Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	Sicherheit Modulübergreifend
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 – Teil 6
Version:	1.3

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: de-mail@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Dieses Modul spezifiziert die Anforderungen und den Ablauf der Testierung entsprechend ISO 27001 auf der Basis von IT-Grundschutz. Es wird ein Überblick gegeben über die notwendigen Schritte zur Erstellung des konkreten IT-Sicherheitskonzepts des IT-Verbunds (Untersuchungsgegenstand).

Dieses Modul beschreibt den Nachweis über die Erbringung der Anforderungen an eine sichere De-Mail-Infrastruktur. Es richtet sich einerseits an den DMDA, indem es aufzeigt, welche Anforderungen an ihn aus der Anforderung an ein Informationssicherheitsmanagementsystem (ISMS) auf der Basis von IT-Grundschutz resultieren.

Andererseits ist auch der zertifizierte De-Mail Auditor adressiert, der die Umsetzung der Anforderungen prüfen und bestätigen muss. Für diesen werden in diesem Modul zusätzliche – über das Prüfschema für ISO 27001-Audits [Zert ISO 27001] hinausgehende – Prüfanforderungen definiert.

2 Aufbau des Moduls IT-Sicherheit

Konzeptionelle Vorgaben für die Erstellung eines Sicherheitskonzeptes sind in folgenden Dokumenten enthalten. Die Dokumente enthalten die IT-Sicherheitsziele sowie daraus abgeleitet Maßnahmen, die zwingend umgesetzt werden müssen (Vorgaben) und solche, die durch alternative Maßnahmen ersetzt werden können (empfohlene Maßnahmen).

a) Technische Richtlinie De-Mail Sicherheit Übergeordnete Komponenten [TR DM Si ÜK]
Dieses Modul enthält eine beispielhafte, technische Abbildung einer De-Mail-Infrastruktur. Der in diesem Dokument skizzierte Ansatz kann dem DMDA als Beispiel für sein Sicherheitskonzept dienen. Die Anforderungen sind analog den Anforderungen für eine ISO-27001-Zertifizierung auf der Basis von IT-Grundschutz keinesfalls vollständig und müssen an die jeweiligen individuellen Gegebenheiten angepasst werden.

Spezifische Sicherheitsaspekte einzelner De-Mail-Dienste werden in den nachfolgend benannten Modulen betrachtet:

b) Technische Richtlinie De-Mail Sicherheit Accountmanagement [TR DM ACM Si]
Es ist Bestandteil des Moduls Accountmanagement.

c) Technische Richtlinie De-Mail Sicherheit IT-Basisinfrastruktur [TR DM IT-BInfra Si]
Es ist Bestandteil des Moduls IT-Basisinfrastruktur.

d) Technische Richtlinie De-Mail Sicherheit – Postfach- und Versanddienst [TR DM PVD Si]
Es ist Bestandteil des Moduls Postfach- und Versanddienst.

e) Technische Richtlinie De-Mail Sicherheit – Dokumentenablage [TR DM DA Si]
Es ist Bestandteil des Moduls Dokumentenablage.

f) Technische Richtlinie De-Mail Sicherheit – Identitätsbestätigungsdienst [TR DM ID Si]
Es ist Bestandteil des Moduls Identitätsbestätigungsdienst.

Der Inhalt von a) bis d) ist in jedem Fall anzuwenden; hingegen ist eine Anwendung von e) bis f) nur notwendig, wenn der DMDA auch den jeweiligen Dienst tatsächlich anbietet.

3 Ablauf des Verfahrens

Im Folgenden wird der Ablauf des Testierungsverfahrens auf der Basis von IT-Grundschutz unter besonderer Berücksichtigung der Anforderungen von De-Mail beschrieben.

3.1 Fokus

Grundlage für das durch den DMDA zu erstellende IT-Sicherheitskonzept sind folgende Standards: [BSI 100-1], [BSI 100-2] und [BSI 100-3] sowie [IT-GS Katalog]. Die darin enthaltenen Standard-Sicherheitsmaßnahmen decken bei vollständiger Umsetzung den normalen Schutzbedarf ab und stellen eine Basis für die adäquate Absicherung von höherem Schutzbedarf dar.

Gegenstand dieses Abschnitts ist es, die wesentlichen Schritte aufzuzeigen, die für die Erstellung eines IT-Sicherheitskonzeptes erforderlich sind. Voraussetzung für ein Testat über die IT-Sicherheit ist die erfolgreiche Etablierung eines Informationssicherheitsmanagementsystems (ISMS) und die Umsetzung aller für den betroffenen De-Mail-Dienst erforderlichen Maßnahmen.

3.2 Etablierung eines ISMS

Die Schaffung, Aufrechterhaltung und stetige Verbesserung von Informationssicherheit ist ein kontinuierlicher Prozess. Um die notwendigen Rahmenbedingungen zu schaffen, sieht der Standard [BSI 100-1] die Einsetzung eines Informationssicherheitsmanagements als Grundlage für ein Testat zwingend vor. Dies bezieht sich verpflichtend auf den betrachteten Informationsverbund, dessen Grundlage der jeweilige De-Mail-Dienst darstellt.

Als Informationssicherheitsmanagement im Sinne dieses Standards wird dabei die Planungs- und Lenkungsaufgabe bezeichnet, die zum sinnvollen Aufbau, zur praktischen Umsetzbarkeit und zur Sicherstellung der Effektivität eines durchdachten und planmäßigen Informationssicherheits-prozesses sowie aller dafür erforderlichen Informationssicherheitsmaßnahmen notwendig ist.

Ziel des Sicherheitsmanagements ist es, das angestrebte Sicherheitsniveau zu erreichen und dieses auch dauerhaft aufrechtzuerhalten sowie zu verbessern. Daher müssen der Sicherheitsprozess und die Organisationsstrukturen für Informationssicherheit regelmäßig daraufhin überprüft werden, ob sie angemessen, wirksam und effizient sind. Ebenso ist zu überprüfen, ob die Maßnahmen des Sicherheitskonzeptes praxisnah sind und ob sie korrekt umgesetzt wurden.

3.3 Erstellung des IT-Sicherheitskonzeptes

Im Folgenden werden die einzelnen Schritte beschrieben, die notwendig sind, um ein individuelles IT-Sicherheitskonzept zur erstellen. Detaillierte Handlungsanweisungen zu diesen Schritten sind in [BSI 100-2] enthalten:

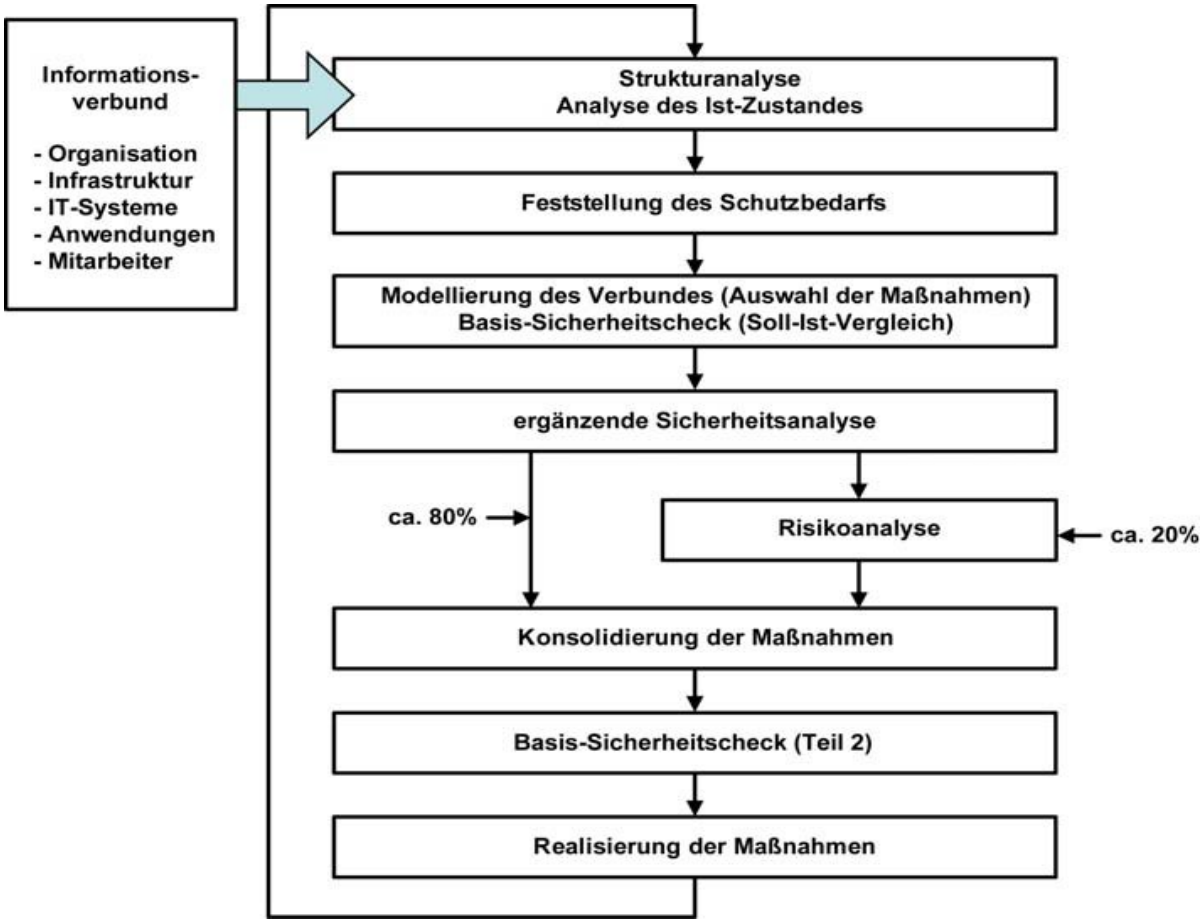

Abbildung 1: Erstellung der Sicherheitskonzeption im Informationssicherheitsmanagement (Quelle: BSI-Standard 100-2)

3.3.1 Definition des Informationsverbundes

In den Geltungsbereich fallen alle Dienste, die der DMDA im Rahmen dieses Projektes anbietet. Dazu ist durch den DMDA innerhalb des Sicherheitskonzepts der Untersuchungsgegenstand darstellen und ggf. zu anderen von ihm angebotenen Diensten abzugrenzen.

3.3.2 IT-Strukturanalyse

Im Rahmen der IT-Strukturanalyse erfolgt eine Aufnahme und Abgrenzung des zu betrachtenden IT-Verbundes. Die Analyse bezieht die vorhandene Infrastruktur, die organisatorischen und personellen Rahmenbedingungen, die eingesetzten IT-Systeme, die Kommunikationsverbindungen zwischen den IT-Systemen und nach außen sowie die im IT-Verbund betriebenen Anwendungen ein.

3.3.3 Schutzbedarfsfeststellung

Mit der Schutzbedarfsfeststellung stellt der DMDA den Schutzbedarf für die zu schützenden Objekte (IT-Anwendungen, Kommunikationsverbindungen, IT-Systeme und Infrastruktur) fest.

Angesichts der regelmäßig bei den De-Mail-Diensten verwendeten Daten ist grundsätzlich von einem hohen Schutzbedarf für die drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit auszugehen.

Der Schutzbedarf der zu schützenden Objekte ergibt sich unmittelbar aus dem Schutzbedarf, der durch die Anwendungen oder IT-Systeme transportierten, verarbeiteten und gespeicherten zu schützenden Informationen.

In der Schutzbedarfsfeststellung wird also ermittelt, welcher Schutzbedarf für die Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Dabei werden mögliche Schäden und Folgeschäden bei einer Beeinträchtigung der Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität betrachtet. Zunächst müssen Schutzbedarfskategorien definiert werden. Danach wird der Schutzbedarf der IT-Anwendungen, der IT-Systeme, der Kommunikationsverbindungen und der betroffenen IT-Räume ermittelt.

Sofern im Rahmen der notwendigen Schutzbedarfsfeststellung für einzelne Grundwerte ein sehr hoher Schutzbedarf ermittelt wird, ist insbesondere zu prüfen, welche Dienste aufgrund der konkreten Verfahrensgestaltung beim De-Mail-Diensteanbieter betroffen sind. Dies ist entsprechend im Rahmen der Sicherheits- und Risikoanalyse zu berücksichtigen. Abhängig vom Ergebnis der Sicherheits- und Risikoanalyse sind dann ggf. zusätzliche Schutzmaßnahmen bei dem jeweils betroffenen Dienst umzusetzen. Wenn Auswirkungen auf weitere Dienste im Informationsverbund nicht auszuschließen sind, ist auch für diese die Notwendigkeit der Anpassung der Maßnahmen zu prüfen.

3.3.4 Modellierung

Bei der Modellierung wird festgelegt, welche Bausteine der IT-Grundschutzkataloge auf welche Zielobjekte im betrachteten IT-Verbund angewandt werden.

Im Rahmen der Modellierung eines Informationsverbunds „De-Mail“ sind nachfolgende Bausteine zwingend umzusetzen:

- B 1.0 IT-Sicherheitsmanagement
- B 1.3 Notfallvorsorgemanagement
- B 1.7 Kryptokonzept
- B 1.8 Behandlung von Sicherheitsvorfällen
- B 1.12 Archivierung

Sofern wesentliche Bereiche des IT-Verbunds (Infrastruktur, Personal) ausgelagert werden, muss der De-Mail-Diensteanbieter folgenden IT-Grundschutzbaustein umsetzen:

- B 1.11 Outsourcing

3.3.5 Basis-Sicherheitscheck

Der Basis-Sicherheitscheck stellt die Aufnahme des tatsächlichen zum jeweiligen Prüfzeitpunkt festgestellten Sicherheitszustands dar. Dabei wird für jede Maßnahme, die in den für die Modellierung herangezogenen Bausteinen enthalten ist, der Umsetzungsstatus vermerkt: "entbehrlich", "ja", "teilweise" oder "nein". Sofern eine Maßnahme als "entbehrlich" angesehen wird, muss dies gesondert begründet werden.

3.3.6 Ergänzende Sicherheitsanalyse

Es wurde festgelegt, dass der Schutzbedarf für die Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität insgesamt hoch ist. Für alle Zielobjekte ist darüber hinaus eine ergänzende Sicherheitsanalyse zu erstellen. In dieser ist festzulegen, für welche Zielobjekte eine ergänzende Risikoanalyse durchgeführt werden muss. Dabei sind die Entscheidungen nachvollziehbar zu begründen. Zusätzlich sind in diesen Betrachtungen Zielobjekte einzubeziehen, die entweder mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet (modelliert) werden können, oder die in Einsatzszenarien betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

Für alle noch nicht durch Grundschutz abgedeckten Zielobjekte ist eine Risikoanalyse durchzuführen.

3.3.7 Risikoanalyse

Die Risikoanalyse hat die Aufgabe, relevante Gefährdungen zu identifizieren und vorhandene Risiken für die Zielobjekte abzuschätzen. Durch die geeignete Auswahl von Gegenmaßnahmen soll das Risiko auf ein vertretbares Maß gesenkt werden. Die Entscheidung, welche Bereiche in der Risikoanalyse betrachtet werden, wird durch die Leitungsebene auf Basis der ergänzenden Sicherheitsanalyse getroffen.

Für die Durchführung der Risikoanalyse kann die Vorgehensweise aus [BSI 100-3] gewählt werden. Die Risikoanalyse gliedert sich dabei in die folgenden Schritte auf:

- Erstellung der Gefährdungsübersicht,
- Ermittlung zusätzlicher Gefährdungen,
- Bewertung der ermittelten Gefährdungen,
- Behandlung der Risiken,
- Konsolidierung des Sicherheitskonzeptes und
- Rückführung in den Sicherheitsprozess.

Die Abdeckung des hohen Schutzbedarfs ist explizit zu begründen. Auch in diesem Schritt sind die durch die Technische Richtlinie De-Mail IT-Sicherheit festgelegten Bedrohungen, Sicherheitsziele und Anforderungen zwingend zu berücksichtigen. Die in der Technischen Richtlinie De-Mail IT-Sicherheit enthaltenen Empfehlungen sind dabei zu würdigen. Abweichungen sind gesondert, im IT-Sicherheitskonzept zu begründen.

Wichtig:

Im Rahmen der Modellierung sind über die Maßnahmen der jeweilig zu betrachtenden Bausteine hinaus die Anforderungen aus den jeweiligen Modulen der Technische Richtlinie De-Mail [TR DM] zu berücksichtigen.

3.3.8 Konsolidierung

Es ist davon auszugehen, dass im Rahmen der ergänzenden Sicherheitsanalyse bzw. der Risikoanalyse bezogen auf die Grundschutzkataloge zusätzliche IT-Sicherheitsmaßnahmen als notwendig erkannt werden. Daher muss eine Konsolidierung des IT-Sicherheitskonzeptes erfolgen. Das Verfahren ist in [BSI 100-3], Kapitel 7 beschrieben.

3.3.9 Ergänzender Basis-Sicherheitscheck

Als nächster Schritt wird für den IT-Verbund ein zweiter Basis-Sicherheitscheck des De-Mail-Diensteanbieters durchgeführt, um den Umsetzungsgrad der zusätzlichen bzw. geänderten Maßnahmen zu überprüfen.

3.3.10 Realisierung

Zum Ende der vorab durchgeführten Prüfungsschritte müssen die erkannten Defizite abgestellt worden sein, sodass der tatsächliche Zustand der Sicherheit der geforderten Sicherheit entspricht.

3.3.11 Penetrationstests und IS-Kurz-Revision

Das Prüfteam besteht aus vom BSI zertifizierten IS-Revisoren und Penetrationstestern oder aus Mitarbeitern des BSI.

Für den erfolgreichen Abschluss der in diesem Modul beschriebenen Testierung ist für jeden betroffenen De-Mail-Dienst ein IT-Penetrationstest sowie eine IS-Kurzrevision durchzuführen und zu dokumentieren. Dies dient der Vorabkontrolle der wesentlichen Sicherheitsmerkmale und der Feststellung grober Sicherheitsmängel. Dem DMDA soll damit die möglichst reibungslose Auditierung nach ISO 27001 auf Basis von IT-Grundschutz für De-Mail-Dienste erleichtert werden. Das diesbezügliche Vorgehen wird nachfolgend beschrieben.

Das IT-Penetrations-Testverfahren für De-Mail-Provider wird mehrstufig durchgeführt. Nach einem Web-Sicherheitsscheck ermittelt das Prüfteam auf Grundlage einer Dokumentenprüfung und einer Vor-Ort-Prüfung den Sicherheitsstatus des Providers. Betrachtet werden Prüfthemen, die eine wesentliche Grundlage für die Informationssicherheit bilden [PenTest].

Im ersten Schritt wird über das Internet die Webanwendung mittels verschiedener Tools auf Schwachstellen untersucht. Bei diesem Test geht es ausdrücklich um die Überprüfung der Sicherheitseigenschaften der Webanwendung und nicht um die Eigenschaften zusätzlich eingesetzter Sicherheitsgateways. Da Firewall-Regeln oft dynamisch im Betrieb verändert werden und alle Komponenten von Sicherheitsgateways ebenso, wie andere Systeme bei Schwachstellen ausgehebelt werden können, legt die Prüfung großen Wert darauf, dass bekannte Schwachstellen wie beispielsweise Cross-Site-Scripting oder Cross Site Request Forgery schon bei den Webanwendungen vermieden werden.

Um diese Tests durchführen zu können, ohne die Sicherheitsgateways abzuschalten, muss für das Prüfteam ein direkter Zugang zur Anwendung bestehen, der unmittelbar nach den Tests wieder entfernt werden kann. Wichtig ist, dass ein kompetenter Ansprechpartner des Providers vor Ort die Tests betreut und sie beobachtet.

Wenn der erste Web-Sicherheitscheck abgeschlossen ist, werden bei einem Vor-Ort Termin weitere Sicherheitseigenschaften getestet. Im Vorfeld der Vor-Ort-Prüfung wird die Dokumentation des Providers gesichtet, um eine Teststrategie zu entwickeln. Dazu erhält das Prüfteam Einsicht in die Dokumentation des Providers (z.B. Netzpläne, Liste der kritischen Geschäftsprozesse, IT-Sicherheitskonzept, Dokumentation der Anlage usw.). Zu Beginn der Vor-Ort-Prüfung findet ein Eröffnungsgespräch statt, in dem kurz die Vorgehensweise und die Zielrichtung der Prüfung und Tests erläutert werden. Bei der Vor-Ort-Prüfung werden Interviews geführt, die Liegenschaft begangen und die Systeme in Augenschein genommen. Das Prüfteam benötigt Shell-Zugänge zu den zu testenden Systemen, um die Konfigurationen zu überprüfen. Zur Analyse des Netzwerkverhaltens braucht das Prüfteam einen Mirror-Port an den zu testenden Stellen im Netzwerk oder die Möglichkeit, Taps anzuschließen, die bei Bedarf auch durch das Prüfteam gestellt werden können. Für Fragen zu den einzelnen Themen müssen kompetente Ansprechpartner verfügbar sein. Insbesondere sollte der IT-Sicherheitsbeauftragte das Prüfteam begleiten. Zusätzlich ist wichtig, dass ein Administrator des Providers die Tests direkt vor Ort betreut, damit Fragen geklärt werden können.

Zum Abschluss der Prüfungen und Tests wird eine Abschlussbesprechung durchgeführt. Hierbei werden die gefundenen Schwächen und Mängel präsentiert. Die Ergebnisse werden in einem Abschlussbericht zusammengefasst. Der De-Mail Provider muss bis zum Audit alle wesentlichen Mängel beseitigen und die Art und Weise der Beseitigung nachvollziehbar dokumentieren. Dieses Dokument ist dann dem zertifizierten De-Mail-Auditor zur Verfügung zu stellen.

3.4 Testat für den De-Mail IT-Verbund

Nach der Umsetzung des IT-Sicherheitskonzeptes kann ein Testat auf Basis von IT-Grundschutz bei einem zertifizierten IT-Sicherheitsdienstleister beantragt werden, der das Testat ausstellt.

Für die Durchführung von Audits eines DMDA muss ein vom BSI zertifizierter De-Mail-Auditor gewählt werden.

Im Rahmen der Auditierung müssen dem zertifizierten De-Mail-Auditor und der Testatstelle dann folgende Referenzdokumente vom Antragsteller zur Verfügung gestellt werden:

- IT-Sicherheitsrichtlinien (A.0),
- IT-Strukturanalyse (A.1),
- Schutzbedarfsfeststellung (A.2),
- Modellierung des IT-Verbundes (A.3),
- Ergebnisse des Basis-Sicherheitschecks (A.4) (optionale Vorlage bei der Testatstelle; verpflichtende Vorlage beim zertifizierten De-Mail-Auditor),
- Ergänzende Sicherheitsanalyse (A.5),
- Risikoanalyse (A.6),
- Ergebnisse der IT-Penetrationstests,
- Ergebnisse der IS-Revision.

Einzelheiten zum Verfahren sind analog zur Zertifizierung in dem Dokument [Zert ISO 27001] festgelegt und anzuwenden.

4 Ergänzende Anforderungen an den zertifizierten De-Mail-Auditor

Die für eine Auditierung von De-Mail-Diensten zu erfüllenden Voraussetzungen durch den zertifizierten De-Mail-Auditor ergeben sich aus der Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen [VB_Personen] sowie dem Programm zur Kompetenzfeststellung und Zertifizierung von Personen [Program_Personen].

Hinsichtlich der Durchführung des Audits gelten grundsätzlich die Vorgaben von [Zert ISO 27001]. Der zertifizierte De-Mail-Auditor hat darüber hinaus insbesondere auch zu prüfen, ob die Festlegungen der Schutzbedarfsfeststellung in Übereinstimmung mit diesem Modul und [TR DM Si ÜK] erfolgt sind. Das Ergebnis dieser Prüfung ist gesondert darzustellen.

Zudem hat der zertifizierte De-Mail-Auditor zu überprüfen, ob bei der Durchführung der ergänzenden Sicherheitsanalyse und der Risikoanalyse die in den relevanten Teilen der Technischen Richtlinie De-Mail IT-Sicherheit festgelegten Sicherheitsziele und zwingenden Vorgaben beachtet und umgesetzt wurden. Das Ergebnis dieser Prüfungen ist explizit darzustellen.

In einigen der zwingenden Anforderungen ist daneben festgelegt, dass für die eingesetzten Produkte eine hinreichende Güte durch eine entsprechende Sicherheitszertifizierung nachgewiesen werden muss. Durch den zertifizierten De-Mail-Auditor ist daher zu prüfen, ob für die eingesetzten Produkte entsprechende Sicherheitszertifikate vorliegen und ob die Anforderungen an die Einsatzumgebung, die der Produktzertifizierung zugrunde liegen, eingehalten werden. Das Ergebnis dieser Prüfung ist darzustellen.

Für die Dokumentation der beschriebenen Zusatzprüfung ist wird dem zertifizierten De-Mail-Auditor ein Musterauditreport zur Verfügung gestellt, den der zertifizierte De-Mail-Auditor beim BSI anfordern kann.