NUR FÜR BEDARFSTRÄGER DES ÖFFENTLICHEN DIENSTES
DER BUNDESREPUBLIK DEUTSCHLAND

WEAKLESS

Rahmen - abrufvertrag

Durchführung von IT-Grundschutzchecks gemäß BSI-Standard 200-2

04. OKTOBER 2021

Inhaltsverzeichnis

1 Vertragsmotivation 4

2 Unsere Qualifikation 4

3 Vertrag 5

§ 1 Vertragsparteien 5

§ 2 Vertragsgegenstand 5

§ 3 Einräumung von Nutzungsrechten 6

§ 4 Entgeltlichkeit 6

§ 5 Haftung 7

§ 6 Datenschutzhinweise 7

§ 7 Wirksamkeitsklausel 7

4 Unsere Dienstleistung im Detail 8

6 Anmerkung 13

7 Unsere Preisgestaltung 14

ANHANG A 15

ANHANG B 16

ANHANG C 17

Dienstleistung

„Durchführung von IT-Grundschutzchecks gemäß BSI-Standard 200-2"

In Kraft getreten am 04. Oktober 2021, Laufzeit 12 Monate

Dienstleistungsnehmer:

Bedarfsträger im öffentlichen Dienst der Bundesrepublik Deutschland,
vertreten durch die

Initiative zur Selbsthilfe für Informationssicherheitsbeauftragte
in Bund, Ländern, Städten und Kommunen (www.plaza-web.de)

Dienstleistungsgeber:

Firma HPW Hagelberg GmbH
Sparte Informationssicherheitsberatung
Herr Dirk Hagelberg, Geschäftsführer
Innungstraße 5, 50354 Hürth

Registergericht:	Amtsgericht Köln, HRB 43719
Steuernummer:	224/5721/0356
UST-ID-Nr.:	DE258917549
Portfolio:	www.hpw-group.de

1 Vertragsmotivation

ist die allgemeine Kooperationsvereinbarung zwischen der

- Initiative zur Selbsthilfe für Informationssicherheitsbeauftragte in Bund, Ländern, Städten und Kommunen (www.plaza-web.de)
- und der Firma HPW GmbH (für Behörden siehe explizit: www.hpw-group.de).

Diese Vereinbarung beinhaltet diverse, gemeinsam entwickelte Unterstützungsmaßnahmen und Tools zum Auf- und Ausbau der Informationssicherheit in Bund, Ländern, Städten und Kommunen, u.a. die hier besprochene Dienstleistung.

2 Unsere Qualifikation

Das Tool WEAKLESS - eigens konzipiert zur strukturierten Durchführung von IT-Grundschutzchecks mit einer konsequente Nachverfolgung gefundener Schwachstellen (ToDo-Tracking) - ist eines unserer Produkte, die wir imAuftrag und in enger Zusammenarbeit mit der „Initiative zur Selbsthilfe der Informationssicherheitsbeauftragter in Bund, Ländern, Städten und Kommunen" entwickelt haben.

WEAKLESS orientiert sich demnach, vom Auftraggeber explizit so gefordert, eng an den Bedürfnissen der Zielgruppe und deren täglicher Basisarbeit. Daraus ergibt sich eine hohe Anwenderfreundlichkeit und eine Vielzahl an nützlichen Features, die von den Anwendern im Rahmen einer Evaluierung in den vergangenen 24 Monaten als Erweiterungen gewünscht wurden.

Wir setzen WEAKLESS selbst in mehreren Behörden im Rahmen von Dienstleistungen ein und haben uns dabei zunehmend auf die Durchführung von IT-Grundschutzchecks (GSCs) spezialisiert. Auch der zugrundeliegende IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist uns vertraut.

3 Vertrag

§ 1 Vertragsparteien

Dienstleistungsgeber:

ist der Hersteller und alleinige Rechteinhaber der Software WEAKLESS und ANUBIS, Herr Dirk Hagelberg, Geschäftsführer der Firma HPW GmbH, Innungstrasse 5 in 50354 Hürth.

Die HPW GmbH führt mehrere zielgruppen- und dienstleistungsorientiere Sparten, u.a. die Sparte „Strategie- und IT-Sicherheitsberatung", sowohl für den öffentlichen Dienst, als auch für Industrie und Handel in Deutschland.

Dienstleistungsnehmer:

ist der Nutzer als berechtigter, nachweislicher Bedarfsträger im öffentlichen Dienst der Bundesrepublik Deutschland.

§ 2 Vertragsgegenstand

Gegenstand des Vertrages ist die strukturierte Durchführung von IT-Grundschutzchecks gemäß BSI-Standard 200-2. Der dabei zugrunde gelegte Arbeitsprozess sowie die Übergabe der Endergebnisse werden im Kapitel 4 im Detail beschrieben und sind Basis dieser Dienstleistung.

§ 3 Einräumung von Nutzungsrechten

(1) Im Rahmen in § 2 beschriebenen Umfang und Verwendungszwecks räumt der Dienstleistungsgeber dem Dienstleistungsnehmer das Recht ein, die beauftragte Dienstleistung 24 Monate lang abzurufen.

(2) Die Übertragung dieses eingeräumten verlängertem Nutzungsrechts an Dritte ist nicht gestattet.

(3) Hat der Dienstleistungsnehmer in einem Rahmenabruf mehr Tagessätze beauftragt, als er letztendlich für die Durchführung seiner IT-Grundschutz-checks braucht, so wird ihm das Recht eingeräumt, diese beauftragten Tagessätze für andere Dienstleistungen des Auftraggebers nach inhaltlicher Absprache einzusetzen.

§ 4 Entgeltlichkeit

(1) Die Dienstleistung „Durchführung von IT-Grundschutzchecks" wird zu einem Tagessatz von 520,00 Euro netto erbracht.

(2) Jeder IT-Grundschutzcheck wird mit genau einem Tagessatz abrechnet.

(3) Zeitliche Mehraufwände gehen zu Lasten des Dienstleistungsgebers.

Diese Sonderkonditionen gelten ausschließlich nur für berechtigte Bedarfsträger gegen Nachweis. Diese Preisbindung gilt für alle Abrufe bis zum 01.10.2022.

Nachrichtlich:
Für alle anderen Bedarfsträger im In- und Ausland gelten bis zum 01.07.2022 die gleichen Abrufbedingungen, jedoch zu einem Tagessatz von 1.050 Euro netto.

§ 5 Haftung

(1) Der Dienstleistungsgeber verpflichtet sich zur absoluten Geheimhaltung der Informationen, die er im Rahmen der Durchführung von IT-Grundschutz-checks erfährt, verarbeitet und dokumentiert.

(2) Vorsorglich wird an dieser Stelle ausdrücklich darauf hingewiesen, dass bei der Durchführung von IT-Grundschutzchecks Übersichten von eventuell identifizierten IT-Schwachstellen des Dienstleistungsnehmers erzeugt werden.

(3) Somit erwächst für produzierte Ergebnisse und deren Speicherorte ein „höherer Schutzbedarf" gemäß der Definition der BSI-Standards 200-x. Beide Vertragspartner müssen daher für die Speicherung und Verarbeitung der erzielten Ergebnisse entsprechende Vorsichtsmaßnahmen ergreifen.

§ 6 Datenschutzhinweise

(1) Bei der Durchführung von IT-Grundschutzchecks werden KEINE personen-bezogene Daten im Sinne des Art. 4 Nr. 1 Datenschutzgrundverordnung (DSGVO) und Art. 9 Abs. 1 DSGVO zum Zwecke der Verarbeitung erhoben.

(2) Es gilt die Allgemeine Datenschutzerklärung des Lizenzgebers unter: http://www.werkzeug-einsatz-optimierung.de/datenschutzerklaerung

§ 7 Wirksamkeitsklausel

(1) Die Unwirksamkeit einer Bestimmung dieses Vertrages berührt den übrigen Vertragsinhalt nicht.

(2) Der Vertrag gilt in seiner jetzigen Form ab dem Datum seiner Inkraftsetzung (s. Seite 2).

4 Unsere Dienstleistung im Detail

Wie Sie unserer speziellen Webseite für Behörden **www.hpw-group.de** entnehmen können, unterstützen wir proaktiv die Umsetzung und den Ausbau des IT-Grundschutzes im öffentlichen Dienst.

Alle auf dieser Webseite angebotenen Produkte und Dienste wurden unter Mitwirkung von Behörden entwickelt und werden von uns, in speziell ausgehandelten Abrufverträgen festgehalten und zu einem erheblich reduzierten Preis an diese Nutzergruppe abgegeben.

So beläuft sich beispielsweise der Abgabepreis von WEAKLESS für alle Anwender aus dem öffentlichen Dienst auf 25% des Originalpreises, der für Anwender aus Industrie und Wirtschaft gilt.

Auch dieser Abrufvertrag beruht auf dieser Kooperation und einer speziellen Abruf-vereinbarung mit der „Initiative zur Selbsthilfe der Informationssicherheitsbeauftragten in Bund, Ländern, Städten und Kommunen".

Unsere Ausführungsstrategie

Um unserem eigenen Qualitätsanspruch gerecht werden zu können, haben wir uns bei der Durchführung von IT-Grundschutzchecks (GSCs) in der HPW-GROUP einen standardisierten Prozess auferlegt. Diese Vorgehensweise möchten wir Ihnen im Folgenden darlegen.

Schritt 1 - Terminabsprache und Vorbereitung

Mit den von Ihnen benannten Interviewpartner nehmen wir Kontakt auf und bieten wahlweise mehrere Audittermine an. Bei diesem ersten Kontakt erläutern wir den Inhalt und den Umfang des Audits und klären zweifelsfrei ab, ob unser Gesprächs-partner sich für diesen IT-Grundschutzcheck zuständig fühlt und auskunftsfähig ist.

Ansonsten werden von uns alternative Ansprechpartner erfragt und im Weiteren mit Ihnen abgestimmt. Der so ermittelte Interviewpartner erhält von uns eine spezielle Ausfertigung des zu besprechen Grundschuldschecks, mit der Bitte, sich einzulesen. In einer dafür vorgesehenen Spalte kann er sich bereits vor dem Interview eigene Notizen zum IST-Zustand machen. Hierzu nutzen wir in WEAKLESS den Menüpunkt „GSC to PDF" (siehe Anhang A, *1).

Schritt 2 -
Durchführung des GSCs (Istzustand aufnehmen)

Unmittelbar vor dem Interview wird der Auftraggeber von uns gebeten in seinem WEAKLESS (sofern vorhanden) den entsprechenden Baustein zu sperren (siehe Menüpunkt „CHECK-OUT" im Anhang A unter *3), um spätere Datenkollisionen und Eingabeverluste zu vermeiden.

Die IT-Grundschutzchecks werden von uns in Interviewform durchgeführt und sowohl online als auch vor Ort stattfinden. Aufgrund der aktuellen pandemischen Lage werden die IT-Grundschutzchecks grundsätzlich in Form von Video-Konferenzen, vorzugsweise und wann immer technisch verfügbar, über die sichere BDBOS-Meeting-Plattform des Bundes durchgeführt.

Dabei wird der Bildschirm geteilt, so dass alle Teilnehmer der Dokumentation des gemeinsam besprochenen Istzustand mitlesen können. Somit können Missverständnisse bereits beim Entstehen vermieden werden. Ist ein IT-Grundschutzcheck sehr umfangreich und überschreitet die Dauer von 2 Stunden, so wird aufgrund der sinkenden Konzentrationsfähigkeit ein Fortsetzungstermin vereinbart.

Fühlt sich der Interviewpartner nicht in der Lage eine konkrete Anforderung zu beantworten, wird wie folgend verfahren:

Option A:
Der Interviewpartner muss zuerst Hintergründeinformationen einholen, um seine Antworten geben zu können.

Unsere Vorgehensweise
Der Sachverhalt wird als Istzustand notiert. Erfolgt das Nachreichen der fehlenden Informationen nicht bis zum finalen Abschluss des IT-Grundschutzchecks, wird daraus ein Arbeitsauftrag (ToDo) gefertigt und diese Anforderung auf „nicht erfüllt" gesetzt (siehe Anhang B, *9).

Option B:
Der Interviewpartner fühlt sich für die Darstellung des IST-Zustandes dieser Anforderung nicht zuständig.

Unsere Vorgehensweise
Der Sachverhalt wird als Istzustand notiert. Wir nehmen im Nachgang zum GSC mit dem vom Interviewpartner alternativ genannten Ansprechpartner Kontakt auf um den fehlenden IST-Zustand zu ermitteln.

Schritt 3 -
Umsetzungsbewertung des SOLL-IST-Vergleiches

Unsere Vorgehensweise bei der Umsetzungsbewertung

Erläuterung zum Verständnis:

In Anlehnung an das „alte" IT-Grundschutztool des BSI bedeutet in WEAKLESS
- die Farbe Grün: „Diese Anforderung ist umgesetzt",
- die Farbe Gelb: „Diese Anforderung ist nur teilweise umgesetzt",
- die Farbe Rot: „Diese Anforderung ist nicht umgesetzt" und
- die Farbe Blau: „Diese Anforderung ist in unserem Hause nicht von Relevanz und daher entbehrlich".

Nach der Dokumentation des IST-Zustandes wird der Umsetzungsgrad dieses Zustandes gemeinsam diskutiert und eine vorläufige Bewertung festgelegt.
Dies erfolgt in WEAKLESS durch die Zuweisung einer der zuvor genannten Farben (siehe Anhang B, *9).

Schritt 4 -
ToDos erzeugen in WEAKLESS

Kann der Befragte den IST-Zustand einer Anforderung zweifelsfrei beschreiben und ist die SOLL-Anforderung des IT-Grundschutzes, gemessen an diesem IST-Zustand, nicht oder nur teilweise umgesetzt, so wird zum festgestellten Delta ein oder mehrere ToDos erstellt, die geeignet sind, dieses Delta zu beseitigen.

Entsprechend Ihrer Anforderung, wird der Auditor von WEAKLESS automatisch aufgefordert, sobald er die Farben Gelb oder Rot auswählt, ein ToDo zu erstellen (siehe Anhang C, *10). Dabei wird der Inhalt des ToDos, der Verantwortliche und ein realistischer Wiedervorlagetermin abgesprochen und in WEAKLESS dokumentiert " (siehe Anhang C, *11).

Wie geht es für Sie in WEAKLESS mit dem ToDo weiter?

Im Idealfall ist nach Ablauf des Wiedervorlagetermins das ToDo erledigt und kann auf „Grün" gesetzt werden. Ansonsten wird das weitere Vorgehen mit dem ToDo-Verantwortlichen besprochen und ein neuer Wiedervorlagetermin gesetzt.

Dies geschieht in WEAKLESS im Menü „TODO EDIT" (siehe Anhang A, *2).

Alle während der IT-Grundschutzchecks entstehenden ToDos werden in einer zentralen Liste in Ihrem WEAKLESS gesammelt und bei einer zeitlichen Überschreitung des Wiedervorlageermins farbig gekennzeichnet.

Schritt 5 - 1. QS-Stufe durch den Auditor nach dem Interview

In Abstimmung mit einem 2. Auditor werden die dokumentierten Ergebnisse diskutiert und sowohl inhaltlich als auch formal geschärft.

Schritt 6 - 2. QS-Stufe durch einen unbeteiligten sachkundigen Dritten

Die Dokumentation des IT-Grundschutzchecks wird von einem fachkundigen Dritten, der beim Interviwew bewusst nicht anwesend war, gegengelesen und bewertet. Dabei arbeitet dieser eine von der HPW-GROUP erstellte QS-Prüfliste ab und kommentiert Stellen, an denen er als außenstehender Leser Verständnis-probleme mit dem dokumentierten IST-Zustand hat. Beispielhaft sei hier eine unzureichend umfängliche Beantwortung der Anforderung genannt, Abkürzungen, die nicht zuvor erklärt wurden oder offengebliebene weitere Fragen.

Ist der QS-Prüfer einverstanden, setzt er den Prüfbutton „QS" in Zeile 37 auf „Grün" (siehe Anhang B, *8).

Hat der QS-Prüfer Beanstandungen, so notiert er seine konkreten Anmerkungen in WEAKLESS im Feld „Notizen" und setzt der Prüfbutton „QS" auf „Rot".

Schritt 7 - Bearbeitung der QS-Findings durch den Disponenten der HPW-GROUP

Nach der zweiten QS-Prüfung geht der IT-Grundschutzcheck-Auditbogen an den GSC-Disponenten der HPW-GROUP. Findet dieser im Auditbogen vom 2. QS-Prüfer nicht freigegebene IST-Zustände, leitet der GSC-Disponent den Auditbogen an den ursprünglichen Auditor zur Nachbesserung weiter. Hierzu nutzt der GSC-Disponent in WEAKLESS den Menüpunkt „GSC QS".

Dieser Prozess ist iterativ und erst abgeschlossen, wenn die beanstandete Stelle in GSC-Auditbogen vom 2. QS-Prüfer freigegeben wird.

Schritt 8 -
Freigabe des GC Bogens durch Interviewpartner

Als Nächstes erhält der Interviewpartner die Dokumentation des IT-Grundschutz-checks mit der Bitte um Freigabe. Dieser Schritt ist erfahrungsgemäß sinnvoll, um falsch verstandene Informationen frühzeitig zu erkennen und korrigieren zu können.

Schritt 9 -
Übergabe der Dokumentation des IT-Grundschutzchecks an den Auftraggeber

Nach der Freigabe des Auditbogens durch den Interviewpartner fertigt der GSC-Disponent zu diesem IT-Grundschutzcheck einen Abschlussbericht. Dieser beinhaltet die Dokumentation IT-Grundschutzcheck, Eine Liste der identifizierten Schwachstellen (nicht umgesetzte Anforderungen), eine Liste der vereinbarten ToDos sowie eine Berechnung des Umsetzungsgrades dieses IT-Grundschutzchecks.

Die Übergabe der Dokumentation des IT-Grundschutzchecks erfolgt in einem speziellen Dateiformat, das in das WEAKLESS des Auftraggebers „per Knopfdruck" importiert werden kann (siehe Menüpunkt „CHECK-IN", (Anhang A, *4).

Schritt 10 -
Freigabe des GC Bogens durch den Auftraggeber

Nachdem der Auftraggeber die Dokumentation des IT-Grundschutzchecks importiert und geprüft hat, wird er gebeten diesen IT-Grundcheck der HPW-GROUP gegenüber als „erfolgreich durchgeführt" freizugeben.

5 Projektabwicklung und -lieferungen

Eine von Ihnen erstellte Liste der gewünschten Bausteine kann von der HPW-GROUP in beliebiger Reihenfolge nach Ihren Vorgaben abgearbeitet werden. Die Lieferung der Dokumentation eines finalisierten IT-Grundschutzchecks erfolgt wahlweise per E-Mail oder Download in einer AES-256 verschlüsselten ZIP-Datei. Zu Beginn des Projektes wird mit Ihnen ein gemeinsamer Schlüssel separat ausgetauscht.

Wir schlagen zur Besprechung der Abwicklung und zu Details des gewünschten Projektverlaufs zu Anfang des Projektes ein kostenfreies Kick-Off-Meeting vor.

6 Anmerkung

Nach jedem Import und im Verlauf des gesamten Auftrages ist der Auftraggeber in der Lage, in seinem WEAKLESS durch den Aufruf des Menüpunktes „Statistik“ (s. Anhang A, *7) sich über den Fortschritt der IT-Grundschutzchecks und die Umsetzungsgrade der einzelnen Bausteine einen Überblick zu verschaffen.

Erfahrungsgemäß gibt es bei bestimmten Bausteinen mehrere Zielobjekte, deren IST-Zustände sich in Bezug auf die Umsetzung einzelnen Anforderungen stark voreinander unterscheiden und daher nicht in einem einzigen IT-Grundschutzcheck gemeinsam abgebildet werden können. Hier ist es ratsam den Baustein in mehrere IT-Grundschutzchecks aufzuteilen. Beispielhaft sei hier der Baustein „INF.1 Allgemeines Gebäude“ oder der Baustein „APP.4.3 Relationale Datenbanksysteme“.

Die dadurch eventuell zusätzlich benötigten IT-Grundschutzchecks bieten wir Ihnen zu den gleichen Konditionen an, wie die von Ihnen ursprünglich gewünschten IT-Grundchutzchecks.

7 Unsere Preisgestaltung

Die Tätigkeit eines IT-Grundschutz-Auditors bieten wir Ihnen im Rahmen einer von Ihnen benötigte IT-Sicherheitsdienstleistungen grundsätzlich zu einem Tagessatz von 520,00 Euro netto an.

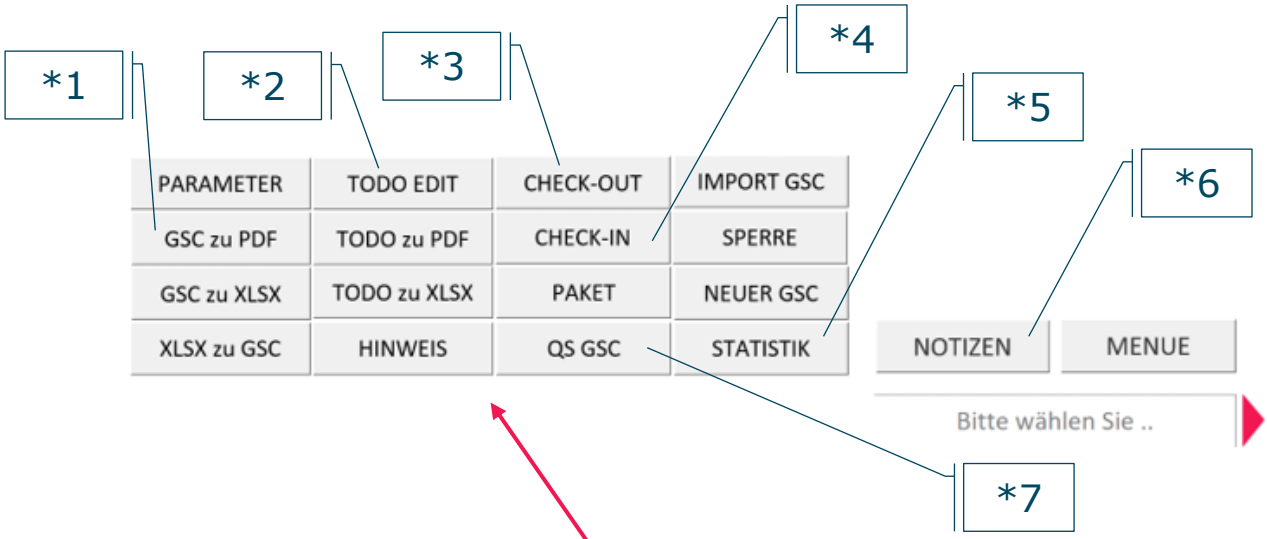
Um Ihnen eine finanzielle Planungssicherheit zu geben, sagen wir Ihnen verbindlich zu, unabhängig von unserem tatsächlichen zeitlichen Aufwand, für das Erstellen eines IT-Grundschutzchecks einen Tagessatz, also 520,00 Euro netto abzurechnen.

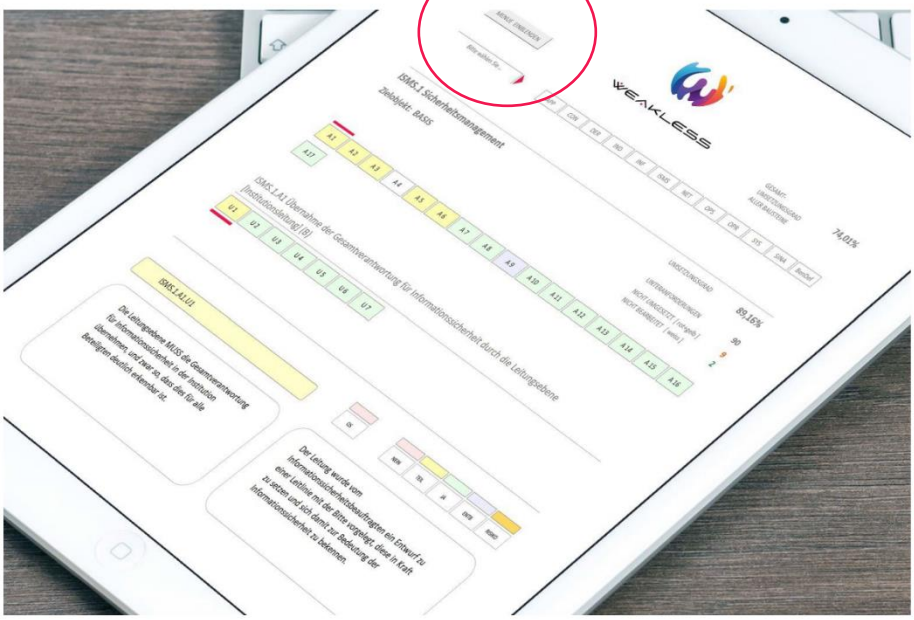
Sonstige, eventuell entstehende Kosten

Sollte es unvermeidlich oder von Ihnen ausdrücklich gewünscht sein, eine Besprechung vor Ort in Ihren Räumen durchzuführen, würden wir Ihnen eine Fahrkostenpauschale in Form einer Selbstkostenbeteiligung unseres Aufwandes in Höhe von 50,00 Euro netto je Termin anbieten.

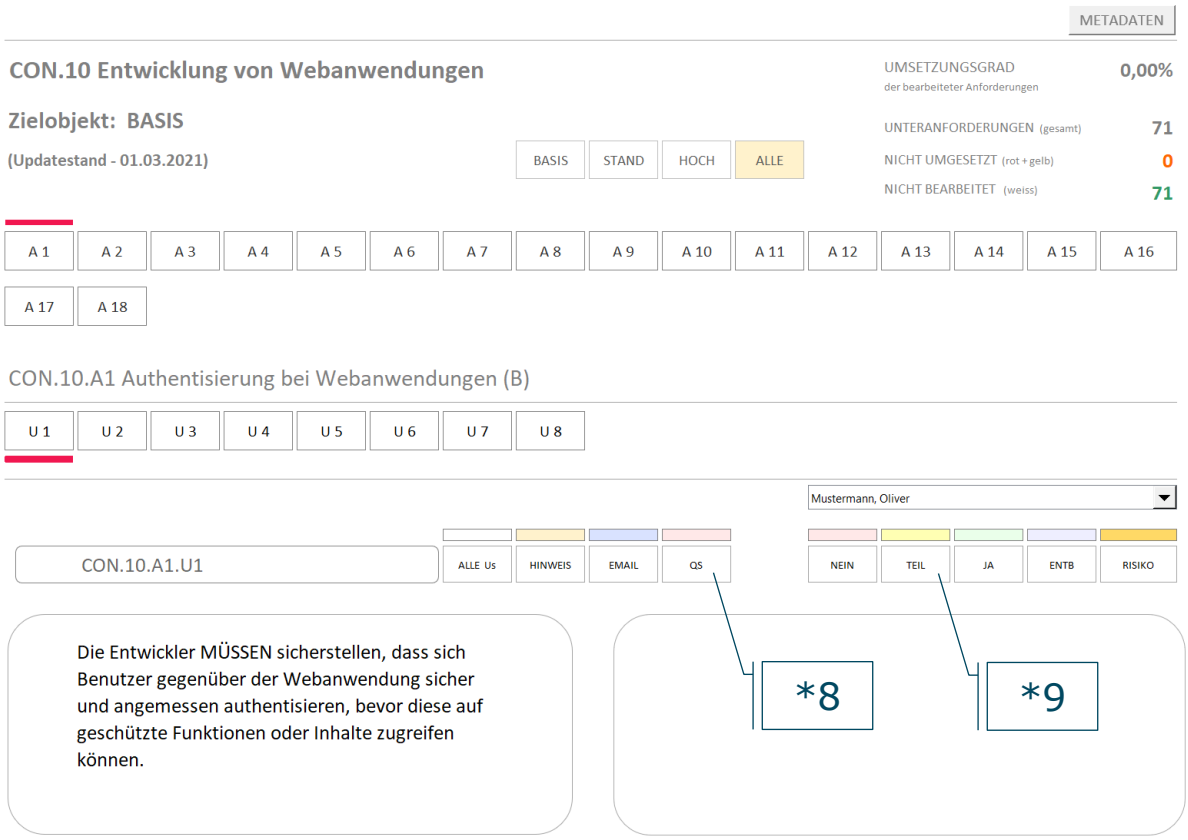
Wir gehen davon aus, dass es im Verlauf Auftrages keine Sachkosten geben wird.

ANHANG A

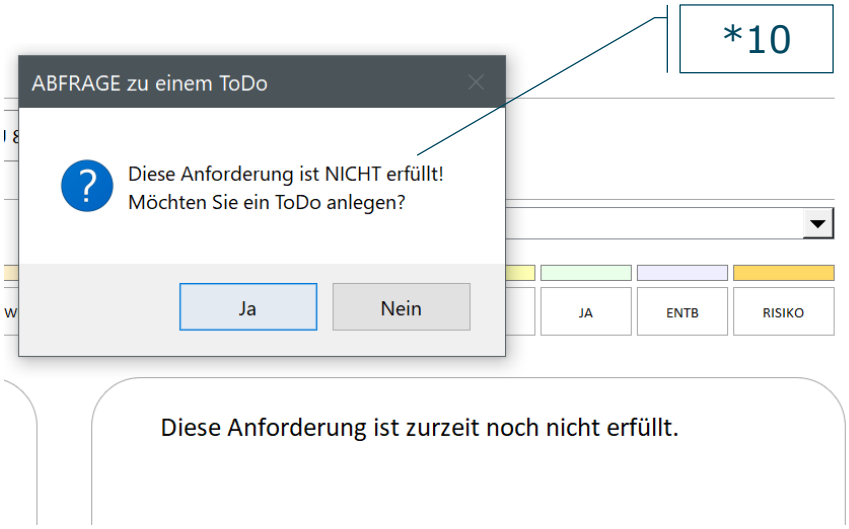

*1
*2
*3
*4
*5
*6
*7
PARAMETER
TODO EDIT
CHECK-OUT
IMPORT GSC
GSC zu PDF
TODO zu PDF
CHECK-IN
SPERRE
GSC zu XLSX
TODO zu XLSX
PAKET
NEUER GSC
XLSX zu GSC
HINWEIS
QS GSC
STATISTIK
NOTIZEN
MENUE
Bitte wählen Sie ..

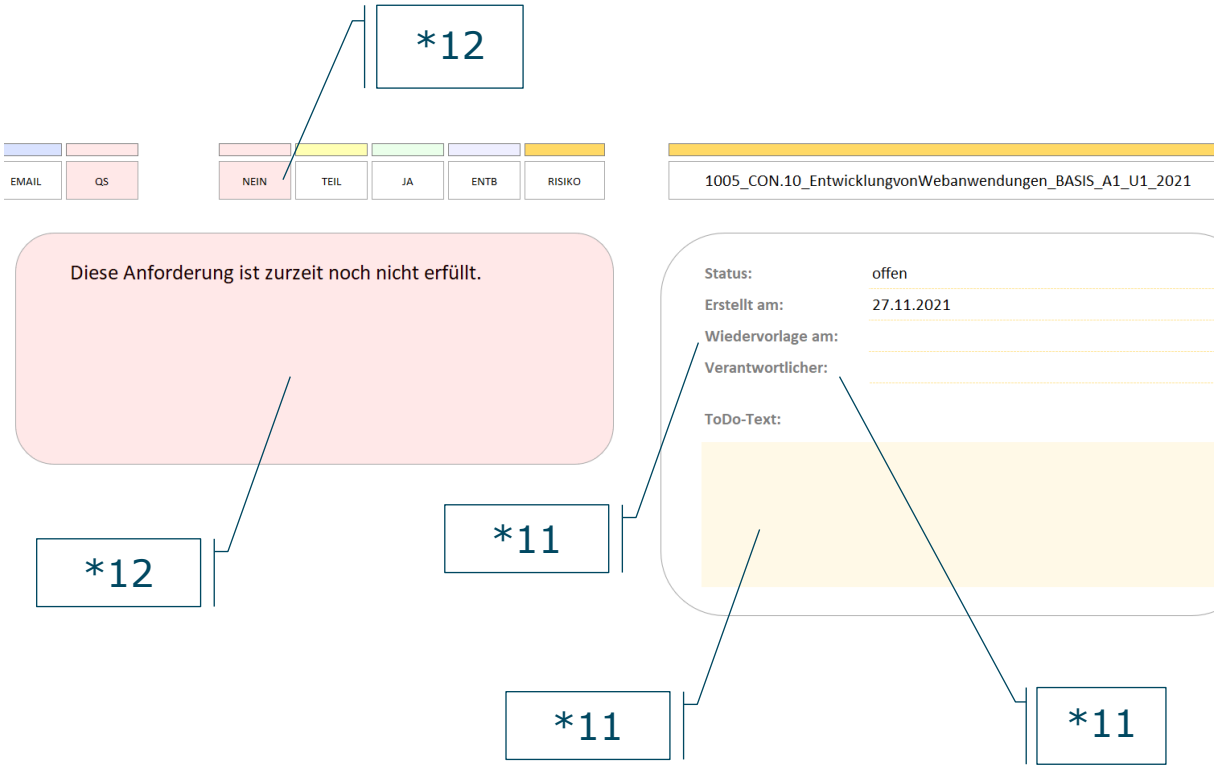


ANHANG B


METADATEN
CON.10 Entwicklung von Webanwendungen
Zielobjekt: BASIS
(Updatestand - 01.03.2021)
BASIS
STAND
HOCH
ALLE
UMSETZUNGSGRAD
der bearbeiteter Anforderungen
0,00%
UNTERANFORDERUNGEN (gesamt)
71
NICHT UMGESETZT (rot + gelb)
0
NICHT BEARBEITET (weiss)
71
A 1
A 2
A 3
A 4
A 5
A 6
A 7
A 8
A 9
A 10
A 11
A 12
A 13
A 14
A 15
A 16
A 17
A 18
CON.10.A1 Authentisierung bei Webanwendungen (B)
U 1
U 2
U 3
U 4
U 5
U 6
U 7
U 8
Mustermann, Oliver
CON.10.A1.U1
ALLE Us
HINWEIS
EMAIL
QS
NEIN
TEIL
JA
ENTB
RISIKO
Die Entwickler MÜSSEN sicherstellen, dass sich Benutzer gegenüber der Webanwendung sicher und angemessen authentisieren, bevor diese auf geschützte Funktionen oder Inhalte zugreifen können.
*8
*9

ANHANG C


*10
ABFRAGE zu einem ToDo
Diese Anforderung ist NICHT erfüllt!
Möchten Sie ein ToDo anlegen?
Ja
Nein
JA
ENTB
RISIKO
Diese Anforderung ist zurzeit noch nicht erfüllt.


*12
EMAIL
QS
NEIN
TEIL
JA
ENTB
RISIKO
1005_CON.10_EntwicklungvonWebanwendungen_BASIS_A1_U1_2021
Diese Anforderung ist zurzeit noch nicht erfüllt.
Status: offen
Erstellt am: 27.11.2021
Wiedervorlage am:
Verantwortlicher:
ToDo-Text:
*12
*11
*11
*11