

System Assessment Bericht
bezogen auf elektronische Daten und elektronische Unterschriften;
21 CFR Part 11

System: *tiamo*
(Software Version 3.0)

1 Verfahren und Kontrollen für geschlossene Systeme

| Ifd. Nr. | Ref. | Thema | Frage | Ja | Nein | Bemerkungen |
|----------|---------------------------|---------------------|---------------------------|----------|------|--|
| 1.1 | 11.10 (a) | Validierung, IQ, OQ | Ist das System validiert? | B | | <p>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.</p> <p>Metrohm bietet diesbezüglich eine Reihe von Validierungs-Services an: Konformitätszertifikate, vorbereitete Unterlagen für IQ und OQ, Durchführung der IQ und OQ beim Betreiber, ...</p> <p>Im System sind Standardmethoden für die Systemvalidierung gespeichert.</p> |

| Ifd. Nr. | Ref. | Thema | Frage | Ja | Nein | Bemerkungen |
|----------|---------------------------|--|---|----------|------|---|
| 1.2 | 11.10 (a) | Audit Trail, Änderung | Kann das System ungültige oder geänderte Aufzeichnungen erkennen? | X | | <p>Alle relevanten 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 Systemzeit des Clients verlässlich ist (bspw. indem die Systemuhren der angeschlossenen Clients mit einem Zeitserver synchronisiert sind).</p> <p>Der Report kann im Reportgenerator so definiert werden, dass geänderte Ergebnisdaten (Resultate) angezeigt werden.</p> <p>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.</p> <p>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.</p> <p>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.</p> |
| 1.3 | 11.10 (b) | Report, Ausdruck, elektronische Aufzeichnung | Kann das System einen genauen und vollständigen Papiausdruck der elektronischen Aufzeichnungen erstellen? | X | | <p>Für Bestimmungen (Ergebnisdaten) können konfigurierbare Reports gedruckt werden. Das Ändern der Report-Konfiguration kann für Routineanwender gesperrt werden.</p> <p>Der automatische Ausdruck am Ende einer Analyse kann in der Methode 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.</p> <p>Jeder Ausdruck ist mit einem Zeitstempel mit Angabe der Differenz zu UTC versehen.</p> |

| Ifd. Nr. | Ref. | Thema | Frage | Ja | Nein | Bemerkungen |
|----------|---------------------------|---|---|----------|------|---|
| 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 | | <p>Alle Daten können als verschlüsseltes XML-File abgespeichert werden und können mit <i>Tiamo</i> ausgewertet werden.</p> <p>Daten können in das XML-, CSV- und SLK-Format exportiert werden.</p> <p>Über den Reportgenerator können alle Berichte im PDF-Format zur Verfügung gestellt werden.</p> <p>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.</p> |
| 1.5 | 11.10 (c) | Elektronische Aufzeichnung, Aufbewahrungszeit, Archivierung | Sind die Aufzeichnungen während der ganzen Aufbewahrungszeit ohne weiteres wiederauffindbar? | B | | <p>Für die Aufbewahrung/Archivierung ist ausschliesslich der Betreiber verantwortlich.</p> <p><i>tiamo</i> lässt sich als Local-Server oder Client-Version installieren. Das System kann Daten in der <i>tiamo</i>-Datenbank oder mittels Archivierungssystem auf dem PC, oder auf einem Netzlaufwerk, oder durch Ausdrucken auf Papier dauerhaft speichern. Die Datenbank besitzt eine automatische Backup-Funktion.</p> <p>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 <i>tiamo</i>-Software jederzeit gelesen werden.</p> <p>Das Verfahren, wie Daten archiviert werden und welche Daten das sind, muss durch den Betreiber festgelegt werden. Schnittstellen zur Archivierung (XML-Files) sind im System vorhanden.</p> |

| Ifd. Nr. | Ref. | Thema | Frage | Ja | Nein | Bemerkungen |
|----------|---------------------------|---|--|----|------|--|
| 1.6 | 11.10 (d) | Login, Zugriffsschutz, Berechtigung Benutzer, Administrator | Ist der Systemzugriff auf berechtigte Personen beschränkt? | X | | <p>Die Software besitzt ein Login mit einer unbegrenzten Anzahl Profilen (Zugriffsrechten/ Personengruppen). Die Zugriffsrechte für die einzelnen Benutzergruppen können von Administratoren frei definiert werden.</p> <p>Die für das System verantwortliche Person (i. d. R. der Administrator) muss sicherstellen, dass nur berechtigte Personen eine Zugangsberechtigung erhalten.</p> <p>Alle Änderungen an den Zugriffsrechten werden im Audit Trail aufgezeichnet.</p> |
| 1.7 | 11.10 (e) | Audit Trail, elektronische Aufzeichnung, Bediener-eingaben | Besteht ein sicherer, rechnergenerierter, zeitgestempelter Audit Trail, der Datum und Zeit der Bediener-eingaben und Aktionen protokolliert, welche elektronische Aufzeichnungen erstellen, ändern oder löschen? | X | | <p>Im Audit Trail werden alle relevanten Bediener-eingaben und Aktionen zu den elektronischen Daten mit Benutzername, Datum und Uhrzeit mit Differenz zu UTC dokumentiert; Änderungen an Methoden, Bestimmungen und Probanden (nur Live-Änderungen) erfordern vom Bediener zusätzlich die Eingabe eines Kommentars.</p> <p>Zusätzlich werden alle Änderungen an den Sicherheitseinstellungen, der Anwenderverwaltung und den Konfigurationsdaten im Audit Trail protokolliert.</p> |
| 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. |

| Ifd. Nr. | Ref. | Thema | Frage | Ja | Nein | Bemerkungen |
|----------|---------------------------|--|--|----------|------|--|
| 1.9 | 11.10 (e) | Audit Trail, Aufbewahrungszeit | Bleibt der Audit Trail einer elektronischen Aufzeichnung während der ganzen Aufbewahrungszeit der Aufzeichnung wiederauffindbar? | X | | <p>Sämtliche Audit Trail Daten werden in der Konfigurationsdatenbank gespeichert und bleiben so lange bestehen, wie der Audit Trail nicht gelöscht wird. Der Speicherplatz ist hier der beschränkende Faktor. Der Audit Trail kann nur gelöscht werden, wenn er vorher archiviert wurde. Der Audit Trail wird als Textdatei mit einer Checksumme archiviert.</p> <p>Für die sichere Aufbewahrung der archivierten Audit Trails ist ausschliesslich der Betreiber verantwortlich.</p> <p>Die als „Audit Trail“ bezeichnete Protokollierung, in der sämtliche Änderungen an Methoden, Bestimmungen und Konfigurationsdaten (Geräte, globale Tabellen, GLP, Anwenderverwaltung, globale Systemeinstellungen, usw.) aufgezeichnet werden, wird vom normalen Logging der Systemaktionen (Datenverkehr, Geräteaktionen, Fehler, usw.) unterschieden.</p> |
| 1.10 | 11.10 (e) | Audit Trail, FDA, Einsichtnahme | Ist der Audit Trail zur Überprüfung und Vervielfältigung durch die FDA verfügbar? | X | | <p>Der Audit Trail kann als Textdatei mit einer Checksumme exportiert werden und ist so in elektronischer Form verfügbar. Über die Checksumme, kann die Integrität des Audit Trails verifiziert werden.</p> <p>Unabhängig davon kann eine schreibgeschützte PDF-Datei des Audit Trails erzeugt und gedruckt werden.</p> |
| 1.11 | 11.10 (f) | Ablaufsteuerung, 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 | | <p>Im System werden Plausibilitätsprüfungen schon beim Start der Bestimmung durchgeführt, so wird zum Beispiel überprüft, ob alle benötigten Geräte vorhanden sind.</p> <p>Der Ablauf der Bestimmung ist in der Methode festgelegt und muss strikt eingehalten werden.</p> <p>Das Einhalten des Ablaufs wird durch die Verwendung der Probenzuordnungstabelle oder der automatischen Probedatenabfrage unterstützt. So sind immer nur die Funktionen zugänglich, die ausgeführt werden können.</p> |

| Ifd. Nr. | Ref. | Thema | Frage | Ja | Nein | Bemerkungen |
|----------|---------------------------|--|---|-----|------|---|
| 1.12 | 11.10 (g) | Login, Zugriffsschutz, Berechtigung, Benutzer, Administrator | Stellt das System sicher, dass nur berechnigte 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 verantwortliche Person (= Administrator) muss sicherstellen, dass nur berechnigte 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 dieselbe Person ist. |
| 1.13 | 11.10 (h) | Waage, Anschluss, Endgerät, Eingabedaten, Geräte | Kontrolliert das System die Gültigkeit der angeschlossenen Geräte? <i>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.</i> | X/B | | Während der IQ werden alle angeschlossenen Geräte in die Geräte-liste eingetragen und später geprüft. Metrohm-Geräte werden erkannt, auf Gültigkeit geprüft und automatisch in die Geräteliste eingetragen. Die Validierung der angeschlossenen Geräte erfolgt im Rahmen der Systemvalidierung (siehe auch 11.10 (a), Nr. 1.1) in der Verantwortung des Betreibers. |
| 1.14 | 11.10 (i) | Schulung, Support, Benutzer, Administrator | Gibt es dokumentierte Schulungen, einschliesslich Ausbildung am Arbeitsplatz (training 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. |
| 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. |

| Ifd. Nr. | Ref. | Thema | Frage | Ja | Nein | Bemerkungen |
|----------|---------------------------|--|--|------------|------|---|
| 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 Systemdokumentation (bspw. Handbuch) liegt in der Verantwortung des Betreibers. |
| 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. Die Protokollierung von Änderungen der Systemdokumentation und Software – bspw. im Gerätelogbuch – liegt in der Verantwortung des Betreibers. Vorlagen für diese Dokumente werden von Metrohm zur Verfügung gestellt. |

2 Zusätzliche Verfahren und Kontrollen für offene Systeme

| Ifd. Nr. | Ref. | Thema | Frage | Ja | Nein | 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 <i>Tiamo</i> über das Internet ist nicht vorgesehen. Die Daten werden als Datei gespeichert, verschlüsselt und mit einer 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 elektronische Unterschriften verwendet, um die beteiligten Personen zu authentifizieren? | N/A | | Ein Zugriff auf <i>Tiamo</i> über das Internet ist nicht vorgesehen. Es sind zwei Unterschriftsebenen eingerichtet. Das System fordert, dass Prüfer und Freigebender nicht dieselbe Person (d. h., nicht derselbe Benutzername) ist. Methoden und Bestimmungen können unterschrieben und somit elektronisch freigegeben werden. Die Daten werden als Datei gespeichert, verschlüsselt und mit einer 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. |

3 Unterschriebene elektronische Daten

| Ifd. Nr. | Ref. | Thema | Frage | Ja | Nein | 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 Bedeutung (aus Auswahl-liste) für die Unterschrift. Zusätzlich kann zu einer Unterschrift ein Kommentar eingegeben werden, der zusammen mit der elektronischen Unterschrift abgespeichert wird. |
| 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 können die kompletten Unterschriftsdaten ausgegeben werden. |
| 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 sicher mit der Methode oder der Bestimmung verbunden. Das Ausschneiden, Kopieren oder Übertragen der Unterschriftsdaten ist mit gewöhnlichen Mitteln 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)

| Ifd. Nr. | Ref. | Thema | Frage | Ja | Nein | Bemerkungen |
|----------|----------------------------|--|---|----------|------|---|
| 4.1 | 11.100 (a) | Elektronische Unterschrift | Sind elektronische Unterschriften eindeutig einer Person zugeordnet? | X | | Jedem Benutzer ist ein eindeutiger Anmeldename zugeordnet; das System überwacht die Eindeutigkeit des Anmeldens. Betrieblich ist sicherzustellen, dass ein und derselbe Anmeldename nicht verschiedenen Personen zugeordnet wird. |
| 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, Stellvertreterregelung | Erlaubt das System die Übertragung der Berechtigung von elektronischen Unterschriften (Stellvertreterregelung)? | B | | Die sichere und nachvollziehbare Verwaltung von Benutzerrechten ist Aufgabe des Betreibers. Die Zuordnung eines Stellvertreters ist Teil der regulären Benutzerverwaltung und ist durch den Administrator durchzuführen. Hierfür muss eine betriebliche Regelung vorhanden sein. |
| 4.4 | 11.100 (b) | Elektronische Unterschrift | Wird die Identität einer Person vor der Zuteilung einer elektronischen Unterschrift überprüft? | B | | Der Betreiber muss im Zuge der Berechtigungsvergabe die Identität der jeweiligen Person gegen den Berechtigungsantrag prüfen. |

5 Elektronische Unterschriften (nicht-biometrisch)

| Ifd. Nr. | Ref. | Thema | Frage | Ja | Nein | 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 | | Die Unterschriftsfunktion wird mittels Anmeldename und Passwort ausgeführt. |
| 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, elektronische Unterschrift fälschen | Benötigt ein Versuch, eine elektronische Unterschrift zu fälschen, das Zusammenwirken von mindestens zwei Personen? | X | | Die Daten in der Datenbank sind in einem für den Menschen nicht lesbarem Format codiert. |

6 Elektronische Unterschriften (biometrisch)

| Ifd. Nr. | Ref. | Thema | Frage | Ja | Nein | Bemerkungen |
|----------|----------------------------|---|---|-----|------|--|
| 6.1 | 11.200 (b) | Elektronische Unterschrift, biometrische elektronische Unterschrift | Ist es erwiesen, dass biometrische elektronische Unterschriften ausschliesslich durch ihren tatsächlichen Eigentümer verwendet werden können? | N/A | | Mit dem System werden keine biometrische Unterschriften verwaltet. |

7 Kontrolle von Identifikationscode und Passwort

| lfd. Nr. | Ref. | Thema | Frage | Ja | Nein | 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 | | <p>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!</p> <p>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.</p> <p>Generell wird empfohlen, organisationsweit Richtlinien festzulegen, in denen die Erstellung von Anwenderkonten und die Verwendung von Passwörtern (Länge, Gültigkeitsdauer,...) festgelegt wird.</p> |
| 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 periodische Überprüfung der Identifikationscodes ist der Betreiber verantwortlich. |
| 7.3 | 11.300 (b) | Passwort, Gültigkeit, Verfall Passwort, Identifikation, Login, Zugriffsschutz | Unterstehen Passwörter dem periodischen Verfall, damit sie regelmässig geändert werden müssen? | X | | <p>Die Gültigkeitsdauer für das Passwort kann vom Administrator festgelegt werden. Nach Ablauf dieser Frist muss das Passwort vom Benutzer zwingend geändert werden.</p> <p>Sofern die Sicherheitseinstellung „Eindeutiges Passwort“ gesetzt ist, verhindert die Passworthistorie eine Wiederverwendung von Passwörtern.</p> |
| 7.4 | 11.300 (b) | Identifikationscode, Passwort, Gültigkeit, Sperrung Zugangsbe- rechtigung, 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 | | <p>Das Verfahren muss vom Betreiber festgelegt werden.</p> <p>Der entsprechende Benutzer kann im System vom Administrator deaktiviert werden, bleibt jedoch im System in der Gruppe „entfernte Anwender“ ohne jegliche Zugriffsrechte gespeichert.</p> |

| Ifd. Nr. | Ref. | Thema | Frage | Ja | Nein | Bemerkungen |
|----------|----------------------------|---|--|------------|------|--|
| 7.5 | 11.300 (c) | Identifikationscode, Passwort, Gültigkeit, Sperrung Zugangsbe- rechtigung, 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 deaktiviert werden, bleibt jedoch im System in der Gruppe „entfernte Anwender“ ohne jegliche Zugriffsrechte gespeichert. |
| 7.6 | 11.300 (c) | Verlust / Kompromittierung ID-Karte, elektronische Sperrung | Besteht ein Verfahren zur elektronischen Sperrung eines Zugangsgeräts (z. B. ID-Karte), falls es verloren oder gestohlen wurde, oder möglicherweise unsicher ist? | N/A | | Ein spezielles Gerät zur Identifikation des Benutzers ist nicht vorgesehen. |
| 7.7 | 11.300 (c) | ID-Karte, Ersatz | Gibt es kontrollierte Verfahren wie ein Zugangsgerät (z. B. ID-Karte) vorübergehend oder dauerhaft gegen ein Ersatzgerät ausgetauscht wird? | N/A | | Ein spezielles Gerät zur Identifikation des Benutzers ist nicht vorgesehen. |
| 7.8 | 11.300 (d) | Missbrauch, Login, Zugriffsschutz | Bestehen Kontrollen zur Verhinderung und/oder Erkennung von missbräuchlicher Verwendung von Benutzererkennung oder Passwort? | X/B | | Nach n-maligen Fehlversuchen (Anzahl kann vom Administrator definiert werden) wird eine Meldung ausgegeben, dass die maximale Anzahl erfolgloser Login-Versuche erreicht wurde und der Benutzer gesperrt; diese Meldung kann per E-Mail verschickt werden. |
| 7.9 | 11.300 (d) | Missbrauch, Login, Zugriffsschutz, Information an verantwortliche Stelle | Existiert ein Verfahren, nach dem beim Auftreten einer missbräuchlichen Verwendung von Benutzererkennung oder Passwort, die für Sicherheitsfragen zuständigen Stelle(n) sofort und direkt informiert werden? | B | | Das Verfahren zur Benachrichtigung der für die Sicherheit zuständigen Stelle ist durch den Betreiber zu regeln. |
| 7.10 | 11.300 (e) | Überprüfung ID-Karte, ID-Karte, Zugriffsschutz | Werden Identifikationsmarken und Karten am Anfang und danach periodisch überprüft? | N/A | | Ein spezielles Gerät zur Identifikation des Benutzers ist nicht vorgesehen. |
| 7.11 | 11.300 (e) | Änderung ID-Karte, ID-Karte, Missbrauch, Zugriffsschutz | Beinhaltet diese Prüfung auch eine Kontrolle, dass keine unerlaubten Änderungen vorgenommen wurden? | N/A | | Ein spezielles Gerät zur Identifikation des Benutzers ist nicht vorgesehen. |

B = Der Betreiber ist für die Umsetzung verantwortlich.

N/A = Trifft auf das System nicht zu (not applicable)

Das hier dokumentierte 21 CFR Part 11 Assessment basiert auf einem Audit, das am 13.01.2009 auf Basis der Version *tiamo* 2.0 durchgeführt wurde. Alle nachfolgenden Softwareversionen – einschliesslich der aktuellen Version – beinhalten gemäss Aussage der Metrohm AG (Entwicklung und Qualitätssicherung) keine 21 CFR Part 11 relevanten Änderungen bzw. sind die vorgenommenen Änderungen 21 CFR Part 11 konform (s. Release Notes 8.101.8017EN, 8.101.8027EN,

8.101.8039EN, 8.101.8055EN, 8.101.8072EN und 8.101.8080EN). Aus diesem Grunde konnte auf eine Nachprüfung in Form eines Vor-Ort-Audits verzichtet werden.

8 Indizes

Verweise auf die Seitenzahl:

A

| | |
|-------------------------|------------|
| Ablaufsteuerung | 6 |
| Administrator | 5, 7 |
| Änderung | 3, 5 |
| Änderung ID-Karte | 15 |
| Anschluss | 7 |
| Archivierung | 4 |
| Audit Trail | 3, 5, 6, 8 |
| Aufbewahrungszeit | 4, 6 |
| Ausdruck | 3 |

B

| | |
|---|------|
| Bedienereingaben | 5 |
| Benutzer | 5, 7 |
| Berechtigung | 5, 7 |
| biometrische elektronische Unterschrift | 13 |

D

| | |
|------------------------|---|
| Daten | 9 |
| Datenübertragung | 9 |
| Dokumentation | 8 |

E

| | |
|---|----------------------|
| Eindeutigkeit | 14 |
| Eingabedaten | 7 |
| Einsichtnahme | 6 |
| elektronische Aufzeichnung | 3, 4, 5 |
| elektronische Sperrung | 15 |
| elektronische Unterschrift | 7, 9, 10, 11, 12, 13 |
| elektronische Unterschrift fälschen | 12 |
| Endgerät | 7 |
| Ersatz | 15 |

F

| | |
|-----------|------|
| FDA | 4, 6 |
|-----------|------|

G

| | |
|----------------------------|--------|
| Gebrauchsanleitungen | 8 |
| Geräte | 6, 7 |
| Gültigkeit | 14, 15 |

I

| | |
|---|--------|
| Identifikation | 14, 15 |
| Identifikationscode | 14, 15 |
| ID-Karte | 15 |
| Information an verantwortliche Stelle | 15 |
| IQ | 2 |

K

| | |
|---------------------------------|----|
| Kompromittierung ID-Karte | 15 |
|---------------------------------|----|

L

| | |
|---------------|--------------|
| Logbuch | 8 |
| Login | 5, 7, 14, 15 |

M

| | |
|------------------|----|
| Missbrauch | 15 |
|------------------|----|

O

| | |
|----------|---|
| OQ | 2 |
|----------|---|

P

| | |
|----------------|--------|
| Passwort | 14, 15 |
|----------------|--------|

| | |
|-----------------------------|---|
| Plausibilitätsprüfung | 6 |
| Policy | 7 |

R

| | |
|--------------|------|
| Report | 3, 4 |
|--------------|------|

S

| | |
|------------------------------------|--------|
| Schulung | 7 |
| SOP | 8 |
| Sperrung Zugangsberechtigung | 14, 15 |
| Stellvertreterregelung | 11 |
| Support | 7 |
| Systemdokumentation | 8 |

U

| | |
|-------------------------------|----|
| Überprüfung ID-Karte | 15 |
| Überschreiben von Daten | 5 |

V

| | |
|--------------------------------|----|
| Validierung | 2 |
| Verantwortung | 7 |
| Verfall Passwort | 14 |
| Verlust ID-Karte | 15 |
| Verschlüsselung | 9 |
| Verteilung Dokumentation | 8 |

W

| | |
|-------------|---|
| Waage | 7 |
|-------------|---|

Z

| | |
|---------------------------------|--------------|
| Zugriff auf Dokumentation | 8 |
| Zugriffsschutz | 5, 7, 14, 15 |

Verweise auf die laufende Nummer des Tabelleneintrags:**A**

| | |
|-------------------------|---------------------------|
| Ablaufsteuerung | 1.11 |
| Administrator | 1.14, 1.12, 1.6 |
| Änderung | 1.8, 1.2 |
| Änderung ID-Karte | 7.11 |
| 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 elektronische 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 |
| elektronische Aufzeichnung | 1.8, 1.7, 1.5, 1.4, 1.3 |
| elektronische Sperrung | 7.6 |
| 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 |
| elektronische Unterschrift fälschen | 5.5 |
| Endgerät | 1.13 |
| Ersatz | 7.7 |

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 | 7.11, 7.10, 7.7 |
| Information an verantwortliche Stelle | 7.9 |
| IQ | 1.1 |

K

| | |
|---------------------------------|-----|
| Kompromittierung ID-Karte | 7.6 |
|---------------------------------|-----|

L

| | |
|---------------|--|
| Logbuch | 1.17, 1.16 |
| Login | 7.9, 7.8, 7.5, 7.4, 7.3, 7.2, 7.1, 1.12, 1.6 |

M

| | |
|------------------|----------------|
| Missbrauch | 7.11, 7.9, 7.8 |
|------------------|----------------|

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 |
| SOP | 1.17 |
| Sperrung Zugangsberechtigung | 7.5, 7.4 |
| Stellvertreterregelung | 4.3 |
| Support | 1.14 |
| Systemdokumentation | 1.17, 1.16 |

U

| | |
|-------------------------------|------|
| Überprüfung ID-Karte | 7.10 |
| Überschreiben von Daten | 1.8 |

V

| | |
|--------------------------------|----------|
| Validierung | 1.1 |
| Verantwortung | 1.15 |
| Verfall Passwort | 7.3 |
| Verlust ID-Karte | 7.6, 7.5 |
| Verschlüsselung | 2.1 |
| Verteilung Dokumentation | 1.16 |

W

| | |
|-------------|------|
| Waage | 1.13 |
|-------------|------|

Z

| | |
|---------------------------------|--|
| Zugriff auf Dokumentation | 1.16 |
| Zugriffsschutz | 7.11, 7.10, 7.9, 7.8, 7.5, 7.4, 7.3, 7.2, 7.1, 1.12, 1.6 |