Anhang B – Überwachungskategorien und -ereignisse

(Engl. Originaltitel: Appendix B - Audit Categories and Events)

Matrix zur Einhaltung der Sicherheitsziele bei der Überwachung

Komponente	Ereignis	Überwachungsereignis	Erforderliche Einstellung	
			E	**F**
FAU_GEN.1	Starten und Beenden der Überwachungsfunktionen.	**Kategorie: Richtlinienänderung** 612 – Änderung der Überwachungsrichtlinien. (Das Ereignis wird bei jedem Aktivieren oder Deaktivieren der Überwachung für eine beliebige Überwachungskategorie erzeugt. Eine Liste der Überwachungs-änderungen wird im Ereignisprotokoll angezeigt.)	✓	
FAU_GEN.2	Kein			
FAU_SAR.1	Lesen von Informationen aus den Überwachungsdatensätzen.	**Kategorie: Rechteverwendung** 578 – Privilegiertes-Objekt-Vorgang. (Zugriff auf das Sicherheitsereignisprotokoll. Bei SeSecurityPrivilege sollte sich ein Erfolg ergeben.)	✓	
FAU_SAR.2	Nicht erfolgreiche Versuche, Informationen aus den Überwachungsdatensätzen zu lesen.	**Kategorie: Rechteverwendung** 578 – Privilegiertes-Objekt-Vorgang. (Bei SeSecurityPrivilege sollte sich ein Fehler ergeben.)		✓
FAU_SAR.3	Kein			
FAU_SEL.1	Alle Änderungen der Überwachungskonfiguration, die während der Überwachungserfassung auftreten.	**Kategorie: Richtlinienänderung** 612 – Änderung der Überwachungsrichtlinien. (Eine Liste der Überwachungsänderungen wird im Ereignisprotokoll angezeigt.)	✓	
FAU_STG.1	Kein			

Komponente	Ereignis	Überwachungsereignis	Erforderliche Einstellung	
FAU_STG.3	Aktionen, die aufgrund der Überschreitung eines Schwellenwerts durchgeführt wurden.	**Kategorie: System** 516 – Die für die Überwachung reservierten internen Ressourcen sind ausgelastet. Dies wird zu einem Verlust von Überwachungsereignissen führen. 517 – Das Überwachungsprotokoll wurde gelöscht. (Überprüfungsaktion eines autorisierten Administrators, um die Ereignisprotokolle zu löschen, weil das System einen vordefinierten Überwachungsschwellenwert überschritten hat.) 523 – Die Überwachungsliste ist zu x% voll. **Anmerkung:** Das obige Ereignis wird nur mit SP3 erzeugt. Der Schlüsselwert muss auf den vom Administrator gewünschten Prozentwert festgelegt werden, den das Überwachungsprotokoll nicht überschreiten soll. (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel)	✓	
FAU_STG.4	Aktionen, die aufgrund von Fehlern im Überwachungsspeicher durchgeführt werden.	517 – Das Überwachungsprotokoll wurde gelöscht. (Überprüfungsaktion eines autorisierten Administrators, um die Ereignisprotokolle zu löschen, weil das System einen vordefinierten Überwachungsschwellenwert überschritten hat.)		
FDP_ACC.1(a)	Kein			
FDP_ACF.1(a)	Alle Anforderungen, einen Vorgang für ein Objekt auszuführen, das von SFP abgedeckt wird.	**Kategorie: Objektzugriff** 563 – Objekt kann gelöscht werden. 564 – Gelöschtes Objekt. 565 – Geöffnetes Objekt. 566 – Objektvorgang. **Kategorie: Prozessnachverfolgung** 594 – Ein Handle eines Objekts wurde dupliziert. 595 – Indirekter Zugriff auf ein Objekt erfolgreich.	✓	✓

Komponente	Ereignis	Überwachungsereignis	Erforderliche Einstellung	
FDP_RIP.2	Kein			
FDP_RIP.2. Anmerkung 1	Kein			
FIA_ATD.1	Kein			
FIA_SOS.1	Ablehnung oder Annahme von TSF eines überprüften Kennworts.	**Kategorie: Anmeldung** 528 – Erfolgreiche Anmeldung. 529 – Fehlgeschlagene Anmeldung: unbekannter Benutzername oder falsches Kennwort. 535 – Fehlgeschlagene Anmeldung: Das angegebene Kennwort des Kontos ist abgelaufen. 540 – Erfolgreiche Netzwerkanmeldung. 545 – IKE-Peerauthentifizierung fehlgeschlagen. **Kategorie: Kontoanmeldung** 680 – Verwendetes Konto für die Anmeldung. 681 – Die Anmeldung des Kontos: <Clientname> durch: <Quelle> von der Arbeitsstation <Arbeitsstation> ist fehlgeschlagen. Fehlercode: <Fehler>.	✓ ✓	✓ ✓
FIA_UAU.7	Kein			
FIA_USB.1	Erfolg oder Fehler beim Binden der Sicherheitsattribute eines Benutzers an ein Subjekt (z. B. Erfolg und Fehler beim Erstellen eines Subjekts).	**Kategorie: Prozessnachverfolgung** 592 – Ein neuer Vorgang wurde erstellt.	✓	✓
FMT_MSA.1(a)	Alle Änderungen der Werte von Objektsicherheitsattributen.	**Kategorie: Objektzugriff** 560 – Geöffnetes Objekt. (Unter **Beschreibung: Zugriffe** sollten die folgenden Einträge vorhanden sein: **Daten anhängen**, **Attribute lesen** und **Attribute schreiben**.)	✓	
FMT_MSA.3(a)	Änderungen der Standardeinstellung von Zulassungs- oder Einschränkungsregeln. Alle Änderungen des Anfangswertes von Sicherheitsattributen.	**Kategorie: Objektzugriff** 560 – Geöffnetes Objekt.	✓	

Komponente	Ereignis	Überwachungsereignis	Erforderliche Einstellung	
FMT_MTD.1(a) CAPP – 5.4.3	Alle Änderungen der Werte von TSF-Daten (Erstellen, Entfernen und Löschen des Überwachungsprotokolls).	**Kategorie: System** 517 – Das Überwachungsprotokoll wurde gelöscht. **Kategorie: Objektzugriff** (Diese Ereignisse können das direkte Löschen der Sicherheitsprotokolldateien protokollieren, wenn die Überwachung der Sicherheitsprotokolldateien eingerichtet ist.) 563 – Objekt kann gelöscht werden. 564 – Gelöschtes Objekt. **Kategorie: Rechteverwendung** 578 – Privilegiertes-Objekt-Vorgang. (Gezeigt als Verwendung von SeSecurityPrivilege; die tatsächlichen Änderungen sind in Ereignis 612 aufgeführt.) **Kategorie: Richtlinienänderung** 612 – Änderung der Überwachungsrichtlinien.	✓ ✓ ✓ ✓	
FMT_MTD.1(b) CAPP – 5.4.4	Alle Änderungen der Werte von TSF-Daten (Änderung des Überwachungsprotokolls, einschließlich des neuen Wertes der TSF-Daten).	**Kategorie: Richtlinienänderung** 612 – Änderung der Überwachungsrichtlinien.		
FMT_MTD.1(c) CAPP – 5.4.5	Alle Änderungen der Werte von TSF-Daten (Sicherheitsattribute des Benutzers, einschließlich des neuen Wertes der TSF-Daten).	**Kategorie: Richtlinienänderung** 608 – Zugewiesenes Benutzerrecht. 609 – Entferntes Benutzerrecht. **Kategorie: Kontenverwaltung** 624 – Erstelltes Benutzerkonto. 625 – Geänderter Benutzerkontentyp. 626 – Aktiviertes Benutzerkonto. 629 – Deaktiviertes Benutzerkonto. 630 – Gelöschtes Benutzerkonto. 631 – Globale Gruppe mit aktivierter	✓ ✓	

Komponente	Ereignis	Überwachungsereignis	Erforderliche Einstellung	
		Sicherheit (Sicherheitsgruppe) erstellt. 632 – Mitglied zu globaler Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe) hinzugefügt. 633 – Mitglied aus globaler Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe) entfernt. 634 – Gelöschte globale Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe). 636 – Mitglied zu lokaler Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe) hinzugefügt. 637 – Mitglied aus lokaler Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe) entfernt. 638 – Gelöschte lokale Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe). 639 – Geänderte lokale Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe). 640 – Allgemeine Kontendatenbankänderung. 641 – Geänderte globale Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe). 642 – Geändertes Benutzerkonto. 644 – Gesperrtes Benutzerkonto. 648 – Erstellte lokale Gruppe mit deaktivierter Sicherheit (Verteilergruppe). 649 – Geänderte lokale Gruppe mit deaktivierter Sicherheit (Verteilergruppe). 650 – Mitglied zu lokaler Gruppe mit deaktivierter Sicherheit (Verteilergruppe) hinzugefügt. 651 – Mitglied aus lokaler Gruppe mit deaktivierter Sicherheit (Verteilergruppe) entfernt. 652 – Gelöschte lokale Gruppe mit deaktivierter Sicherheit		

Komponente	Ereignis	Überwachungsereignis	Erforderliche Einstellung	
		(Verteilergruppe). 653 – Globale Gruppe mit deaktivierter Sicherheit erstellt. 654 – Geänderte globale Gruppe mit deaktivierter Sicherheit (Verteilergruppe). 655 – Mitglied zu globaler Gruppe mit deaktivierter Sicherheit (Verteilergruppe) hinzugefügt. 656 – Mitglied aus globaler Gruppe mit deaktivierter Sicherheit (Verteilergruppe) entfernt. 657 – Gelöschte globale Gruppe mit deaktivierter Sicherheit (Verteilergruppe). 659 – Geänderte universelle Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe). 658 – Universelle Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe) erstellt. 660 – Mitglied zu universeller Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe) hinzugefügt. 661 – Mitglied aus universeller Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe) entfernt. 662 – Gelöschte universelle Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe). 664 – Geänderte universelle Gruppe mit deaktivierter Sicherheit (Verteilergruppe). 665 – Mitglied zu universeller Gruppe mit deaktivierter Sicherheit (Verteilergruppe) hinzugefügt. 666 – Mitglied aus universeller Gruppe mit deaktivierter Sicherheit (Verteilergruppe) entfernt. 667 – Gelöschte universelle Gruppe mit deaktivierter Sicherheit (Verteilergruppe). 668 – Geänderter Gruppentyp.		

Komponente	Ereignis	Überwachungsereignis	Erforderliche Einstellung	
FMT_MTD.1(d) CAPP – 5.4.6	Alle Änderungen der Werte von TSF-Daten (Authentifizierungsdaten).	**Kategorie: Kontenverwaltung** 627 – Versuch, Kennwort zu ändern. 628 – Kennwort für Benutzerkonto gesetzt.	✓	✓
FMT_REV.1(a) CAPP – 5.4.7	Alle Versuche, Sicherheitsattribute (Benutzerattribute) zu widerrufen.	**Kategorie: Richtlinienänderung** 609 – Entferntes Benutzerrecht. **Kategorie: Kontenverwaltung** 629 – Deaktiviertes Benutzerkonto. 644 – Gesperrtes Benutzerkonto.	✓ ✓	
FMT_REV.1(b) CAPP – 5.4.8	Alle Änderungen der Werte von TSF-Daten (Objektattribute).	(Siehe FMT_MSA.1a.)		
FMT_SMR.1	Änderungen der Gruppe von Benutzern, die Teil einer Rolle sind. Jede Verwendung der Rechte einer Rolle. (Zusätzlich/Detailliert)	**Kategorie: Rechteverwendung** 578 – Privilegiertes-Objekt-Vorgang. **Kategorie: Kontenverwaltung** 632 – Mitglied zu globaler Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe) hinzugefügt. 633 – Mitglied aus globaler Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe) entfernt. 634 – Gelöschte globale Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe). 636 – Mitglied zu lokaler Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe) hinzugefügt. 637 – Mitglied aus lokaler Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe) entfernt. 638 – Gelöschte lokale Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe). 639 – Geänderte lokale Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe). 640 – Allgemeine Kontendatenbankänderung. 641 – Geänderte globale Gruppe mit	✓ ✓	✓

Komponente	Ereignis	Überwachungsereignis	Erforderliche Einstellung	
		aktivierter Sicherheit (Sicherheitsgruppe). 648 – Erstellte lokale Gruppe mit deaktivierter Sicherheit (Verteilergruppe). 649 – Geänderte lokale Gruppe mit deaktivierter Sicherheit (Verteilergruppe). 650 – Mitglied zu lokaler Gruppe mit deaktivierter Sicherheit (Verteilergruppe) hinzugefügt. 652 – Gelöschte lokale Gruppe mit deaktivierter Sicherheit (Verteilergruppe). 654 – Geänderte globale Gruppe mit deaktivierter Sicherheit (Verteilergruppe). 655 – Mitglied zu globaler Gruppe mit deaktivierter Sicherheit (Verteilergruppe) hinzugefügt. 656 – Mitglied aus globaler Gruppe mit deaktivierter Sicherheit (Verteilergruppe) entfernt. 657 – Gelöschte globale Gruppe mit deaktivierter Sicherheit (Verteilergruppe). 659 – Geänderte universelle Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe). 660 – Mitglied zu universeller Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe) hinzugefügt. 661 – Mitglied aus universeller Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe) entfernt. 662 – Gelöschte universelle Gruppe mit aktivierter Sicherheit (Sicherheitsgruppe). 664 – Geänderte universelle Gruppe mit deaktivierter Sicherheit (Verteilergruppe). 665 – Mitglied zu universeller Gruppe mit deaktivierter Sicherheit (Verteilergruppe) hinzugefügt.		

Komponente	Ereignis	Überwachungsereignis	Erforderliche Einstellung	
		666 – Mitglied aus universeller Gruppe mit deaktivierter Sicherheit (Verteilergruppe) entfernt. 668 – Geänderter Gruppentyp.		
FPT_AMT.1	Ausführen des Tests des zugrunde liegenden Computers und die Ergebnisse des Tests.	Nicht zutreffend		
FPT_RVM.1	Kein			
FPT_SEP.1	Kein			

Komponente	Ereignis	Überwachungsereignis	Erforderliche Einstellung	
FPT_STM.1	Änderungen der Uhrzeit.	**Kategorie: Rechteverwendung** 577 – Aufgerufener privilegierter Dienst. (Gezeigt als Verwendung von SeSystemTimePrivilege.)	✓	✓
FIA_AFL.1	Anmeldung fehlgeschlagen. (Deaktivieren eines Kontos aufgrund der Übereinstimmung mit einem vordefinierten Schwellenwert.)	**Kategorie: Anmeldung** 529 – Anmeldung fehlgeschlagen: unbekannter Benutzername oder falsches Kennwort. (Führt zur Sperre.) **Kategorie: Kontenverwaltung** 642 – Geändertes Benutzerkonto – Konto gesperrt. 644 – Gesperrtes Benutzerkonto.	✓	✓
FIA_UAU.2	Verwendung des Authentifizierungsmechanismus.	**Kategorie: Anmeldung** 528 – Erfolgreiche Anmeldung. 529 – Anmeldung fehlgeschlagen: unbekannter Benutzername oder falsches Kennwort. 540 – Erfolgreiche Netzwerkanmeldung. **Kategorie: Kontoanmeldung** 680 – Verwendetes Konto für die Anmeldung. 681 – Die Anmeldung des Kontos: <Clientname> durch: <Quelle> von der Arbeitsstation <Arbeitsstation> ist fehlgeschlagen. Fehlercode: <Fehler>.	✓	✓

Komponente	Ereignis	Überwachungsereignis	Erforderliche Einstellung	
FIA_UID.2	Jegliche Verwendung des Benutzeridentifizierungsmechanismus, einschließlich der bei erfolgreichen Versuchen bereitgestellten Identität.	**Kategorie: Anmeldung** 528 – Erfolgreiche Anmeldung. 529 – Anmeldung fehlgeschlagen: unbekannter Benutzername oder falsches Kennwort. 535 – Anmeldung fehlgeschlagen: Das angegebene Kennwort des Kontos ist abgelaufen. 540 – Erfolgreiche Netzwerkanmeldung. 545 – IKE-Peerauthentifizierung fehlgeschlagen. **Kategorie: Kontoanmeldung** 625 – Fehlgeschlagene Vorbestätigung. 681 – Die Anmeldung des Kontos: <Clientname> durch: <Quelle> von der Arbeitsstation <Arbeitsstation> ist fehlgeschlagen. Fehlercode: <Fehler>.	✓	✓
FMT_MOF.1(a)	Änderungen der Überwachungsrichtlinien.	**Kategorie: Rechteverwendung** 578 – Privilegiertes-Objekt-Vorgang. (Gezeigt als Verwendung von SeSecurityPrivilege.) **Kategorie: Richtlinienänderung** 612 – Änderung der Überwachungsrichtlinien.	✓ ✓	✓
FMT_MTD.1(g)	Versuch, das Recht eines autorisierten Administrators zu verwenden, um die TSF-Zeit zu ändern.	**Kategorie: Rechteverwendung** 577 – Aufgerufener privilegierter Dienst. (Gezeigt als Verwendung von SeSystemTimePrivilege.)	✓	

Komponente	Ereignis	Überwachungsereignis	Erforderliche Einstellung	
TRANSFER_PROT_EX	IPSec-relevante Ereignisse.	**Kategorie: Anmeldung** 541 – IKE-Sicherheitszuordnung wurde hergestellt. 542 – IKE-Sicherheitszuordnung wurde beendet. Modus: Datenschutz (Schnellmodus). 543 – IKE-Sicherheitszuordnung wurde beendet. Modus: Schlüsselaustausch (Hauptmodus). 544 – IKE-Sicherheitszuordnung konnte nicht hergestellt werden, da der Peer nicht authentifizieren konnte. 545 – IKE-Peerauthentifizierung fehlgeschlagen. 546 – IKE-Sicherheitszuordnung konnte nicht hergestellt werden, da der Peer eine ungültige Anfrage gesendet hat. 547 – IKE-Sicherheitszuordnung konnte nicht ausgehandelt werden.. **Kategorie: Richtlinienänderung** 613 – Starten des IP-Sicherheitsrichtlinien-Agenten. 614 – Geänderte IPSec-Richtlinie. 615 – IP-Sicherheitsrichtlinien-Agent hat einen schwerwiegenden Fehler entdeckt. 616 – IP-Sicherheitsrichtlinien-Agent hat einen schwerwiegenden Fehler entdeckt.	✓ ✓	✓ ✓
FTA_SSL1	Versuch, Sperrung aufzuheben.	**Kategorie: Anmeldung** 528 – Erfolgreiche Anmeldung (Eintrag 6 ist entsperrt). 529 – Fehlgeschlagene Anmeldung (Eintrag 6 ist entsperrt).	✓	✓
FTA_SSL.2	Versuch, Sperrung aufzuheben.	**Kategorie: Anmeldung** 528 – Erfolgreiche Anmeldung (Eintrag 6 ist entsperrt). 529 – Fehlgeschlagene Anmeldung (Eintrag 6 ist entsperrt).	✓	✓

Komponente	Ereignis	Überwachungsereignis	Erforderliche Einstellung	
FTA_TSE.1	Anmeldung fehlgeschlagen.	**Kategorie: Anmeldung** 535 – Fehlgeschlagene Anmeldung: Das angegebene Kennwort des Kontos ist abgelaufen.		✓