Aktueller Baustein - LINK zum BSI

NAME DER ORGANISATION

INFORMATIONSSICHERHEITSMANAGEMENT

101 Anforderungen dieses Bausteines sind Basis- und Standardanforderungen

Aktueller Umsetzungsstand dieser Anforderungen: 90 %

DER.3.1 Audits und Revisionen

Auditor:

Befragte:

Termine:

ERFÜLLT	TEILWEISE ERFÜLLT	NICHT ERFÜLLT	ENTBEHRLICH	RISIKOÜBERNAHME
90	2	6	1	0

Referenz	Fragen aus dem IT-Grundschutzcheck	Antworten	UMGESETZT?	ToDo-Vorschlag: WER soll WAS tun?	Empfehlung des Auditor (HPW) - in WEAKLESS unter "Notizen" zu finden
	DER.3.1.A2 Vorbereitung eines Audits oder einer Revision (B)				
U1	Vor einem Audit oder einer Revision MUSS die Institution den Prüfgegenstand und die Prüfungsziele festlegen.	Es gibt zum einen Jahresplan, der mit der Behördenleitung abgestimmt wird (welche Revisionsverfahren durchzuführen sind). Zum anderen erarbeiten die jeweiligen Revisionsteams vor der Durchführung der jeweiligen Revisionsprüfung dezidierte Konzepte und legen das Vorgehen fest.	ERFÜLLT		
U2	Die betroffenen Ansprechpartner MÜSSEN unterrichtet werden.	Zu Beginn wird das Jahresprogramm der Revision im Intranet veröffentlicht. Im Rahmen der jeweiligen Revisionsverfahren werden die betroffenen Organisationseinheiten gesondert informiert.	ERFÜLLT		Hinweis an den Informationssicherheitsbeauftragten Ins das Veröffentlichen ALLER Prüfthemen im INTRANET für ALLE sinnvoll? Bedenken Sie bitte, dass die Ansage zur Prüfung eines sensiblen Themas dem Leser u.U. auch eine Hinweis darauf gibt, dass SIE hier Zweifel oder Bedenken haben, das dort nicht alles korrekt läuft und dadurch angreifbare Defizite oder Sicherheitslücken bestehen könnten? Wir empfehlen Ihnen hier vorsichthalber das Need-to-Know-Prinzip, statt Information an "Nicht-Betroffene".

Referenz	Fragen aus dem IT-Grundschutzcheck	Antworten	UMGESETZT?	ToDo-Vorschlag: WER soll WAS tun?	Empfehlung des Auditor (HPW) - in WEAKLESS unter "Notizen" zu finden
	DER.3.1.A5 Integration in den Informationssicherheitsprozess (S)				
U1	Die Institution SOLLTE eine Richtlinie zur internen ISMS-Auditierung vorgeben.	Es gibt eine Informationssicherheits-Leitlinie, in der das ISMS als ein Punkt erwähnt und beschrieben ist.	NICHT ERFÜLLT	ToDo 7150: an den Informationssicherheitsbeauftragten 1.) Bitte erstellen Sie eine IT-Sicherheitsrichtlinie zur "internen ISMS-Auditierung" und setzen diese in Kraft. 2.) Bitte beziehen Sie dabei den Baustein DER.3.2 mit ein. 3.) Geben Sie bitte dieses Dokument in der IT allen Beschäftigten zur Kenntnis. 4.) Bitte tragen Sie hier den Speicherort dieses Dokumentes nach.	
U2	Außerdem sollte sie eine Richtlinie zur Lenkung von Korrekturmaßnahmen erstellen.	Das findet sich in der Informationssicherheits-Leitlinie wieder. Eine Richtlinie zur Lenkung von Korrekturmaßnahmen in Bezug auf Informationssicherheit existiert nicht.	NICHT ERFÜLLT	ToDo 7151: an den Informationssicherheitsbeauftragten 1.) Bitte erstellen Sie eine IT-Sicherheitsrichtlinie zur "Lenkung von Korrekturmaßnahmen" und setzen diese in Kraft. 2.) Geben Sie bitte dieses Dokument in der IT allen Beschäftigten zur Kenntnis. 3.) Bitte tragen Sie hier den Speicherort dieses Dokumentes nach.	
U3	Die Richtlinien SOLLTEN vorgeben, dass regelmäßige Audits und Revisionen ein Teil des Sicherheitsprozesses sind und durch diesen initiiert werden.	Ist in der Informationssicherheits-Leitlinie so festgelegt und ein gelebter Prozess.	NICHT ERFÜLLT	siehe ToDo 7150 und 7151	
U4	Der ISB SOLLTE sicherstellen, dass die Ergebnisse der Audits und Revisionen in das ISMS zurückfließen und dieses verbessern.	Ist auch so in der Leitlinie festgelegt.	ERFÜLLT		

Referenz	Fragen aus dem IT-Grundschutzcheck	Antworten	UMGESETZT?	ToDo-Vorschlag: WER soll WAS tun?	Empfehlung des Auditor (HPW) - in WEAKLESS unter "Notizen" zu finden
	DER.3.1.A7 Erstellung eines Auditprogramms (S)				
U1	Der ISB SOLLTE ein Auditprogramm für mehrere Jahre aufstellen, das alle durchzuführenden Audits und Revisionen erfasst.	Ist noch nicht umgesetzt, da man noch an der SOLL-IST Aufnahme arbeitet.	NICHT ERFÜLLT	ToDo 7152: an den Informationssicherheitsbeauftragten 1.) Bitte erstellen Sie für die kommenden Jahre (mind. 3) schriftlich ein Liste, die alle geplanten Audits und Revisionen in der Zeit umfasst. 2.) Bitte legen Sie diese Liste Ihrer Hausleitung und der in A2 genannten Person vor. 3.) Bitte ergänzen Sie hier, wo diese Liste abgelegt und nachvollziehbar ist.	

QS	Rückfrage an den Informationssicherheitsbeauftragten Im Laufe des Audits werden in den Antworten gleich mehrere Dokumente genannt. Wir (HPW-QS) hatten den subjektiven Eindruck, dass für ein und das selbe Dokument manchmal mehrer Bezeichnungen gewählt wurden.. Dadurch entstand gelegentlich Verwirrung. (z.B. Plan, Bericht, Richtlinie, Handbuch). Eine diesbezügliche Überprüfung der Eindeutigkeit der Bezeichnungen Durch SIE wäre sicherlich sinnvoll. - DANKE!!!

NAME DER ORGANISATION

INFORMATIONSSICHERHEITSMANAGEMENT

101 Anforderungen dieses Bausteines sind Basis- und Standardanforderungen

Aktueller Umsetzungsstand dieser Anforderungen: 90 %

DER.3.1 Audits und Revisionen

Auditor:

Befragte:

Termine:

ERFÜLLT	TEILWEISE ERFÜLLT	NICHT ERFÜLLT	ENTBEHRLICH	RISIKOÜBERNAHME
90	2	6	1	0

U2	Für das Auditprogramm SOLLTEN Ziele definiert werden, die sich insbesondere aus den Institutionszielen sowie aus den Informationssicherheitszielen ableiten.	Informationssicherheitsziele sind in der Leitlinie definiert, die später im Rahmen der Revisionen berücksichtigt werden.	TEILWEISE ERFÜLLT	siehe ToDo 7152	
U3	Der ISB SOLLTE Reserven für unvorhergesehene Ereignisse in der jährlichen Ressourcenplanung vorsehen.	Der ISB kann im Notfall Reserven zur Verfügung stellen.	ERFÜLLT		
U4	Das Auditprogramm SOLLTE einem eigenen kontinuierlichen Verbesserungsprozess unterliegen.	Es findet eine jährliche Qualitätssicherung statt, in der ermittelt wird, wo man sich noch verbessern kann.	ERFÜLLT		

Referenz	Fragen aus dem IT-Grundschutzcheck	Antworten	UMGESETZT?	ToDo-Vorschlag: WER soll WAS tun?	Empfehlung des Auditor (HPW) - in WEAKLESS unter "Notizen" zu finden
	DER.3.1.A8 Erstellung einer Revisionsliste (S)				
U1	Der ISB SOLLTE eine oder mehrere Revisionslisten pflegen, die den aktuellen Stand der Revisionsobjekte sowie die geplanten Revisionen dokumentieren.	Ist noch nicht umgesetzt, da man an der SOLL-IST Aufnahme arbeitet.	NICHT ERFÜLLT	ToDo 7153: An den Informationssicherheitsbeauftragten 1.) Bitte erstellen und pflegen Sie Revisionslisten gemäß dieser Unteranforderung.	

Referenz	Fragen aus dem IT-Grundschutzcheck	Antworten	UMGESETZT?	ToDo-Vorschlag: WER soll WAS tun?	Empfehlung des Auditor (HPW) - in WEAKLESS unter "Notizen" zu finden	
	DER.3.1.A9 Auswahl eines geeigneten Audit- oder Revisionsteams (S					
U1	Die Institution SOLLTE für jedes Audit beziehungsweise für jede Revision ein geeignetes Team zusammenstellen.	Es werden geeignete Teams (grds. bestehend aus 2 Personen) zusammengestellt.	ERFÜLLT			
U2	Es SOLLTE ein leitender Auditor (Auditteamleiter) beziehungsweise ein leitender Revisor benannt werden.	Es gibt grds. ein Zweier-Team, bestehend aus Leitende/r Revisor/in und Revisor/in.	ERFÜLLT			
U3	Dieser SOLLTE die Gesamtverantwortung für die Durchführung der Audits beziehungsweise der Revisionen tragen.	Genauso ist es und im Revisionshandbuch verankert.	ERFÜLLT			QS: Rückfrage an den Informationssicherheitsbeauftragten Wer ist der Autor dieses Dokumentes? Wo ist es nachzulesen? Ist das Revisionshandbuch das gleiche wie die in Zeile 71/72 genannte Richtlinie? Wenn ja, bitte benutzen Sie immer die gleiche Bezeichnung - DANKE!
U4	Die Größe des Audit- beziehungsweise Revisionsteams SOLLTE dem Prüfbereich entsprechen.	Das Team entspricht dem Prüfbereich.	ERFÜLLT			
U5	Die Institution SOLLTE insbesondere die Kompetenzanforderungen der Prüfthemen sowie die Größe und die örtliche Verteilung des Prüfbereichs berücksichtigen.	Diese Anforderung ist so umgesetzt.	ERFÜLLT			
U6	Die Mitglieder des Audit- beziehungsweise Revisionsteams SOLLTEN angemessen qualifiziert sein.	Die Mitglieder sind qualifiziert, die Anforderungen an das Team ist in der Richtline für die Wahrnehmung der Aufgabe der Internen Revision beschrieben (bspw. B.,VI.,4.).	ERFÜLLT			
U7	Die Neutralität des Auditteams SOLLTE sichergestellt werden.	Das ist der Richtline für die Wahrnehmung der Aufgabe der Revision beschrieben (vgl. B.,VI.,3.).	ERFÜLLT			QS: Rückfrage an den Informationssicherheitsbeauftragten Wer ist der Autor dieses Dokumentes? Wo ist es nachzulesen?
U8	Darüber hinaus SOLLTEN auch die Revisoren unabhängig sein.	Das ist der Richtline für die Wahrnehmung der Aufgabe der Revision beschrieben (vgl. B.,VI.,3.).	ERFÜLLT			QS: Rückfrage an den Informationssicherheitsbeauftragten Wer ist der Autor dieses Dokumentes? Wo ist es nachzulesen?