Prüfstelle
Organismo di valutazione
Organn de valutazion

Informationssicherheitsmanagement in der Landesverwaltung

Südtiroler Landtag
Consiglio della Provincia autonoma di Bolzano
Cunsëi dla Provinzia autonoma de Bulsan

PRÜFER Martin Steinmann (bis 9.7.2021)
Wolfgang Bauer

PRÜFSTELLE
ORGANISMO DI VALUTAZIONE

39100 Bozen | Freiheitsstraße 66
39100 Bolzano | Corso Libertà, 66

Tel. 0471 402 212 | Fax 0471 260 114
pruefstelle@landtag-bz.org | organismodivalutazione@consiglio-bz.org
www.landtag-bz.org/de/pruefstelle.asp
www.consiglio-bz.org/it/organismo-di-valutazione.asp
PEC: pruefstelle.organismovalutazione@pec.prov-bz.org

September 2021

INHALT

I. BEGRÜNDUNG UND ZIEL DER ERHEBUNG ZUM INFORMATIONSSICHERHEITSMANAGEMENT IN DER LANDESVERWALTUNG ---4

II. UMFANG UND METHODISCHER ANSATZ ----------4

III. SACHVERHALTSDARSTELLUNG ----------5

IV. BEWERTUNG UND EMPFEHLUNGEN----------9

I. Begründung und Ziel der Erhebung zum Informationssicherheitsmanagement in der Landesverwaltung

Im Sinne von Art. 24, Abs. 1, Buchstabe a) des LG Nr. 10/1992 in geltender Fassung überwacht die Prüfstelle die Funktionsweise des Systems der internen Kontrollen (IKS) innerhalb der Landesverwaltung.
Diese Prüftätigkeit ist in den entsprechenden Berichten[1] dokumentiert.

In das Arbeitsprogramm 2021 wurde - aufgrund der strategischen und transversalen[2] Bedeutung des Themas[3] - eine Erhebung zum Informationssicherheitsmanagement in der Landesverwaltung aufgenommen.

Ziel der Erhebung ist eine Bestandsaufnahme und Evaluierung der Funktionsweise des Systems der internen Kontrollen im Bereich des Informationssicherheitsmanagements, indem Aspekte aus dem IT-Grundschutz betrachtet und bewertet werden.

II. Umfang und methodischer Ansatz

Der Fokus der Erhebung ist auf das System der IT-Informationssicherheit gerichtet, welches sowohl die Governance als auch operative Aspekte berücksichtigt; nachdem es sich um eine System- und Organisationsprüfung handelt, werden rein technische Aspekte nicht eingehender erhoben.

Für die Erhebung wird auf die fünf Komponenten des IKS nach dem COSO-Modell[4] Bezug genommen:
-*Kontrollumfeld,*
-*Risikobeurteilung,*
-*Kontrolltätigkeiten,*
-*Information und Kommunikation,*
-*Monitoring*.

Besonders in der IT-Sicherheit sind das Kontrollumfeld und die Definition von Sicherheitszielen, die Bewertung des Risikos und die Ergreifung entsprechender Maßnahmen von grundlegender Bedeutung. Ebenso stellen die Kommunikation, nach innen aber auch nach außen, sowie ein konstantes Monitoring wichtige Bestandteile eines funktionierenden IKS-Modells dar.

---

[1] Veröffentlicht auf der Homepage der Prüfstelle: https://www.landtag-bz.org/de/pruefstelle.asp

[2] Laut dem staatlichen Dreijahresplan für die Informatik in der öffentlichen Verwaltung (2020 – 2022) ist die Informationssicherheit ein transversales Thema in der staatlichen Strategie für die technologische Innovation und die Digitalisierung, S. 48.

[3] Das Thema Sicherheit spielt auch im Zusammenhang mit der Aktivierung von Smart-Working-Modellen zunehmend eine wichtige Rolle.

[4] COSO: Committee of Sponsoring Organizations of the Treadway Commission; das weltweit anerkannte Modell hat verschiedene Konzepte und Definitionen der Internen Kontrolle in einem Grundlagenkonzept vereint.

Grundlage der Erhebung bildet ein ausführlicher an die Abteilung Informationstechnik gerichteter Fragenkatalog, welcher die folgenden Themenfelder schwerpunktmäßig aufgreift: **Sicherheitsmanagement, Organisation und Personal, Infrastruktur, IT-Systeme, Netzwerke und Anwendungen.**[5]

III. Sachverhaltsdarstellung[6]

Sicherheitsmanagement

*Als **Informationssicherheitsmanagement**[7] (ISM) wird die Planungs-, Lenkungs- und Kontrollaufgabe definiert, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen. Dabei spielt der Informationssicherheitsbeauftragte eine zentrale Rolle, indem er gewährleistet, dass die IT-Systeme der Organisation jederzeit angemessen geschützt sind und somit das angestrebte Niveau in der Datensicherheit sowie Informationssicherheit erreicht und aufrechterhalten wird.*

Auf die Frage, ob ein **Informationssicherheitsbeauftragter** namhaft gemacht wurde, teilt die Abteilung Informationstechnik mit, dass in der Südtiroler Informatik AG (in der Folge: SIAG)[8] diese Figur im Jahre 2018 formell nominiert wurde, während für die Abteilung im Jahr 2001 eine Nominierung erfolgt ist, die allerdings nicht erneuert wurde. Auf Nachfrage erläutert die Abteilung, dass bis zum Abschluss des eben erst eingeleiteten Organisationsentwicklungsprozesses, welcher auch die Rolle des Informationssicherheitsbeauftragten betreffen wird, die Aufgaben der Planung, Koordinierung und des Monitorings der Informationssicherheit vom Verantwortlichen[9] für die digitale Transformation, unterstützt durch die 2001 namhaft gemachte Mitarbeiterin, wahrgenommen werden.

Eine von der Landesregierung erlassene umfassende **Sicherheitsleitlinie**, in der Bedeutung und Organisationsstruktur für die Informationssicherheit geregelt werden, existiert nicht als eigenständiges Grundsatzdokument; laut Auskunft der Abteilung hält sich die SIAG, Informationssicherheitsziele und Sicherheitsstrategie betreffend, an die im staatlichen Dreijahresplan für die Informatik (Kapitel 6)[10] enthaltenen Vorgaben.

Die Abteilung Informationstechnik bestätigt, dass ein aktuelles **Sicherheitskonzept** zur Umsetzung der Sicherheitsstrategie, das alle Geschäftsprozesse und Anwendungen umfänglich abbildet und die Vorgehensweise zur Erreichung der Sicherheitsziele beschreibt, zur Anwendung gelangt; entsprechend erfolgten Risikoeinstufung und Risikobehandlung, welche ständig aktualisiert wird.

Was den **Risikomanagementplan** betrifft, erläutert die Abteilung, dass zur formellen Abbildung sämtlicher Aktivitäten eine webbasierte Plattform von AGID (Agenzia per l'Italia digitale) verwendet

---

[5] Wichtigste Quellen und Bezugsdokumente für die vorliegende Erhebung: Bundesamt für Sicherheit in der Informationstechnik (BSI); Agenzia per l'Italia digitale (AGID); Klaus-Rainer Müller, IT-Sicherheit mit System, Springer Vieweg, 2018.

[6] Die im nachfolgenden Text enthaltenen Begriffsbestimmungen sind im Wesentlichen dem IT-Grundschutzkompendium und verschiedenen Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entnommen: https://www.bsi.bund.de/DE/Home/home_node.html

[7] Das Informationssicherheitsmanagement (ISM) ist zentrales Thema der ISO/IEC-27000-Familie.

[8] Zur Ausübung der Governance gegenüber der SIAG s. Bericht der Prüfstelle „Gesetzmäßigkeit, Unparteilichkeit und reibungslose Abwicklung der Verwaltungstätigkeit", Februar 2018.

[9] Der Verantwortliche für die digitale Transformation laut Art. 17 des Kodex für die digitale Verwaltung (CAD) wurde mit Beschluss der Landesregierung Nr. 85/2018 namhaft gemacht.

[10] https://pianotriennale-ict.italia.it/piano/; einschlägig ist außerdem das Rundschreiben der AGID Nr. 2/2017 betreffend Mindestmaßnahmen zur Informationssicherheit in den öffentlichen Verwaltungen.

wird, welche ein Risikomanagement-Framework auf der Grundlage von IRAM2 (Information Risk Analyse Methodology) und ISO 31000 (Risikomanagement-Leitlinien) implementiert.

Zusätzlich zum **Kommunikationsplan bei Notfällen** kommt im Falle eines Datenmissbrauchs (Data Breach) in der Landesverwaltung und in der SIAG ein eigenes Verfahren im Sinne der Datenschutzgrundverordnung zur Anwendung. Diese Verfahren wurde zwischen Abteilung und SIAG sowie den entsprechenden Datenschutzverantwortlichen abgestimmt und soll laut Abteilung noch heuer (oder spätestens 2022 nach Abschluss des erwähnten Organisationsentwicklungsprozesses) als Anlage zum neuen Rahmenabkommen zwischen Landesverwaltung und SIAG unterzeichnet werden.

Zur Überprüfung des **Status der Informationssicherheit** werden regelmäßige Maßnahmen wie Penetrationstests und Schwachstellenanalysen (Vulnerability Assessments) durchgeführt. Außerdem gibt es neben dem externen Auditor für die Überprüfung nach Standard ISO 27001 eine interne Auditfunktion; diese ist formell unabhängig und führt regelmäßig Sicherheitsrevisionen unter Beachtung von Standard ISO 27001 durch.

Die Abteilung bestätigt, dass **Sicherheitsvorfälle** erkannt, kontrolliert bearbeitet, dokumentiert und nachbearbeitet werden (Behandlung der Sicherheitsvorfälle nach ISO 9001 und ISO 27001).

Auch das **Datensicherungskonzept** und die regelmäßigen **Wiederherstellungstests** orientieren sich an Standard ISO 27001.

Das **Sicherheitskonzept** umfasst auch externe **Cloud-Dienste**; dies ist auch durch die Vorgaben von AGID im Bereich der IKT-Beschaffungen gewährleistet.

Das **Informationssicherheitsmanagement ist nach ISO 27001 zertifiziert**; die ausschließlich SIAG betreffende Zertifizierung wurde erst kürzlich (Juni 2021) nach einem externen Audit erneuert; die dabei ausgesprochenen Bemerkungen und Empfehlungen wurden im Rahmen punktueller Aktivitäten und Fristen bereits berücksichtigt bzw. umgesetzt.[11]

Organisation und Personal

*Allgemeine und übergreifende Anforderungen im Bereich **Organisation** sollen dazu beitragen, das Niveau der Informationssicherheit zu erhöhen. In diesem Zusammenhang sind Informationsflüsse, Prozesse, Rollenverteilungen sowie die Aufbau- und Ablauforganisation zu regeln.*
*Die **Mitarbeiter:innen** haben die wichtige Aufgabe, Informationssicherheit umzusetzen; sie sollen daher systematisch und zielgruppengerecht zu Sicherheitsrisiken sensibilisiert[12] und zu Fragen der Informationssicherheit geschult werden.*

Einstellungen, Dienstaustritte und organisatorische Veränderungen von Mitarbeiter:innen werden formell über das Tool ITSM (IT-Service Management) Ky2Help zwischen Personalabteilung und IT kommuniziert; über einen Workflow, der den Führungskräften und internen Benutzerbetreuer:innen zu Verfügung steht, werden auch die Anmeldeinformationen der Bediensteten der Landesverwaltung (Bereitstellung, Aufhebung der Bereitstellung/Provisioning, Deprovisioning) mitgeteilt. In Hinblick auf eine vollständige Automatisierung wird die Vernetzung zwischen Personalabteilung und SAP/AS400 überprüft.

[11] Zur Bedeutung der Zertifizierung des ISM-Systems: BSI-Standard 200-1, Kapitel 9.

[12] Zum Thema Sicherheitsbewusstsein und Sicherheitskultur: Cybersecurity-Audits – Bedeutung und Messung der Informationssicherheits-Awareness, in ZIR 01.21, S. 16 ff.; staatlicher Dreijahresplan für die Informatik in der öffentlichen Verwaltung (2020 – 2022), S. 46.

Sicherheitsprüfungen bei neu eintretenden Mitarbeiter:innen im Informatikbereich werden laut Abteilung nicht durchgeführt.

Die erwähnte **Schulung und Sensibilisierung** aller Mitarbeiter:innen zum Thema Informationssicherheit erfolgt im Rahmen eines Weiterbildungsprogramms auf der Grundlage von E-Learning, Fragebögen und simulierten Angriffen. Auf die Frage, ob die Ergebnisse der Schulung evaluiert werden, erklärt die Abteilung, dass die Lernplattform über einige Instrumente verfügt, die nach Abschluss der Schulung implementiert werden, um die Reaktionen der Mitarbeiter:innen (z. B. auf Pishing-E-Mails) konkret zu prüfen. Zur Frage, wie die Ausprägung des Risiko- und Sicherheitsbewusstseins bei den Führungskräften und den Mitarbeiter:innen der Landesverwaltung generell eingeschätzt wird, äußert sich die Abteilung nicht.

Für die Planung und Durchführung von **Änderungen an der IT-Architektur**[13] findet ein formelles Verfahren im Rahmen des Systems ITSM Ky2Help Anwendung.

Die Abteilung bestätigt, dass bei **Verträgen im IT-Bereich** sicherheitsrelevante Aspekte berücksichtigt, dokumentiert und überprüft werden, indem die einschlägigen Leitlinien der AGID (s. oben) im Bereich der IKT-Beschaffungen genau umgesetzt werden.

Infrastruktur

*Unter **Infrastruktur** werden die für die Informationsverarbeitung und die IT genutzten Gebäude, Räume, Energieversorgung, Klimatisierung und die Verkabelung verstanden (nicht dazu gehören die IT-Systeme und Netzkoppelelemente wie z.B. Router).*

Durch Mechanismen der Authentisierung und Autorisierung, welche für physische und logische Zugänge implementiert werden, stellt die Abteilung Informationstechnik sicher, dass der **Zutritt zur IT-Infrastruktur** durch unbefugte Personen verhindert oder überwacht wird.

Besucher unterliegen einer Registrierungspflicht und dürfen sich nicht unbegleitet bewegen, für **externes Personal** (z. B. Reinigungspersonal) sind Badges für den physischen Zutritt zu internen Räumlichkeiten erforderlich.

Die Abteilung bestätigt das Vorliegen eines **Brandschutzkonzepts** für die Rechnerräume, welches den geltenden Bestimmungen entspricht.

Ebenso wird die angemessene **Klimatisierung** von Serverräumen, Räumen für technische Infrastruktur (z. B. Verteilerräume) und Rechenzentrum bestätigt, einschließlich automatischer Hinweise im Falle von Anomalien; dasselbe gilt für die automatisierte Überwachung der **Umgebungsparameter** (wie Temperatur, Luftfeuchtigkeit).

Maßnahmen zur **Fortführung des IT-Betriebes bei Stromausfall** sind innerhalb der SIAG gewährleistet (unterbrechungsfreie Stromversorgung - USV, Notstrom-Aggregat). Auch die Wirkungskette aller Maßnahmen bei Stromausfall wird im Rahmen von Tests regelmäßig auf ihre Wirksamkeit geprüft.

Schließlich bestätigt die Abteilung, dass eine umfassende **Dokumentation der elektrischen und IT-**

[13] Mit dem Begriff IT-Architektur werden verschiedene Aspekte der Informationstechnik (IT) in einer Organisation bezeichnet, z. B. die Entwicklung von methodischen IT-Spezifikationen, Modellen und Guidelines. Dies dient dem Ziel, ein kohärentes IT-Architektur-Framework zu entwickeln (aus: Wikipedia, September 2021).

Verkabelung samt Trassenführung im System ITSM vorhanden bzw. abgebildet ist.

IT-Systeme

IT-Systeme *sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Mobiltelefone, Smartphones, Tablets, IoT-Komponenten, Router, Switches und Firewalls.*

Die Abteilung Informationstechnik bestätigt, dass alle IT-Systeme grundsätzlich nach dem **Minimalprinzip** konfiguriert werden; dies bedeutet, dass nur die Funktionen und Informationen zur Verfügung gestellt werden, welche zur Fortführung der Geschäftstätigkeit unbedingt erforderlich sind.

Betriebssysteme und Anwendungen werden regelmäßig aktualisiert; außerdem werden periodisch (mindestens ein Mal im Jahr) Prüfungen/Tests im Rahmen des Patch Managements[14] durchgeführt.

Eine eigene Policy für die Nutzung von **Multifunktionsgeräten** regelt das Verfahren bei Defekt oder Rückgabe und stellt sicher, dass sie über nichtflüchtige Datenspeicher verfügen.

Was die Nutzung **mobiler Endgeräte** betrifft, wird (vorerst) nicht sichergestellt, dass diese angemessen verschlüsselt sind; eine diesbezügliche Neubewertung ist geplant.

Das Regelwerk der **Sicherheitsgateways[15]** ist nachvollziehbar dokumentiert, alle Aktivitäten sind im ITSM-System aufgezeichnet. Auch werden Sicherheitsgateways regelmäßig auf ihre korrekte Funktionsfähigkeit hin geprüft.

Netzwerke

Ein zuverlässiges ***Netzmanagement*** *ist Grundvoraussetzung für den sicheren und effizienten Betrieb moderner Netze. Dazu ist es erforderlich, dass das Netzmanagement alle Netzkomponenten umfassend integriert. Durch geeignete Maßnahmen werden Netzmanagement-Kommunikation und -infrastruktur geschützt.*

Aktuelle und vollständige **Netzpläne** (graphische Übersicht über die Komponenten eines Netzes und ihre Verbindungen) sind laut Aussage der Abteilung vorhanden und offiziell dokumentiert.

Das **System- und Netzwerkmanagementsystem** gewährleistet die automatisierte Überwachung kritischer IT-Systeme und Netzwerkkomponenten durch das System SolarWinds sowie die Auswertung der Ereignisprotokolle.

Die Netzkomponenten werden nach dem **Minimalprinzip** konfiguriert; laut Abteilung wird vor der Implementierung generell eine Angemessenheits- und Sicherheitsanalyse der Konfigurationen vorgenommen. Die **Konfiguration** der Netzkomponenten ist **nachvollziehbar dokumentiert**.

Alle **Zugänge zu LAN/WLAN** werden kontrolliert und monitoriert; der Zugang fremder Endgeräte ist

[14] Das Patch Management beschäftigt sich mit der Beschaffung, dem Test und der Installation benötigter Updates für Applikationen, Treiber und Betriebssystem von Computern.

[15] Ein Sicherheitsgateway (oft auch Firewall genannt) ist ein System aus soft- und hardware-technischen Komponenten, das die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer Sicherheitsrichtlinie als ordnungsgemäß definierte Kommunikation gewährleistet.

einzig und allein über VPN (Virtual Private Network) möglich.

Anwendungen

Zur **Nutzung nicht dienstlicher mobiler Datenträger** teilt die Abteilung mit, dass es zwar eine entsprechende Regelung gibt, bisher aber keine Technologien implementiert wurden, um die Nutzung zu beschränken.

Für die **dienstliche und private Nutzung von Internet und E-Mail** gibt es sowohl in der Landesverwaltung[16] als auch in der SIAG eine eigene Regelung.

IV. Bewertung und Empfehlungen

Informationssicherheitsmanagement ist ein **kontinuierlicher Prozess**[17], dessen Strategien und Konzepte ständig auf ihre Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind. Dafür sind Sicherheitsschwerpunkte und -ziele sowie die Risikotragfähigkeit und -bereitschaft ausreichend und verbindlich zu definieren.[18]

In Hinblick auf ein anschauliches, umfassendes und durchgängiges Vorgehensmodell[19] dafür, wie das Sicherheits-, Kontinuitäts- und Risikomanagement in der Landesverwaltung strategisch, systematisch, zielorientiert, konsistent und effizient betrieben und weiterentwickelt werden soll, wird die grundsätzliche Empfehlung ausgesprochen, im Sinne der Transparenz und Nachvollziehbarkeit den **Sicherheitsmanagementprozess** zu beschreiben und also entsprechend zu formalisieren.

Da sich die Sicherheitsanforderungen kontinuierlich verändern („Sicherheit ist ein bewegliches Ziel"), sollte der Sicherheitsmanagementprozess auch einen kontinuierlichen Verbesserungsprozess enthalten; dafür bietet sich beispielsweise der aus dem Qualitätsmanagement bekannte PDCA-Zyklus an.[20]

Um die angestrebten Informationssicherheitsziele und die verfolgte Sicherheitsstrategie spezifisch für die Landesverwaltung zu definieren, wird die formelle Festlegung einer **Sicherheitsleitlinie** - unbeschadet der AGID-Vorgaben - empfohlen.

Die formelle Nominierung des **Informationssicherheitsbeauftragten** sollte spätestens nach Abschluss des Organisationsentwicklungsprozesses der Abteilung vorgenommen werden.

Die für das Sicherheits-, Kontinuitäts- und Risikomanagement im Jahr 2020 eingesetzten **Personal- und Finanzressourcen** belaufen sich laut Abteilung auf eine Million Euro für Sicherheitstechnologien (70% davon für die Implementierung des neuen Data Center in Bruneck) sowie eine VZÄ-Ressource,

[16] https://www.provinz.bz.it/verwaltung/personal/personal-landesdienst/personalentwicklung-weiterbildung/willkommenspaket/pc-arbeitsplatz.asp

[17] Der Sicherheitsprozess nach BSI-Standard 200-2 besteht aus den Phasen: Initiierung des Sicherheitsprozesses, Erstellung der Leitlinie zur Informationssicherheit, Aufbau einer geeigneten Organisationsstruktur für das ISM, Erstellung und Umsetzung einer Sicherheitskonzeption, Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit.

[18] Klaus-Rainer Müller, IT-Sicherheit mit System, Springer Vieweg, S. 17.

[19] Ebenda: Klaus-Rainer Müller, IT-Sicherheit mit System, Springer Vieweg, S. 17.

[20] Ebenda: Klaus-Rainer Müller, IT-Sicherheit mit System, Springer Vieweg, S. 723.

welche sich ausschließlich dem Risikomanagement (einschließlich Kontinuitätsplänen und Notfallwiederherstellung) widmet. Ob dieser Ressourceneinsatz angesichts der Dimension der Landesverwaltung mit mehreren Tausend Mitarbeiter:innen und der Anzahl der IT-Systeme ausreichend bzw. angemessen ist, sollte von den verantwortlichen Führungskräften kritisch überprüft werden.[21]

Besonderes Augenmerk sollte auf eine starke **Ausprägung des Risiko- und Sicherheitsbewusstseins** bei Führungskräften und Mitarbeiter:innen gelegt werden, da Gefährdungen nicht ausschließlich technischer Natur sind oder durch vorsätzliches Handeln entstehen, sondern potenzielles Unwissen oder Fahrlässigkeit von Mitarbeitenden innerhalb der Verwaltung auch ein erhebliches Bedrohungspotenzial in sich bergen können.[22]

Der **IKS-Reifegrad[23] des Sicherheits-, Kontinuitäts- und Risikomanagements** in der Landesverwaltung erscheint - im Rahmen einer allgemeinen Einschätzung auf der Grundlage der Ergebnisse der vorliegenden Erhebung zu den schwerpunktmäßig aufgegriffenen Themenfeldern Sicherheitsmanagement, Organisation und Personal, Infrastruktur, IT-Systeme, Netzwerke und Anwendungen - insgesamt gut ausgeprägt.

Ein Follow-up zu den ausgesprochenen Empfehlungen und Anregungen wird Ende 2022 erfolgen.

Abschließend sei dem Direktor der Abteilung Informationstechnik und seinen Mitarbeiter:innen für die konstruktive Zusammenarbeit im Zuge der Erhebung gedankt.

Wolfgang Bauer
Firmato digitalmente da:Wolfgang Bauer
Data:08/10/2021 09:13:48

[21] Laut „2015 Global Study on IT Security Spending & Investments“ des Ponemon Institute vom Mai 2015 ordnen die befragten Unternehmen aus insgesamt 42 Ländern ca. 8,2 % des IT-Budgets der IT-Security zu. Ebenda: Klaus-Rainer Müller, IT-Sicherheit mit System, Springer Vieweg, S. 23.

[22] S. Fn 9, S.26. Ziele und erwartete Ergebnisse bei der Stärkung der Cyber Security Awareness werden auch im erwähnten Dreijahresplan für die Informatik definiert.

[23] Zur Reifegradbestimmung der IT-Sicherheit existieren verschiedene Systeme bzw. Modelle. S. auch: Reifegradmodell des Sicherheits-, Kontinuitäts- und Risikomanagements in Klaus-Rainer Müller, IT-Sicherheit mit System, Springer Vieweg, S. 713 ff.

Südtiroler Landtag
Consiglio della Provincia autonoma di Bolzano
Cunsëi dla Provinzia autonoma de Bulsan

Prüfstelle
39100 Bozen | Freiheitsstraße 66
Organismo di valutazione
39100 Bolzano | Corso Libertà, 66

Tel. 0471 402 212 | Fax 0471 260 114
pruefstelle@landtag-bz.org | organismodivalutazione@consiglio-bz.org
PEC: pruefstelle.organismovalutazione@pec.prov-bz.org
www.landtag-bz.org/de/pruefstelle.asp
www.consiglio-bz.org/it/organismo-di-valutazione.asp