System Assessment Bericht

bezogen auf elektronische Daten und elektronische Unterschriften;

Final Rule, 21 CFR Part 11

System: tiamo 2.0

1 Verfahren und Kontrollen für geschlossene Systeme

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.1	11.10 (a)	Validierung, IQ, OQ	Ist das System validiert?	**B**			Für die Validierung des Systems ist ausschliesslich der Betreiber verantwortlich. Die Verantwortung des Lieferanten liegt in der Bereitstellung validierfähiger Systeme. Dabei hilft das Metrohm-interne Qualitätswesen, welches jederzeit auditiert werden kann. Metrohm bietet diesbezüglich eine Reihe von Validierungs-Services an: Konformitätszertifikate, vorbereitete Unterlagen für IQ und OQ, Durchführung der IQ und OQ beim Betreiber,... Im System sind Standardmethoden für die Systemvalidierung gespeichert.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.2	11.10 (a)	Audit Trail, Änderung	Kann das System ungültige oder geänderte Aufzeichnungen erkennen?	**X**			Alle Bedienereingaben werden in einem automatisch generierten Audit Trail mit Datum, Uhrzeit mit Differenz zu UTC (Coordinated Universal Time) und Anwender dokumentiert. Diese Zeit ist die Client-Zeit, deshalb muss der Administrator dafür Sorge tragen, dass die Serverzeit auf den Client übertragen wurde. Der Report kann im Reportgenerator so definiert werden, dass geänderte Ergebnisdaten (Resultate) angezeigt werden. Bei Methodenänderung werden alle früheren Versionen in der Datenbank gespeichert und es muss ein Kommentar eingegeben werden. Methoden unterliegen einer Versionskontrolle. Das heisst, die geänderten Daten einer Methode führen zu einem neuen Eintrag (Version) in der Datenbank. Beim Ändern von Ergebnisdaten (Nachrechnen) werden alle früheren Versionen in der Datenbank gespeichert und es muss ein Kommentar eingegeben werden. Für Bestimmungen ist eine Versionskontrolle implementiert. Das heisst, die geänderten Daten führen zu einem neuen Eintrag in der Datenbank. Ungültige Resultate können dadurch erkannt werden, dass Grenzwerte definiert werden. Im System kann festgelegt werden, ob bei Überschreiten der Grenzen eine Meldung auf dem Bildschirm oder dem Report erscheint oder per e-mail gesendet wird. Zusätzlich kann definiert werden, ob die Bestimmung abgebrochen werden soll.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.3	11.10 (b)	Report, Ausdruck, elektronische Aufzeichnung	Kann das System genaue und vollständige Papierausdrucke der elektronischen Aufzeichnungen erstellen?	**X**			Für Bestimmungen (Ergebnisdaten) können konfigurierbare Reports gedruckt werden. Das Ändern der Report-Konfiguration kann für Routineanwender gesperrt werden. Der automatische Ausdruck am Ende einer Analyse kann im Methodenablauf definiert werden. Damit kann erreicht werden, dass der Betreiber des Systems mit Sicherheit vor dem Ändern, Überschreiben oder Löschen einer Bestimmung die Daten nachvollziehen kann. Jeder Ausdruck ist mit einem Zeitstempel mit Angabe der Differenz zu UTC versehen.
1.4	11.10 (b)	Report, elektronische Aufzeichnung, FDA	Kann das System genaue und vollständige Kopien der Aufzeichnungen in elektronischer Form zur Kontrolle, Überprüfung und Vervielfältigung durch die FDA erstellen?	**X**			Alle Daten können als verschlüsseltes XML-File abgespeichert werden und können mit Tiamo ausgewertet werden. Daten können als XML-, CSV- und SLK-Format exportiert werden. Über den Reportgenerator können alle Berichte im PDF-Format zur Verfügung gestellt werden. Der automatische Datenexport am Ende einer Analyse kann im Methodenablauf definiert werden. Damit kann erreicht werden, dass der Betreiber des Systems mit Sicherheit vor dem Ändern, Überschreiben oder Löschen einer Bestimmung die Daten nachvollziehen kann.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.5	11.10 (c)	elektronische Aufzeichnung, Aufbewahrungszeit, Archivierung	Sind die Aufzeichnungen während der ganzen Aufbewahrungszeit ohne weiteres wiederauffindbar?	**B**			Für die Aufbewahrung/Archivierung ist ausschliesslich der Betreiber verantwortlich. *tiamo* lässt sich als Local-Server oder Client-Version installieren. Das System kann Daten in der *tiamo*-Datenbank oder mittels Archivierungssystem auf dem PC oder auf einem Netzlaufwerk oder mittels Papier dauerhaft speichern. Die Datenbank besitzt eine automatische Backup-Funktion. Die Daten auf den Datenträgern werden verschlüsselt und mit einer Checksumme versehen. Sie sind so vor ungewollter und unsachgemässer Änderung geschützt. Änderungen werden vom System erkannt. Der Inhalt kann mit der *tiamo*-Software jederzeit gelesen werden. Das Verfahren, wie Daten archiviert werden und welche Daten das sind, muss der Betreiber festlegen. Schnittstellen zur Archivierung (XML-Files) sind im System vorhanden.
1.6	11.10 (d)	Login, Zugriffsschutz, Berechtigung Benutzer, Administrator	Ist der Systemzugriff auf berechtigte Personen beschränkt?	**X**			Die Software besitzt ein Login mit einer unbegrenzten Anzahl Profilen (Zugriffsrechten/ Personengruppen). Die Zugriffsrechte für die einzelnen Benutzergruppen können von Administratoren frei definiert werden. Die für das System verantwortlichen Personen (Administratoren) müssen sicherstellen, dass nur berechtigte Personen eine Zugangsberechtigung erhalten. Alle Änderungen an den Zugriffsrechten werden im Audit Trail aufgezeichnet.
1.7	11.10 (e)	Audit Trail, elektronische Aufzeichnung, Bedienereingaben	Besteht ein sicherer, rechnergenerierter, zeitgestempelter Audit Trail, der Datum und Zeit der Bedienereingaben und Aktionen protokolliert, welche elektronische Aufzeichnungen erstellen, ändern oder löschen?	**X**			Im Audit trail werden alle Bedienereingaben und Aktionen zu den elektronischen Daten mit Datum, Uhrzeit mit Differenz zu UTC und Anwender dokumentiert. Zusätzlich werden alle Änderungen an den Sicherheitseinstellungen, der Anwenderverwaltung und den Konfigurationsdaten im Audit Trail protokolliert.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.8	11.10 (e)	elektronische Aufzeichnung, Überschreiben von Daten, Änderung	Wenn elektronische Aufzeichnungen geändert werden, bleiben früher aufgezeichnete Informationen im System noch verfügbar (d.h. werden diese durch die Änderung nicht überschrieben)?	**X**			Ja, wenn Methoden oder Bestimmungsdaten verändert und gespeichert werden, wird automatisch eine neue Version erstellt.
1.9	11.10 (e)	Audit Trail, Aufbewahrungszeit	Bleibt der Audit Trail einer elektronischen Aufzeichnung während der ganzen Aufbewahrungszeit der Aufzeichnung wiederauffindbar?	**X**			So lange der Audit Trail nicht gelöscht wird, bleibt er bestehen. Der Speicherplatz ist hier der beschränkende Faktor. Der Audit Trail kann nur gelöscht werden, wenn er archiviert wurde. Der Audit trail wird als Textdatei mit einer Checksumme archiviert. Für die Aufbewahrung der archivierten Audit Trails ist ausschliesslich der Betreiber verantwortlich.
1.10	11.10 (e)	Audit Trail, FDA, Einsichtnahme	Ist der Audit Trail zur Überprüfung und Vervielfältigung durch die FDA verfügbar?	**X**			Der Audit trail kann als Textdatei mit einer Checksumme exportiert werden und ist so in elektronischer Form und auf Papier verfügbar. Über die Checksumme, kann die Integrität des Audit Trails verifiziert werden. Ausserdem kann eine schreibgeschützte pdf-Datei des Audit Trails erzeugt werden.
1.11	11.10 (f)	Sequenzialisierung, Ablauf, Plausibilitätsprüfung, Geräte	Wenn der Ablauf der Systemschritte oder Ereignisse wichtig ist, wird dieser durch das System erzwungen (z.B. wie es in einem Steuerungssystem der Fall wäre)?	**X**			Im System werden Plausibilitätsprüfungen schon beim Start der Bestimmung durchgeführt, so wird zum Beispiel überprüft, ob alle benötigten Geräte vorhanden sind. Der Ablauf der Bestimmung ist in der Methode programmiert und muss strikt eingehalten werden. Das Einhalten des Ablaufs wird durch die Verwendung der Probenzuordnungstabelle oder der automatischen Probedatenabfrage unterstützt. Es sind immer nur die Funktionen zugänglich, die ausgeführt werden können.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.12	11.10 (g)	Login, Zugriffsschutz, Berechtigung, Benutzer, Administrator	Stellt das System sicher, dass nur berechtigte Personen das System benutzen, Aufzeichnungen elektronisch visieren, auf die Funktion, die Rechnersystemeingabe- oder Ausgabeeinheit zugreifen, eine Aufzeichnung ändern oder andere Funktionen ausführen können?	**X**			Durch die Loginfunktion kann der Benutzer identifiziert werden. (Die für das System verantwortlichen Personen (Administratoren) müssen sicherstellen, dass nur berechtigte Personen eine Zugangsberechtigung erhalten.) Die Administratorfunktion kann von Benutzerrollen klar getrennt werden, siehe auch 11.10 (d), Nr. 1.6. Methoden und Bestimmungen können unterschrieben und somit elektronisch freigegeben werden. Es sind zwei Unterschriftsebenen eingerichtet. Das System fordert, dass Prüfer und Freigebender nicht die selbe Person ist.
1.13	11.10 (h)	Waage, Anschluss, Endgerät, Eingabedaten, Geräte	Kontrolliert das System die Gültigkeit der angeschlossenen Geräte? *Wenn die Systemanforderung besteht, dass Eingabedaten oder Befehle nur über gewisse Eingabegeräte (z.B. Endgeräte) eingehen können, kontrolliert dann das System die Gültigkeit der Quelle der erhaltenen Daten oder Befehle?* *(Hinweis: Gilt in Fällen, wo Daten oder Befehle über mehr als ein Gerät eingehen können, so dass das System die Integrität der Quelle, z.B. ein Netz von Waagen oder funkgesteuerte Fernendgeräte), überprüfen muss.*	**X**			Während der IQ werden alle angeschlossenen Geräte in die Geräteliste eingetragen und später geprüft. Metrohm-Geräte werden erkannt, auf Gültigkeit geprüft und automatisch in die Geräteliste eingetragen. Waage: Im System wird die Konfiguration der Waage gespeichert. Um zu kontrollieren, dass die korrekte Waage angeschlossen ist, obliegt es dem Betreiber, eine IQ nach einer Systeminstallation oder -änderung durchzuführen. Die erhaltenen Daten werden auf die korrekte Kennung und die Position des Gewichts in der Zeichenfolge geprüft. Die Validierung der angeschlossenen Geräte erfolgt im Rahmen der Systemvalidierung (siehe auch 11.10 (a), Nr. 1.1) durch den Betreiber.
1.14	11.10 (i)	Schulung, Support, Benutzer, Administrator	Gibt es dokumentierte Schulungen, einschliesslich Ausbildung am Arbeitsplatz (trainig on the job), für Systembenutzer, Entwickler, IT-Supportpersonal?	**X/B**			Für die Schulung der Anwender und Administratoren ist der Betreiber verantwortlich. Metrohm bietet Standard-Schulungen für alle Anwendungsbereiche an. Individuelle Trainings können gesondert vereinbart werden. Entwickler und Service-Personal der Metrohm werden regelmässig weitergebildet.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.15	11.10 (j)	Policy, Verantwortung, elektronische Unterschrift	Bestehen schriftliche Grundsätze (Policy), welche die Zuständigkeit und volle Verantwortung von Personen für Handlungen vorschreiben, die mit ihren elektronischen Unterschriften unternommen wurden?	**B**			Der Betreiber muss im Falle der Nutzung der elektronischen Unterschrift eine Policy haben, die die Gleichheit der handschriftlichen und der elektronischen Unterschrift klarstellt.
1.16	11.10 (k)	Dokumentation, Verteilung Dokumentation, Zugriff auf Dokumentation, Systemdokumentation, Logbuch, Gebrauchsanleitungen	Wird die Verteilung, der Zugriff auf sowie die Benutzung der Systembedienungs- und Wartungsdokumentation kontrolliert?	**B**			Das System besitzt eine umfangreiche Online-Hilfe, die den Benutzer und das Wartungspersonal unterstützt. Die Verteilung der papierbasierten Dokumentation liegt beim Betreiber.
1.17	11.10 (k)	SOP, Dokumentation, Gebrauchsanleitungen, Systemdokumentation, Audit Trail, Logbuch	Besteht ein formeller Änderungskontrollablauf für die Systemdokumentation, der einen Audit Trail der Änderungen mit Zeitablauf festhält?	**X/B**			Die Systemdokumentation ist eindeutig einem System und einer Softwareversion zugeordnet. Zu jeder Softwareversion werden Release Notes geführt. Der Betreiber muss jedoch ein Geräte-Logbuch führen und die Änderungen der Dokumentation und Software vermerken. Vorlagen für diese Dokumente werden von Metrohm zur Verfügung gestellt.

2 Zusätzliche Verfahren und Kontrollen für offene Systeme

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
2.1	11.30	Daten, Verschlüsselung, Datenübertragung	Können Methoden oder Bestimmungen sicher von einem System zum Nächsten übertragen werden? Sind Daten auf dem Weg vom Absender zum Empfänger verschlüsselt?	**N/A**			Ein Zugriff auf Tiamo über Internet ist nicht vorgesehen. Die Daten werden als Datei gespeichert, verschlüsselt und mit Prüfsumme versehen abgelegt. Die Daten sind somit vor unerlaubter Veränderung geschützt. Im Falle einer Änderung werden die Daten unbrauchbar. Auch wenn beschädigte Daten auf ein anderes System übertragen werden, wird dies erkannt.
2.2	11.30	elektronische Unterschrift	Werden digitale Unterschriften verwendet?	**N/A**			Ein Zugriff auf Tiamo über Internet ist nicht vorgesehen. Methoden und Bestimmungen können unterschrieben und somit elektronisch freigegeben werden. Es sind zwei Unterschriftsebenen eingerichtet. Das System fordert, dass Prüfer und Freigebender nicht die selbe Person ist.

3 Unterschriebene elektronische Daten

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
3.1	11.50	elektronische Unterschrift	Enthalten unterschriebene elektronische Aufzeichnungen die folgenden verwandten Informationen? - vollständiger Name des Unterzeichners - Datum und Zeit der Unterschrift - Bedeutung der Unterschrift (wie Genehmigung, Überprüfung, Verantwortung)	**X**			Bei Methoden und Bestimmungen enthalten alle Unterschriften den vollständigen Namen des Unterschreibenden, das Datum und die Uhrzeit zum Zeitpunkt der Unterschrift, und die Begründung (aus Auswahlliste) für die Unterschrift. Zusätzlich kann zu einer Unterschrift ein Kommentar eingegeben werden, der zusammen mit der digitalen Unterschrift abgespeichert wird. Benutzerdaten und Audit Trail sind keine unterschriftspflichtigen Daten und werden somit nicht unterschrieben.
3.2	11.50	elektronische Unterschrift	Erscheint die oben erwähnte Information in angezeigten und gedruckten Kopien der elektronischen Aufzeichnung?	**X**			Bei der Anzeige im Display und auf Ausdrucken werden die kompletten Unterschriftsdaten ausgegeben.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
3.3	11.70	elektronische Unterschrift	Besteht eine Verbindung zwischen den Unterschriften und den entsprechenden elektronischen Aufzeichnungen, um sicherzustellen, dass sie nicht mit gewöhnlichen Mitteln zu Fälschungszwecken ausgeschnitten, kopiert oder sonst übertragen werden können?	**X**			Die Unterschrift ist untrennbar mit der Methode oder der Bestimmung verbunden. Fälschungen sind hierbei nicht möglich. In die Unterschrift werden die Benutzerinformationen komplett übernommen. Diese sind bei der Darstellung der Unterschrift dann immer in Klartext lesbar!

4 Elektronische Unterschriften (allgemein)

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
4.1	11.100 (a)	elektronische Unterschrift	Sind elektronische Unterschriften eindeutig einer Person zugeordnet?	**X**			Ja durch eindeutige Beziehung zwischen Anmeldename und Person im System. Betrieblich ist sicherzustellen, dass keine Mehrfachverwendung von Anmeldenamen stattfindet (das System überwacht die Eindeutigkeit des Anmeldenamens).
4.2	11.100 (a)	elektronische Unterschrift	Werden elektronische Unterschriften je durch andere Personen wiederverwendet oder anderen Personen zugeteilt?	**B**			Ein verwendeter Anmeldename ist einer Person zugeordnet. Es ist betrieblich sicherzustellen, dass dieser Anmeldename nicht einer anderen Person zugeordnet wird. Eine Reaktivierung bleibt davon unberührt.
4.3	11.100 (a)	elektronische Unterschrift	Erlaubt das System die Übertragung der Berechtigung von elektronischen Unterschriften (Stellvertreterregelung)?	**B**			Die Zuordnung von Stellvertretern ist durch den Administrator durchzuführen. Betriebliche Regelung ist hier notwendig.
4.4	11.100 (b)	elektronische Unterschrift	Wird die Identität einer Person vor der Zuteilung einer elektronischen Unterschrift überprüft?	**B**			Der organisatorische Prozess des Berechtigungsantrags muss sicherstellen, dass die beantragende Person die korrekte Person ist.

5 Elektronische Unterschriften (nicht-biometrisch)

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
5.1	11.200 (a) (1)(i)	elektronische Unterschrift	Besteht die Unterschrift aus mindestens zwei Elementen, wie Identifikationscode (z.B. Benutzername) und Passwort oder Identifikationskarte und Passwort?	**X**			Ja (Anmeldename und Passwort).
5.2	11.200 (a) (1)(ii)	elektronische Unterschrift	Wird das Passwort bei jeder Unterschrift verlangt, wenn mehrere Unterschriften im Laufe einer durchgehenden Sitzung angebracht werden? (Hinweis: beide Elemente müssen bei der ersten Unterschrift einer Sitzung angegeben werden)	**X**			Zu jeder Unterschrift muss das Passwort eingegeben werden.
5.3	11.200 (a) (1)(iii)	elektronische Unterschrift	Werden immer beide Elemente der elektronischen Unterschrift verlangt, wenn Unterschriften nicht während einer durchgehenden Arbeitssitzung angebracht werden?	**X**			Zu jeder Unterschrift muss der Anmeldename und das Passwort eingegeben werden.
5.4	11.200 (a) (2)	elektronische Unterschrift	Werden nichtbiometrische Unterschriften ausschliesslich durch ihre tatsächlichen Eigentümer verwendet?	**B**			Der Betreiber muss sicherstellen, dass jeder Anwender nur seine eigene Unterschrift verwendet.
5.5	11.200 (a) (3)	elektronische Unterschrift, el. Unterschrift fälschen	Benötigt ein Versuch, eine elektronische Unterschrift zu fälschen, das Zusammenwirken von mindestens zwei Personen?	**X**			Ja (die Daten in der Datenbank sind in einem nicht durch den Menschen lesbares Format codiert).

6 Elektronische Unterschriften (biometrisch)

lfd. Nr.	Ref.		Frage	Ja	Nein	zum Teil	Bemerkungen
6.1	11.200 (b)	elektronische Unterschrift, biometrische el. Unterschrift	Ist es erwiesen, dass biometrische elektronische Unterschriften ausschliesslich durch ihren tatsächlichen Eigentümer verwendet werden können?	**N/A**			Keine biometrische Unterschrift.

7 Kontrolle von Identifikationscode und Passwort

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
7.1	11.300 (a)	Identifikationscode, Eindeutigkeit, Passwort, Identifikation, Login, Zugriffsschutz	Bestehen Kontrollen, um die Einmaligkeit jeder Kombination von Identifikationscode und Passwort sicherzustellen, so dass keine Person die gleiche Kombination von Identifikationscode und Passwort haben kann?	**X/ B**			Das System stellt sicher, dass jeder Identifikationscode (Anwendername) nur einmal innerhalb des Systems verwendet wird, so kann auch eine Kombination von Identifikationscode und Passwort nur einmal vorkommen. Namensänderungen müssen vom Betreiber organisatorisch verwaltet werden! Das System kann als Client-Server-System betrieben werden. Dadurch ist sichergestellt, dass die Identifikationscodes in allen Clients identisch sind. Es wird empfohlen, unternehmensweit eindeutige systemübergreifende Identifikationscodes (z.B. Personalnummer oder Namenskürzel) zu verwenden. Generell wird empfohlen, organisationsweit Richtlinien festzulegen, in denen die Erstellung von Anwenderkonten und die Verwendung von Passwörtern (Länge, Gültigkeitsdauer,...) festgelegt wird.
7.2	11.300 (b)	Identifikationscode, Passwort, Gültigkeit, Identifikation, Login, Zugriffsschutz	Sind Verfahren vorgeschrieben, um sicherzustellen, dass die Gültigkeit der Identifikationscodes periodisch überprüft wird?	**B**			Für die Überprüfung der Identifikationscodes ist der Betreiber verantwortlich.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
7.3	11.300 (b)	Passwort, Gültigkeit, Verfall Passwort, Identifikation, Login, Zugriffsschutz	Unterstehen Passwörter dem periodischen Verfall, damit sie regelmässig geändert werden müssen?	**X**			Die Gültigkeitsdauer für das Passwort kann vom Administrator festgelegt werden. Werte zwischen 30 und 90 Tagen sind gebräuchlich. Eine lange Gültigkeitsdauer stellt ein Sicherheitsrisiko dar. Eine zu kurze Gültigkeitsdauer bedeutet, dass sich Anwender häufig ein neues Passwort merken müssen und dieses eventuell aufschreiben. Das System speichert die Passworthistorie, somit ist eine Wiederverwendung von Passwörtern nicht möglich.
7.4	11.300 (b)	Identifikationscode, Passwort, Gültigkeit, Sperrung Zugangsberechtigung, Identifikation, Login, Zugriffsschutz	Besteht ein Verfahren für den Rückruf oder die Sperrung von Identifikationscodes und Passwörtern, wenn eine Person austritt oder den Arbeitsplatz wechselt?	**B**			Das Verfahren muss vom Betreiber festgelegt werden. Der entsprechende Benutzer kann im System vom Administrator entfernt werden, bleibt jedoch im System in der Gruppe „entfernte Anwender“ ohne jegliche Zugriffsrechte gespeichert.
7.5	11.300 (c)	Identifikationscode, Passwort, Gültigkeit, Sperrung Zugangsberechtigung, Identifikation, Login, Zugriffsschutz, Verlust ID-Karte	Besteht ein Verfahren zur elektronischen Sperrung eines Identifikationscodes oder Passwortes, wenn es möglicherweise unsicher oder verloren gegangen ist?	**B**			Das Verfahren muss vom Betreiber festgelegt werden. Der entsprechende Benutzer kann im System vom Administrator entfernt werden, bleibt jedoch im System in der Gruppe „entfernte Anwender“ ohne jegliche Zugriffsrechte gespeichert.
7.6	11.300 (d)	Missbrauch, Login, Zugriffsschutz	Besteht ein Verfahren zur Erkennung von Missbrauchsversuchen und Benachrichtigung der Sicherheitsstelle?	**X**			Nach n-maligen Fehlversuchen (Anzahl kann vom Administrator definiert werden) wird eine Meldung, dass die maximale Anzahl erfolgloser Login-Versuche erreicht wurde, ausgegeben und der Benutzer gesperrt. Eine entsprechende Mitteilung kann per E-mail an das Management verschickt werden.
7.7	11.300 (d)	Missbrauch, Login, Zugriffsschutz	Besteht ein Verfahren zur Meldung an das Management von wiederholten oder schwerwiegenden Missbrauchsversuchen?	**B**			Ein Verfahren zur Meldung an das Management muss vom Betreiber festgelegt werden. Nach n-maligen Fehlversuchen wird eine Meldung, dass die maximale Anzahl erfolgloser Login-Versuche erreicht wurde, ausgegeben und der Benutzer gesperrt. Eine entsprechende Mitteilung kann per E-mail an das Management verschickt werden.
7.8	11.300 (c)	Verlust ID-Karte, ID-Karte, Missbrauch, Zugriffsschutz	Besteht ein Verlustbearbeitungsverfahren, falls ein Gegenstand zur Identifikation (z.B. ID-Karte) verloren geht oder gestohlen wird?	**N/A**			Eine Hardware zur Identifikation ist nicht vorgesehen.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
7.9	11.300 (c)	Verlust ID-Karte, elektronische Sperrung ID-Karte, ID-Karte, Missbrauch, Zugriffsschutz	Besteht ein Verfahren zur elektronischen Sperrung eines solchen Gegenstandes, falls er verloren, gestohlen oder möglicherweise unsicher ist?	**N/A**			Eine Hardware zur Identifikation ist nicht vorgesehen.
7.10	11.300 (c)	ID-Karte, Zugriffsschutz	Bestehen Kontrollen über die Ausgabe von temporären und festen Ersatzgeräten?	**N/A**			Eine Hardware zur Identifikation ist nicht vorgesehen.
7.11	11.300 (e)	Überprüfung ID-Karte, ID-Karte, Zugriffsschutz	Werden Identifikationsmarken und Karten am Anfang und danach periodisch überprüft?	**N/A**			Eine Hardware zur Identifikation ist nicht vorgesehen.
7.12	11.300 (e)	Änderung ID-Karte, ID-Karte, Missbrauch, Zugriffsschutz	Beinhaltet diese Prüfung auch eine Kontrolle, dass keine unerlaubten Änderungen vorgenommen wurden?	**N/A**			Eine Hardware zur Identifikation ist nicht vorgesehen.

B = Die Verantwortung liegt beim Betreiber.
N/A = Trifft auf das System nicht zu (not applicable)

8 Indices

Verweise auf die Seitenzahl:

A

Ablauf 6
Administrator 5, 7
Änderung 3, 6
Änderung ID-Karte 14
Anschluss 7
Archivierung 5
Audit Trail 3, 5, 6, 8
Aufbewahrungszeit 5, 6
Ausdruck 4

B

Bedienereingaben 5
Benutzer 5, 7
Berechtigung 5, 7
biometrische el. Unterschrift 12

D

Daten 9
Datenübertragung 9
Dokumentation 8

E

Eindeutigkeit 12
Eingabedaten 7
Einsichtnahme 6
el. Unterschrift fälschen 11
elektronische Aufzeichnung 4, 5, 6
elektronische Sperrung ID-Karte 14
elektronische Unterschrift 8, 9, 10, 11, 12
Endgerät 7

F

FDA 4, 6

G

Gebrauchsanleitungen 8
Geräte 6, 7
Gültigkeit 12, 13

I

Identifikation 12, 13
Identifikationscode 12, 13
ID-Karte 13, 14
IQ 2

L

Logbuch 8
Login 5, 7, 12, 13

M

Missbrauch 13, 14

O

OQ 2

P

Passwort 12, 13
Plausibilitätsprüfung 6
Policy 8

R

Report 4

S

Schulung 7
Sequenzialisierung 6
SOP 8
Sperrung Zugangsberechtigung 13
Support 7
Systemdokumentation 8

U

Überprüfung ID-Karte 14
Überschreiben von Daten 6

V

Validierung 2
Verantwortung 8
Verfall Passwort 13
Verlust ID-Karte 13, 14
Verschlüsselung 9
Verteilung Dokumentation 8

W

Waage 7

Z

Zugriff auf Dokumentation 8
Zugriffsschutz 5, 7, 12, 13, 14

Verweise auf die laufende Nummer des Tabelleneintrags:

A

Ablauf 1.11
Administrator 1.14, 1.12, 1.6
Änderung 1.8, 1.2
Änderung ID-Karte 7.12
Anschluss 1.13
Archivierung 1.5
Audit Trail 1.17, 1.10, 1.9, 1.7, 1.2
Aufbewahrungszeit 1.9, 1.5
Ausdruck 1.3

B

Bedienereingaben 1.7
Benutzer 1.14, 1.12, 1.6
Berechtigung 1.12, 1.6
biometrische el. Unterschrift 6.1

D

Daten 2.1
Datenübertragung 2.1
Dokumentation 1.17, 1.16

E

Eindeutigkeit 7.1
Eingabedaten 1.13
Einsichtnahme 1.10
el. Unterschrift fälschen 5.5
elektronische Aufzeichnung 1.8, 1.7, 1.5, 1.4, 1.3
elektronische Sperrung ID-Karte 7.9
elektronische Unterschrift 6.1, 5.5, 5.4, 5.3, 5.2, 5.1, 4.4, 4.3, 4.2, 4.1, 3.3, 3.2, 3.1, 2.2, 1.15
Endgerät 1.13

F

FDA 1.10, 1.4

G

Gebrauchsanleitungen 1.17, 1.16
Geräte 1.13, 1.11
Gültigkeit 7.5, 7.4, 7.3, 7.2

I

Identifikation 7.5, 7.4, 7.3, 7.2, 7.1
Identifikationscode 7.5, 7.4, 7.2, 7.1
ID-Karte 7.12, 7.11, 7.10, 7.9, 7.8
IQ 1.1

L

Logbuch 1.17, 1.16
Login 7.7, 7.6, 7.5, 7.4, 7.3, 7.2, 7.1, 1.12, 1.6

M

Missbrauch 7.12, 7.9, 7.8, 7.7, 7.6

O

OQ 1.1

P

Passwort 7.5, 7.4, 7.3, 7.2, 7.1
Plausibilitätsprüfung 1.11
Policy 1.15

R

Report 1.4, 1.3

S

Schulung 1.14
Sequenzialisierung 1.11
SOP 1.17
Sperrung Zugangsberechtigung 7.5, 7.4
Support 1.14
Systemdokumentation 1.17, 1.16

U

Überprüfung ID-Karte 7.11
Überschreiben von Daten 1.8

V

Validierung 1.1
Verantwortung 1.15
Verfall Passwort 7.3
Verlust ID-Karte 7.9, 7.8, 7.5
Verschlüsselung 2.1
Verteilung Dokumentation 1.16

W

Waage 1.13

Z

Zugriff auf Dokumentation 1.16
Zugriffsschutz ... 7.12, 7.11, 7.10, 7.9, 7.8, 7.7, 7.6, 7.5, 7.4, 7.3, 7.2, 7.1, 1.12, 1.6