptverantwortung</b> für Assessment <b>bleibt</b> 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.		<b>Abschluss</b> Keine Feststellung=Prüfresultat =Alles erfüllt <b>Beschreibung</b> z.B. Prüfung ohne Feststellung abgeschlossen, konkret beschreiben was, wann und wie geprüft wurde, keine Massnahmen notwendig
32.		<b>Abschluss</b> Prüfresultat = Feststellung „tiefe“ teilweise erfüllt (min. eine Feststellung muss erfasst werden) <b>Beschreibung</b> Konkrete Beschreibung der Feststellung „tiefe“, wenn ergänzende Dokumente vorhanden sind, reicht Kurzbeschreibung, üblicherweise keine Massnahmen erforderlich

Nr.	Abbildung	Beschreibung
33.	 <p>Resultat der Prüfung Abschluss Prüfresultat: Nicht erfüllt Prüfung abge: Alles erfüllt Teilweise erfüllt Beschreibung: Nicht erfüllt Feststellung mit mittlerer/hoher Auswirkung (gemäß beigefügtem Dokument) Massnahme geplant/durchgeführt (gemäß beigefügtem Dokument)</p>	<b>Abschluss</b> Feststellung mittel/hoch = nicht erfüllt immer Massnahmen notwendig
34.	 <p>AssessmentMgmt</p> <p>Haben Sie die Prüfung abgeschlossen und alle Feststellungen und Massnahmen festgehalten?</p> <p>Ja      Nein</p>	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.