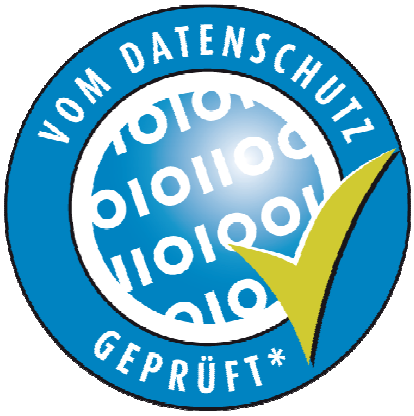

Kurzgutachten

Auditverfahren gemäß § 43 Abs. 2 LDSG

Dataport

Informationssicherheits-Managementsystem (ISMS)

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Datum : 27.08.2007
Aktenz. : 16.01/07.006
Telefon : 0431 988 1200
Fax : 0431 988 1223
E-Mail : mail@datenschutzzentrum.de

Inhaltsverzeichnis

1 Gegenstand des Datenschutz-Audits

Das Unabhängige Landeszentrum für Datenschutz (ULD) und Dataport haben vereinbart, die „**Konzeption** eines **Informationssicherheits-Managementsystems**“ (ISMS) für das Rechenzentrum Dataport am Standort Altenholz auf der Basis des **IT-Grundschutzstandards** des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu auditieren. Die einzelnen Dokumente der Konzeption wurden inhaltlich im Rahmen des Datenschutz-Audits auf ihre Norm- und Rechtskonformität sowie ihre Umsetzbarkeit überprüft. Das Konzept ist für einzelne Fachverfahren bereits umgesetzt, so dass es insoweit auch auf seine Wirksamkeit überprüft werden konnte.

Dataport setzt in seinem Rechenzentrum den IT-Grundschutzstandard des BSI um. Die Konzeptinhalte für das ISMS sind deshalb neben der Berücksichtigung **datenschutzrechtlicher Vorschriften** auch nach den Regelungen des **IT-Grundschutzstandards** ausgerichtet. Es wurde während der Begutachtung besonders auf die Einhaltung folgender Bausteine der BSI-Grundschutzkataloge geachtet:

- B 1.0 IT-Sicherheitsmanagement
- B 1.1 Organisation
- B 1.2 Personal
- B 1.8 Behandlung von Sicherheitsvorfällen
- B 1.13 IT-Sicherheitssensibilisierung und -schulung

Dataport hat während der **Planung** und **Realisierung** des ISMS folgende **Datenschutzziele** festgelegt:

- Beachtung von Rechtsvorschriften, Richtlinien und sonstigen Arbeitsanweisungen zur **Datensicherheit** und zur **Ordnungsmäßigkeit** der Datenverarbeitung,
- Einhaltung der in der Dataport **IT-Sicherheitsleitlinie** festgelegten Sicherheitsziele und die damit verbundene Gewährleistung der Umsetzung des festgelegten **Sicherheitsniveaus**,
- Einrichtung einer **IT-Sicherheitsorganisation** durch die Festlegung von Zuständigkeiten sowie die Abgrenzung der Verantwortung der beteiligten Personen,

- Umsetzung von **IT-Sicherheitsstandards** durch die Ausgestaltung der für das ISMS erforderlichen technischen und organisatorischen Maßnahmen,
- Einführung von **IT-Sicherheitsprozessen** für die Aufrechterhaltung des festgelegten Sicherheitsniveaus durch die Anpassung der aufbau- und ablauforganisatorischen Strukturen,
- Erarbeitung eines übergreifenden **IT-Sicherheitskonzepts** nach den Vorgaben der BSI-Standards 100-1, 100-2 und 100-3[1].
- Schaffung geeigneter und einheitlicher **Schnittstellen** zum Sicherheitsmanagement des Kunden,
- revisionssichere **Kontrolle** der festgelegten Sicherheitsmaßnahmen,

Mit der **Planung** und **Umsetzung** der für das ISMS festgelegten Ziele hat Dataport die **Stabsstelle** Datenschutz, Revision und Justiziariat betraut.

Zur Konzeption des ISMS gehören nachfolgend vorgelegte Unterlagen. Sie sind **Gegenstand des Audits** und wurden einer ausführlichen **Begutachtung** unterzogen (siehe Tz. 2):

- Einsatzverfügung für das Projekt „Einführung eines ISMS“ bei Dataport
- IT-Sicherheitsleitlinie
- Datenschutz-Merkblatt
- Datenschutzleitlinie
- IT-Sicherheits- und Datenschutz-Managementhandbuch
- Personalmanagementhandbuch
- Schulungskonzept „IT-Sicherheit“
- Handbuch für den Einsatz des GSTools
- Organisationshandbuch

[1] Siehe http://www.bsi.de/literat/bsi_standard/index.htm

- Reports der Maßnahmenumsetzung aus dem GSTool (B 1.0 IT-Sicherheitsmanagement, B 1.1 Organisation, B 1.2 Personal, B 1.8 Behandlung von Sicherheitsvorfällen, B 1.13 IT-Sicherheitssensibilisierung und –schulung)
- Security Management und ITSM
- Rollen im Sicherheitsvorfallmanagement

2 Feststellung zu den sicherheitstechnischen Elementen des ISMS

2.1 Einsetzungsverfügung für das Projekt „Einführung eines ISMS“ bei Dataport

Dataport steht vor der Herausforderung, **Datenschutz und Datensicherheit** nicht nur im eigenen Verantwortungsbereich umsetzen zu müssen. Vielmehr ist Dataport verpflichtet, seine Kunden bei der Umsetzung des Datenschutzes im Rahmen seiner Auftragsdatenverarbeitung zu unterstützen. Dabei muss sich Dataport jeweils auf unterschiedliche Rechtsgrundlagen seiner Auftraggeber, u.a. vier Landesdatenschutzgesetze und zahlreicher bereichsspezifischer Regelungen, einstellen.

Der Vorstand von Dataport hat eine **Einsetzungsverfügung** für das Projekt „Einführung eines ISMS“ mit folgenden Inhalten unterzeichnet:

1. Mit der Entwicklung und Installation eines ISMS sind die Vorraussetzungen für eine dauerhafte und angemessene IT-Sicherheit zu schaffen.
2. Es ist eine IT-Sicherheitspolitik umzusetzen, die u.a. Sicherheitsziele vorgibt, Organisationsstrukturen für das ISMS enthält, Aufgaben und Verantwortlichkeiten festlegt und den IT-Sicherheitsprozess beschreibt.
3. Mit der Einführung des ISMS sind Rollen und Funktionen festzulegen und auf Mitarbeiter zu übertragen sowie IT-Sicherheitsrichtlinien zu erarbeiten.
4. Es ist ein IT-Sicherheitskonzept unter der Einhaltung des BSI-Standards zu erstellen.
5. Mitarbeiter sind in Bezug auf IT-Sicherheit zu sensibilisieren und zu schulen.

Die Einführung des ISMS ist an den **Standorten** Altenholz, Hamburg, Bremen und Rostock vorgesehen.

Dataport richtet derzeit den IT-Betrieb des Rechenzentrums an der **IT Infrastructure Library** (ITIL)[2] aus. ITIL wird vom britischen Office for Government Commerce (OGC)[3] entwickelt und verfügt in der Version 2.0 über eine Sammlung von 10 Musterprozessen (Good-Practice-Prozessen) für den IT-Betrieb.

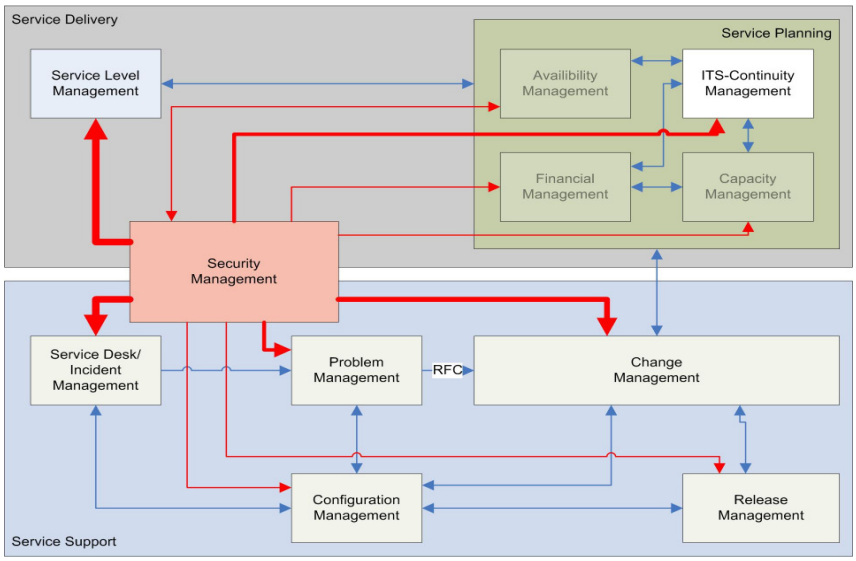

Abb.: ITIL-Prozesse

Dataport hat sein **ISMS** unter der Einbeziehung der **ITIL-Prozesse** auf Basis der Norm ISO 27001 (Information Security Management Systems, ISMS), den zugehörigen BSI-Standards BSI 100-1 bis BSI 100-3 und den IT-Grundschutz-Katalogen[4] ausgerichtet. Gleichzeitig wurden die einschlägigen Publikationen des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[5] und der KBSt[6] zur Integration von IT-Grundschutz und ITIL berücksichtigt.

---

[2] Siehe http://www.itil-officialsite.com/home/home.asp

[3] Siehe http://www.ogc.gov.uk/

[4] Siehe http://www.bsi.de/gshb/deutsch/index.htm

[5] Siehe http://www.bsi.de/literat/studien/ITinf/itil.pdf

[6] Siehe http://www.kbst.bund.de/cln_046/nn_836802/SharedDocs/Anlagen-kbst/itil__und__informationssicherheit,templateId=raw,property=publicationFile.pdf/itil_und_informationssicherheit.pdf

2.2 Konzeption des ISMS

2.2.1 IT-Sicherheitsleitlinie

Die IT-Sicherheitsleitlinie bildet die **Grundlage** für die Herstellung und den Erhalt des erforderlichen **Sicherheitsniveaus** für alle IT-Ressourcen im Verantwortungsbereich von Dataport. Sie schafft und erhält das Bewusstsein der Mitarbeiterinnen und Mitarbeiter für die IT-Sicherheit und legt die **IT-Sicherheitsstrategie** von Dataport fest.

Für das ISMS bildet die IT-Sicherheitsleitlinie eine **verbindliche interne Regelung** für die Einhaltung und Umsetzung der von Dataport festgelegten Ziele.

Abb.: IT-Sicherheitsstrategie als zentrale Komponente des ISMS

Folgende Aspekte sind von sicherheitstechnischer und datenschutzrechtlicher Bedeutung:

1. Der **Vorstand** misst der IT-Sicherheit eine **hohe Bedeutung** bei und fördert den IT-Sicherheitsprozess, welcher die Herstellung, den Erhalt, die Entwicklung und Fortschreibung des Sicherheitsniveaus umfasst.

2. Alle Mitarbeiterinnen und Mitarbeiter unterstützen den **IT-Sicherheitsprozess** im Rahmen ihrer jeweiligen Verantwortlichkeiten.

3. Die von Dataport verarbeiteten Informationen und Daten sind gegen **unberechtigte Kenntnisnahme** und **Veränderung** sowie gegen **Verlust** geschützt, auch wenn sie keiner besonderen Geheimhaltung unterliegen.

4. **Kundendaten** werden nach den erteilten Weisungen unter Berücksichtigung der gesetzlichen Vorgaben verarbeitet.

5. Dataport trifft **Schutzmaßnahmen** in Abhängigkeit vom **Schutzbedarf** der jeweiligen Werte und Objekte und gewährleistet grundsätzlich ein normales Sicherheitsniveau im Sinne des BSI-Grundschutzhandbuchs. Die dafür zu treffenden Maßnahmen werden entsprechend den **gesetzlichen** und **vertraglichen** Anforderungen unter Berücksichtigung der Wirtschaftlichkeit realisiert und dokumentiert.

6. Die von Dataport genutzte **IT-Infrastruktur** und die Daten sind durch technische und organisatorische Maßnahmen nach dem **Stand der Technik** vor Beschädigung, Zerstörung, Manipulation, Einschränkung oder Verlust ihrer Funktionalität und Vertraulichkeit geschützt.

7. Mitarbeiterinnen und Mitarbeiter von Dataport werden regelmäßig und bedarfsgerecht für die Belange der IT-Sicherheit **sensibilisiert** und **geschult**.

8. Sicherheitsmaßnahmen für IT-Ressourcen und Daten sind hinsichtlich ihres Umfangs und ihrer Ausprägung auf Grund einer **Risikobetrachtung** so zu gestalten, dass nur ein beschriebenes und für vertretbar gehaltenes **Restrisiko** verbleibt.

9. Bei der Erledigung fachlicher Aufgaben sind die **spezifischen Anforderungen** der IT-Sicherheit stets mit zu berücksichtigen.

10. Für alle **Prozesse** bei Dataport, die Berührungen mit der IT-Sicherheit oder Auswirkungen auf die IT-Sicherheit haben, sind von den **fachlich zuständigen Stellen** Festlegungen zu treffen und zu dokumentieren.

11. Werden Sicherheitsanforderungen eines **Kunden** durch die von Dataport realisierten Maßnahmen nicht erfüllt, so werden die **zusätzlich erforderlichen Maßnahmen** im Rahmen der technischen Möglichkeiten und der technischen Standards von Dataport auftragsgemäß umgesetzt.

12. Für jedes Verfahren und IT-System, ggf. auch von Komponenten von IT-Systemen, werden die erforderlichen Sicherheitsmaßnahmen in einem **IT-Sicherheitskonzept** verbindlich beschrieben. Die IT-Sicherheitskonzepte werden regelmäßig durch die fachlich zuständige Stelle auf ihre **Aktualität** und **Wirksamkeit** geprüft.

13. Alle **Änderungen** an IT-Einrichtungen, -Verfahren oder -Prozessen, die von Dataport betrieben werden, erfordern grundsätzlich eine **Neubewertung** der vorhandenen Sicherheitsmaßnahmen. Die oder der IT-Sicherheitsbeauftragte ist zu

informieren.

14. Der IT-Sicherheitsprozess des jeweiligen Bereichs wird von dem **IT-Sicherheitsmanager**, der übergreifende Prozess von dem **IT-Sicherheitsbeauftragten** regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen **regelmäßig** daraufhin untersucht, ob sie den betroffenen Mitarbeiterinnen und Mitarbeitern bekannt, ob sie umgesetzt und in den Betriebsablauf integriert und wirksam bzw. warum sie nicht bekannt, nicht umgesetzt, nicht integriert oder nicht wirksam sind.

15. **Sicherheitsvorfälle** sind von den verantwortlichen Bereichen in Hinblick auf mögliche Auswirkungen zu untersuchen und zu bewerten. Auf Sicherheitsvorfälle ist mit Maßnahmen zu reagieren, die erforderlich und geeignet sind, die festgestellte Beeinträchtigung oder Abweichung von einer Festlegung zu beseitigen. Der IT-Sicherheitsbeauftragte wirkt bei der Bearbeitung der Sicherheitsvorfälle mit. Die Bearbeitung kann nur mit ihrem oder seinem Einverständnis abgeschlossen werden.

In der IT-Sicherheitsleitlinie werden darüber hinaus die **organisatorischen Strukturen** für das ISMS festgelegt (siehe Tz. 2.3).

2.2.2 Datenschutz-Merkblatt

Das Datenschutz-Merkblatt enthält datenschutzrechtliche **Hinweise**, die Dataport gegenüber seinen **Kunden** zusichert. Die Inhalte des Datenschutz-Merkblattes sind öffentlich und auf der Dataport-Homepage[7] abrufbar. Das Datenschutz-Merkblatt soll nach in Kraft treten der Datenschutzleitlinie durch diese ersetzt werden (siehe Tz. 2.2.3).

2.2.3 Datenschutzleitlinie

Im Gegensatz zu der IT-Sicherheitsleitlinie enthält die Datenschutzleitlinie **datenschutzrechtliche Regelungen**, die durch die BSI-Maßnahmenkataloge (noch) nicht abgedeckt werden.

[7] Siehe http://www.dataport.de/dataport/datenschutz/datenschutzmerkblatt-pdf.pdf

Folgende Regelungen sind von Bedeutung:

1. Dataport gewährleistet als Auftragnehmer die **Konformität** seiner Verarbeitungsprozesse mit den datenschutzrechtlichen Vorschriften.

2. Diese **Datenschutzgrundsätze** gelten für personenbezogene Daten ebenso wie für andere schutzbedürftige Informationen der Kunden Dataports.

3. Dataport erfüllt die Anforderungen an die **Ordnungsmäßigkeit** der im Kundenauftrag erfolgenden Verarbeitungsprozesse durch die Verarbeitung der Daten nach den Weisungen des Auftraggebers, durch die Umsetzung und Einhaltung von Sicherheitskonzepten, durch den Einsatz von informationstechnischen Geräten und Software in der Produktion nach Test und Freigabe sowie durch die Dokumentation der entsprechenden Verfahren.

4. Eine Datenverarbeitung im **Unterauftrag** erfolgt nur auf Grundlage einer schriftlichen Vereinbarung mit dem Auftraggeber unter Benennung des Unterauftragnehmers.

5. Dem **Auftraggeber** wird das **Recht** eingeräumt, nach Vorankündigung während der Geschäftszeiten von Dataport sich durch Inaugenscheinnahme und sonstige Erhebungen davon zu überzeugen, dass die Verarbeitung der personenbezogenen Daten nur im Rahmen seiner Weisungen erfolgt. Der Auftraggeber kann mit der **Kontrolle** auch unabhängige Dritte beauftragen.

6. Dataport setzt, soweit es technisch, wirtschaftlich und qualitativ vertretbar ist, technische **Produkte** ein, deren Vereinbarkeit mit den Vorschriften über den **Datenschutz** und **Datensicherheit** in einem förmlichen Verfahren festgestellt worden ist.

7. Dataport hat die nach dem **Stand der Technik** und der **Schutzbedürftigkeit** der Daten erforderlich und angemessen Maßnahmen getroffen. Es ist insbesondere sichergestellt, dass die **Vertraulichkeit** und **Integrität** der im Kundenauftrag verarbeiteten Daten gewährleistet wird.

8. Dataport stellt sicher, dass Personen Einfluss auf einen Verarbeitungsprozess erst nehmen können, nachdem ihre **Berechtigung** festgestellt worden ist. Es werden Verzeichnisse über die Zugriffsrechte der Mitarbeiter auf die Systeme, die Software und die Datenbestände geführt.

9. Dataport orientiert sich bei der Umsetzung seiner technisch-organisatorischen Maßnahmen an den Anforderungen des IT-Grundschutzes des BSI in **Überein-**

stimmung mit den datenschutzrechtlichen Vorgaben.

10. Dataport wirkt bei der Erstellung von Sicherheitskonzepten und Risikoanalysen der im Auftrag seiner Kunden betriebenen Verfahren mit. Die Sicherheitsmaßnahmen werden **vertraglich** vereinbart.

11. Automatisierte Verfahren, die Dataport in eigener Verantwortung betreibt, sind vor ihrem erstmaligen **Einsatz** oder nach **Änderungen** zu testen und von Dataport freizugeben.

12. **Administrative Zugriffe**, mit denen Änderungen an automatisierten Verfahren bewirkt werden können, sind nur den hierzu ausdrücklich berechtigten Beschäftigten möglich.

13. Dataport gewährleistet, dass administrative Zugriffe sowie Veränderungen **revisionssicher** protokolliert und im Rahmen definierter Verfahren ausgewertet werden. Die Protokolle werden nach den gesetzlichen Anforderungen aufbewahrt und für **Kontrollzwecke** bereitgehalten.

14. Eine Verarbeitung für administrative Zwecke über **mobile Geräte** durch Beschäftigte von Dataport erfolgt in Übereinstimmung mit einem grundschutzkonformen Sicherheitskonzept.

15. Der Vorstand Dataports hat einen **behördlichen Datenschutzbeauftragten** bestellt. Er besitzt die erforderliche Sachkunde und Zuverlässigkeit und kommt bei dieser Tätigkeit nicht in Konflikt mit anderen dienstlichen Aufgaben.

16. Dataport verfügt über ein IT-Grundschutz konformes **Sicherheitsmanagement-System** mit definierten Prozessen nach BSI-Standard 100-2.

17. Dataport führt für jedes automatisierte Verfahren der Datenverarbeitung eine **Dokumentation**.

18. Dataport stellt seinen Kunden für jedes im Auftrag betriebene automatisierte Verfahren die für das **Verfahrensverzeichnis** erforderlichen Informationen zur Verfügung.

2.2.4 IT-Sicherheits- und Datenschutz-Managementhandbuch

Das IT-Sicherheits- und Datenschutz-Managementhandbuch von Dataport beschreibt die **IT-Sicherheitsprozesse** und deren **Zusammenwirken**. Es ist für das

ISMS neben der IT-Sicherheitsleitlinie und der Datenschutzleitlinie das zentrale IT-Sicherheitsdokument. Folgende Aspekte sind für das ISMS von Bedeutung:

- Das IT-Sicherheitsmanagement ist für die **dauerhafte** Aufrechterhaltung einer angemessenen Sicherheit zuständig.
- Entscheidend für den Erfolg des IT-Sicherheitsmanagements ist die **Verankerung** in den Unternehmensstrukturen.
- Sicherheit und Sicherheitsmanagement sind **bereichsübergreifende** Themen und müssen bereichsübergreifend behandelt werden.
- Entscheidungen bei Sicherheitsvorfällen müssen ohne Konflikte mit Betriebsanforderungen getroffen werden. Eine klare **Ressourcenzuordnung** bezüglich der Kernaktivitäten des Sicherheitsmanagements ist erforderlich.
- Das **IT-Sicherheitskonzept** wird nach den BSI-Standards 100-1, 2 und 3 erstellt. Zur Dokumentation wird das GSTool genutzt.

Nähere Einzelheiten zum **Inhalt** und zur **Anwendung** des IT-Sicherheits- und Datenschutz-Managementhandbuchs werden unter Textziffer 2.3 dargestellt.

2.2.5 Personalmanagementhandbuch

Das Personalmanagementhandbuch beschreibt die **Maßnahmenumsetzung** des Bausteins B1.2 Personal. Folgende Maßnahmen werden bezüglich ihrer Umsetzung dargestellt:

- M 3.51 Geeignetes Konzept für Personaleinsatz und -qualifizierung
- M 3.50 Auswahl von Personal
- M 3.1 Geregelte Einarbeitung / Einweisung neuer Mitarbeiter
- M 3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
- M 3.10 Auswahl eines vertrauenswürdigen Administrators und Vertreters
- M 3.33 Sicherheitsüberprüfung von Mitarbeitern

- M 3.55 Vertraulichkeitsvereinbarungen
- M 3.3 Vertretungsregelungen
- M 3.4 Schulung vor Programmnutzung
- M 3.5 Schulung zu IT-Sicherheitsmaßnahmen
- M 3.7 Anlaufstelle bei persönlichen Problemen
- M 3.8 Vermeidung von Störungen des Betriebsklimas
- M 3.11 Schulung des Wartungs- und Administrationspersonals

2.2.6 Schulungskonzept „IT-Sicherheit“

Das Schulungskonzept „IT-Sicherheit“ ist ein Baustein des **Qualifizierungskonzepts** für alle Mitarbeiterinnen und Mitarbeiter und ergänzt die Datenschutz Grundkurse, die ebenfalls für alle Mitarbeiterinnen und Mitarbeiter verbindlich sind und alle 3 Jahre wiederholt werden müssen. Das Schulungskonzept verfügt über folgende Module:

- Modul 1: IT-Grundschutz
- Modul 2: Regelwerk
- Modul 3: Vorgesetztenschulung
- Modul 4: Schulung neuer Mitarbeiterinnen und Mitarbeiter
- Modul5: Anwenderschulung GSTool

2.2.7 Handbuch für den Einsatz des GSTools

Das Handbuch für den Einsatz des GSTools beschreibt den Einsatz des Grundschutztools (GSTool) zur Unterstützung bei der Erstellung von IT-Sicherheitskonzepten. Nach der Erfassung aller sicherheitsrelevanten Informationen im GSTool steht ein umfangreiches **Berichtswesen** zur Verfügung. Das ISMS ist durch den Einsatz des GSTools in der Lage, den IT-Sicherheitsprozess bei der Umsetzung der **Grundschutzvorgaben** zu begleiten und zu überwachen. Das Handbuch behandelt den Umgang mit dem GS-Tool.

2.2.8 Organisationshandbuch

Das Organisationshandbuch beschreibt die **Maßnahmenumsetzung** des Bausteins B1.1 Organisation. Folgende Maßnahmen werden bezüglich ihrer Umsetzung dargestellt:

- M 2.1 Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz
- M 3.3 Vertretungsregelungen
- M 2.2 Betriebsmittelverwaltung
- M 2.4 Regelungen für Wartungs- und Reparaturarbeiten
- M 2.5 Aufgabenverteilung und Funktionstrennung
- M 2.40 Rechtzeitige Beteiligung des Personal-/Betriebsrates
- M 2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten
- M 2.393 Regelung des Informationsaustausches

2.2.9 Reports der Maßnahmenumsetzung aus dem GSTool

Die Reports aus dem GSTool dokumentieren den **Umsetzungsgrad** der vom ISMS zu bearbeitenden Maßnahmen. Der Baustein **B 1.0 IT-Sicherheitsmanagement** zeigt auf, wie ein **funktionierendes** ISMS eingerichtet und im laufenden Betrieb weiterentwickelt werden kann. Er beschreibt dazu sinnvolle Schritte eines systematischen IT-Sicherheitsprozesses und gibt Anleitungen zur Erstellung eines umfassenden IT-Sicherheitskonzepts.

Der Baustein baut auf dem BSI-Standard 100-1 **„Managementsysteme für Informationssicherheit“** und dem BSI-Standard 100-2 **„Vorgehensweise nach IT-Grundschutz“** auf. Er fasst auf dieser Grundlage die wichtigsten Aspekte zum IT-Sicherheitsmanagement zusammen.

2.2.10 Security Management und ITSM

Das Dokument „Security Management und ITSM“ beschreibt die **Behandlung sicherheitsrelevanter Ereignisse** im Rahmen des Sicherheitsmanagements. Es werden insbesondere folgende Aspekte behandelt:

- Aufgaben des Sicherheitsvorfallmanagement
- Bearbeiten von CERT[8]-Meldungen
- IT-Sicherheitsrevision
- Unterstützung der IT-Sicherheitsprozesse durch das Ticket-System ITSM-Suite
- Richtlinie zum Einrichten eines Sicherheitsverdachts
- Priorisierung und Klassifizierung von Security-Tickets
- Eskalationsstufen

2.2.11 Rollen im Sicherheitsvorfallmanagement

In dem Dokument „Rollen im Sicherheitsvorfallmanagement“ werden die Rollen für die Behandlung von sicherheitsrelevanten Ereignissen beschrieben. In einer Tabelle werden Aufgaben aufgelistet und verschiedenen Rollen zugewiesen.

2.3 ISMS in der Umsetzung

Die Implementierung und die Funktionen des ISMS werden im Dokument „IT-Sicherheits- und Datenschutz-Managementhandbuch“ beschrieben. Für das ISMS ist das Handbuch als verbindliche **Handlungsanweisung** und als **Rahmenwerk** für die Bearbeitung von IT-Sicherheitsprozessen anzuwenden. Es gilt für alle **Dataportstandorte** aufgrund des **Vorstandbeschlusses** (vgl. Tz. 2.1). Folgende Inhalte sind von Bedeutung:

[8] Computer Emergency Response Team, Anlaufstelle für alle Fragen zur Sicherheit

2.3.1 IT-Sicherheitsorganisation des ISMS

Die IT-Sicherheitsorganisation des ISMS besteht aus dem Vorstand, dem IT-Sicherheitsbeauftragten (ITSB) sowie den IT-Sicherheitsmanagern (ITSM) der Bereiche und den IT-Sicherheitskoordinatoren (ITSK), die u.a. für die Kundenkommunikation zuständig sind. Die IT-Sicherheitsorganisation wird durch das Notfallmanagement ergänzt.

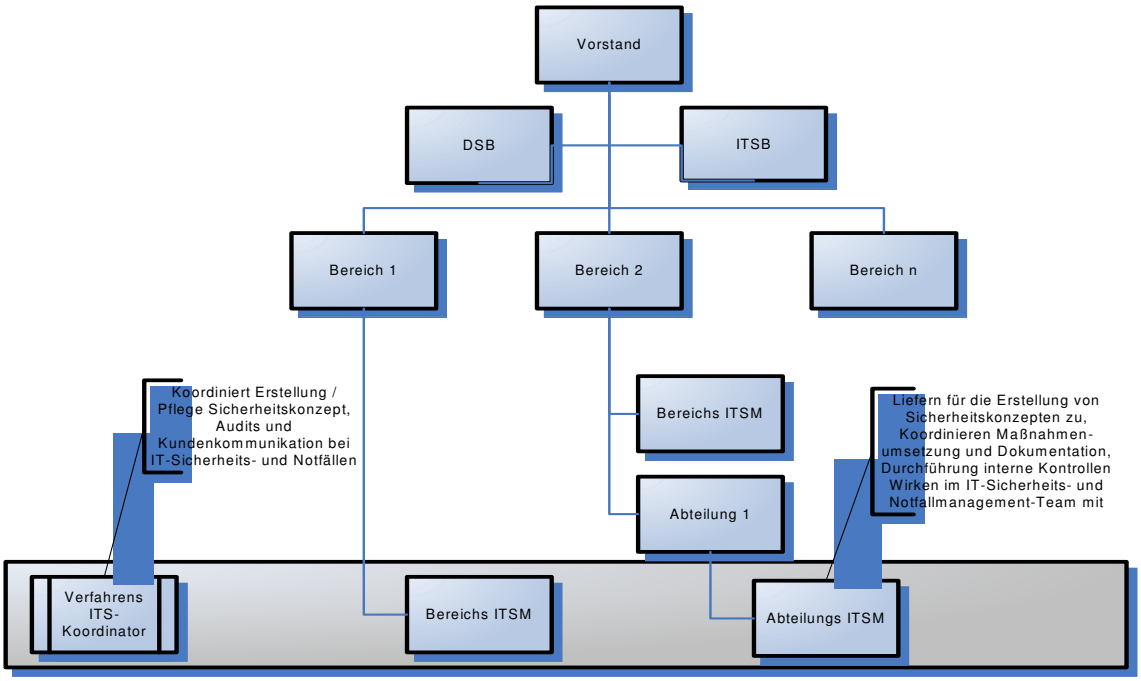

Abb.: Strukturen der IT-Sicherheitsorganisation

Das **Datenschutzmanagement** wird personell durch den Datenschutzbeauftragten (DSB) wahrgenommen. Zwischen dem ITSB und dem DSB findet ein regelmäßiger Austausch über die Durchführung ihrer Aktivitäten statt.

Die IT-Sicherheitsorganisation ist als **Matrix** aufgebaut. Die fachliche Leitung hat der IT-Sicherheitsbeauftragte (ITSB). Er ist für den IT-Sicherheitsprozess verantwortlich, leitet das IT-Sicherheitsmanagement, arbeitet eng mit der Leitungsebene zusammen und berichtet dem Vorstand.

Der **IT-Sicherheitsbeauftragte** wird fachlich unterstützt durch die **IT-Sicherheitsmanager** in den Bereichen, bei Bedarf auch den Abteilungen und Gruppen von Dataport (Linienorganisation). Für fachlich spezifische Aufgaben im Rahmen von unter-

stützenden IT-Sicherheitsprozessen gibt es weitere Funktionsträger. Insbesondere sind hier die **Notfallmanager** für jeden Standort von Dataport (Standort-Notfallmanager) und der Manager für die Bearbeitung von CERT-Meldungen (CERT-Meldungsmanager) zu nennen.

Horizontal zur Linienorganisation des Sicherheitsmanagements werden **die IT-Sicherheitskoordinatoren** eingesetzt. Sie koordinieren die Erstellung von IT-Sicherheitskonzepten für Kunden und führen die Kommunikation mit dem Sicherheitsmanagement des Kunden bei IT-Sicherheitsvorfällen und Notfällen durch.

Der IT-Sicherheitsbeauftragte wird bei der Durchführung seiner Aufgaben durch das **IT-Sicherheitsmanagement-Team** und das **IT-Sicherheitsvorfallmanagement-Team** unterstützt. Beide Teams setzen sich aus den jeweils benötigten Funktionsträgern im IT-Sicherheitsmanagement zusammen. Bei Bedarf können weitere Fachleute und Externe hinzugezogen werden. Der Aufbau der Sicherheitsorganisation entspricht dem BSI-Standard 100-2.

2.3.2 Funktionen und Rollen des ISMS

Der **IT-Sicherheitsbeauftragter** (ITSB) leitet das IT-Sicherheitsvorfallmanagement-Team und die Notfallvorsorge bei Dataport. Er ist zentraler Ansprechpartner bei IT-Sicherheitsvorfällen und Notfällen.

Gemäß der **IT-Sicherheitsleitlinie** sind in allen Bereichen **IT-Sicherheitsmanager** (ITSM) zu benennen. Diese koordinieren die Umsetzung aller nach IT-Grundschutz erforderlichen Sicherheitsmaßnahmen für alle Fachverfahren in ihrem jeweiligen Bereich. Sie unterstützen die Sicherheitskoordinatoren bei der Erstellung und Umsetzung von IT-Sicherheits- und Notfallvorsorgekonzepten für Kunden. Darüber hinaus sind sie Mitglieder des IT-Sicherheitsvorfallmanagement-Teams und koordinieren in ihren bereichen das IT-Sicherheitsvorfallmanagement.

Die **IT-Sicherheitskoordinatoren** (ITSK) koordinieren die Unterstützungsleistungen von Dataport für die Sicherheitskonzeption und Erstellung von Sicherheitskonzepten durch Kunden. Im einfachsten Fall besteht die Unterstützungsleistung in der Erstellung geeigneter GSTool-Reports über die Umsetzung von Standardsicherheitsmaßnahmen bei Dataport. Die ITSK stützen sich dabei auf die Zuarbeit der IT-Sicherheitsmanager. Sie unterstützen im Bedarfsfalle bei der Durchführung von Audits und sind für die Kundenkommunikation bei IT-Sicherheitsvorfällen und Notfällen zuständig.

Für die Bearbeitung von Sicherheitskonzepten und IT-Sicherheitsvorfällen kann sich der ITSB auf ein **Sicherheitsmanagement-Team (SMT)** stützen. Es setzt sich aus den IT-Sicherheitsmanagern zusammen, deren Bereiche von der Erstellung von Sicherheitskonzepten bzw. vom IT-Sicherheitsvorfall betroffen sind. Bei Bedarf können weitere interne Fachleute oder Externe hinzugezogen werden.

Das **IT-Sicherheitsvorfallmanagement-Team** besteht aus dem ITSB, den IT-Sicherheitsmanagern der betroffenen Bereiche und dem behördlichen Datenschutzbeauftragten. Bei Bedarf können weitere interne Fachleute oder Externe hinzugezogen werden. Es unterstützt den ITSB bei der Untersuchung und Bewertung des Vorfalls und bei der Auswahl der notwendigen Maßnahmen und deren Umsetzung.

2.3.3 IT-Sicherheitsprozesse

Das ISMS stützt sich auf einen **Kernprozess**, acht teils eigenständige Unterstützungsprozesse und weitere vier definierte wiederkehrende Aufgaben. Der Kernprozess stellt die Weiterentwicklung der Sicherheitsleitlinie und des Sicherheitsmanagements sicher. Des Weiteren werden im Rahmen dieses Prozesses Sicherheitskonzepte für Dataport eigene Verfahren erstellt und aktualisiert. Dieser Prozess entspricht dem BSI-Standard 100-2.

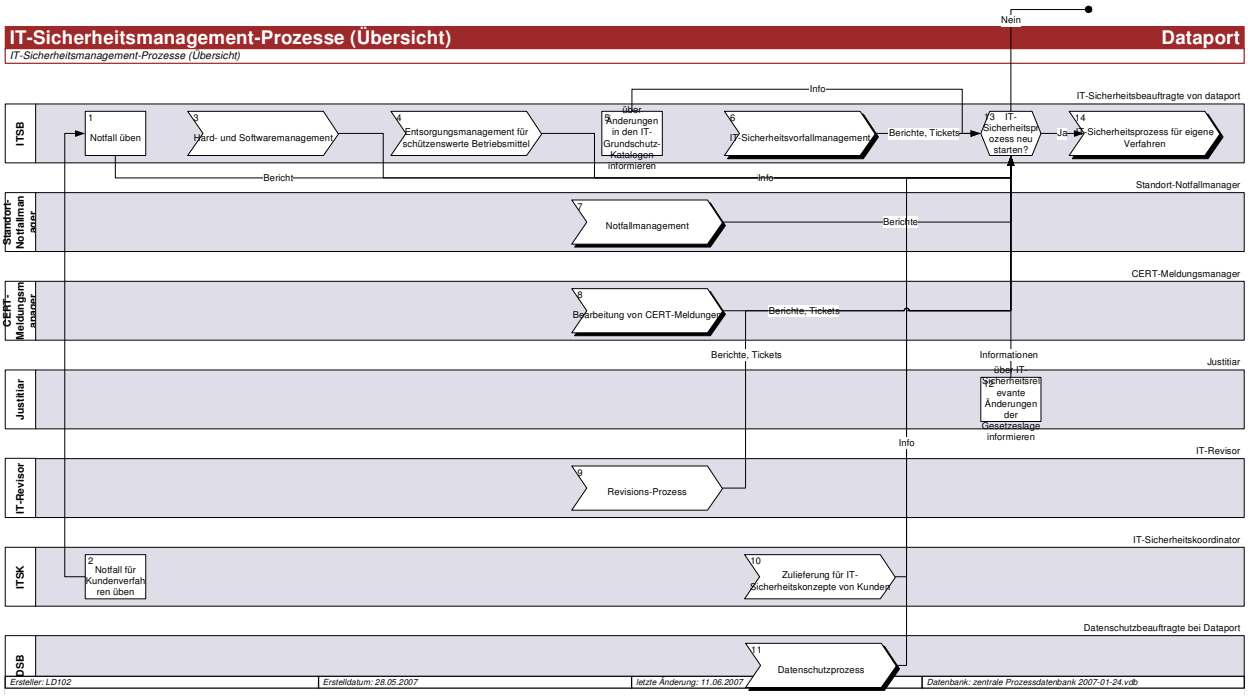

Abb.: IT-Sicherheitsmanagement-Prozesse

Die Unterstützungsprozesse sind:

- IT-Sicherheitsvorfallmanagement
- Notfallmanagementprozess
- Datenschutzmanagementprozess (eigenständiger Prozess unter Leitung des Datenschutzbeauftragten)
- IT-Revisionsprozess (eigenständiger Prozess unter Leitung des IT-Revisors)
- Prozess zur Bearbeitung von CERT-Meldungen
- Hard- und Softwaremanagementprozess
- Entsorgungsprozess für schützenswerte Betriebsmittel
- Zulieferungsprozess für Sicherheitskonzepte von Kunden

Diese Unterstützungsprozesse und Aufgaben fassen die Umsetzung von Maßnahmen zusammen, die im Rahmen verschiedener Bausteine der IT-Grundschutzkataloge wiederholt genannt werden.

Aus Sicht der Kunden von Dataport liefern insbesondere die Unterstützungsprozesse

- IT-Sicherheitsvorfallmanagement
- Notfallmanagementprozess und
- Zulieferungsprozess für Sicherheitskonzepte

eine nachhaltige Unterstützung bei ihrem eigenen Sicherheitsmanagement.

Das IT-Sicherheitsvorfallmanagement bewertet Informationen aus CERT-Meldungen und Störungen in Abstimmung mit dem Kunden als IT-Sicherheitsvorfälle in zwei **Standardkategorien** „Sicherheitsproblem“ und „Sicherheitsvorfall“. Eine Bearbeitung von Sicherheitsvorfällen erfolgt dann gemeinsam mit dem IT-Sicherheitsmanagement des Kunden unter dessen Leitung. Der IT-Sicherheitsbeauftragte von Dataport koordiniert die Unterstützung durch das dataport-eigene Sicherheitsmanagement.

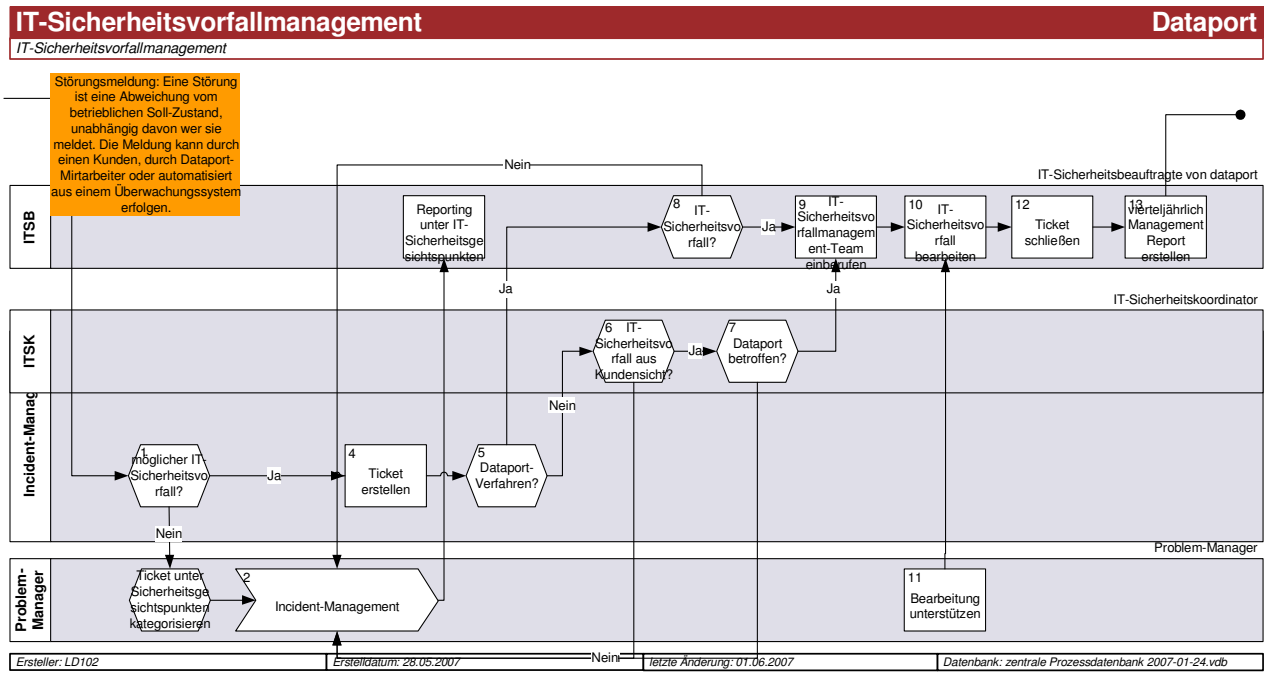

Abb.: Prozess IT-Sicherheitsvorfallmanagement

Analog erfolgt die Unterstützung der Kunden bei **Notfällen** durch die Standort-Notfallmanager. Notfallvorsorgemaßnahmen und Vorgaben für das Notfallmanagement werden im Notfallhandbuch für jeden Dataport-Standort dokumentiert. IT-Sicherheitsvorfallmanagement und Notfallmanagement bauen aufeinander auf. Dabei können IT-Sicherheitsvorfallmanagement und Notfallmanagement als Eskalationen von Betriebsstörungen (Incidents) und Problems verstanden werden. Die folgende Abbildung stellt das Zusammenwirken der genannten Prozesse dar:

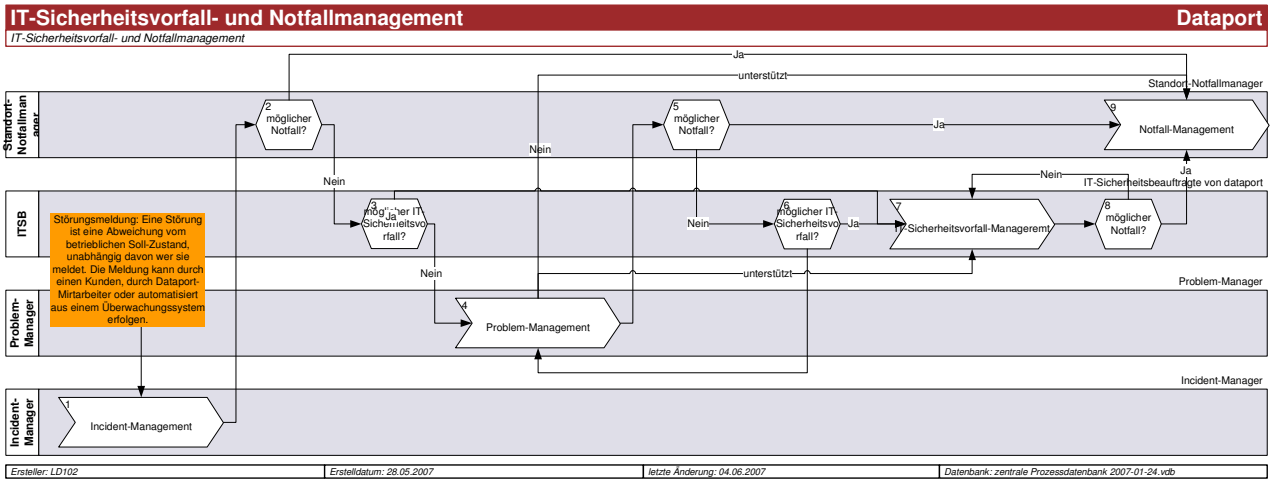

Abb.: Prozess IT-Sicherheitsvorfall- und Notfallmanagement

Der Zulieferungsprozess für Sicherheitskonzepte von Kunden koordiniert unter Leitung eines IT-Sicherheitskoordinators die Leistungen unterschiedlicher Bereiche von Dataport und macht die Dokumentation über die Umsetzung von Standardsicher-

heitsmaßnahmen nach IT-Grundschutz Kunden zugänglich. Ferner unterstützt der IT-Sicherheitskoordinator den Kunden bei internen und externen Audits.

Alle Prozesse sind **einheitlich** dokumentiert. Neben Eingaben und Ergebnissen sind die Abläufe, die Verantwortlichen und Beteiligten sowie die Messparameter für die Optimierung, so genannte **Key-Performance-Indikatoren** (KPI), festgelegt.

2.4 Prozessreifegradmodell

Für das ISMS ist eine Konzeption erarbeitet worden, deren Umsetzung in einem großen Unternehmen wie Dataport sukzessive erfolgt. Die **vollständige** Implementierung des ISMS in die Aufbau- und Ablauforganisation von Dataport erfordert eine Vielzahl von organisatorischen und technischen Änderungen. In Teilbereichen hat Dataport mit dem Aufbau eines **funktionierenden** ISMS begonnen und Aufgaben im Rahmen der im ISMS festgelegten Prozessabwicklung bereits Mitarbeitern zugewiesen.

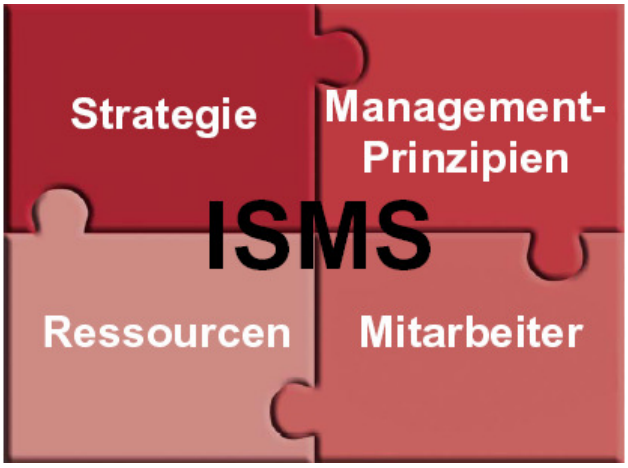

Abb.: Bestandteile des ISMS

Das ISMS umfasst alle Regelungen, die für die **Steuerung** und **Lenkung** zur Zielerreichung sorgen. Weiterhin wurde festgelegt, mit welchen **Instrumenten** und **Methoden** der **Vorstand** die auf die Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt.

Anhand des **Reifegradmodells** kann nun bestimmt werden auf welcher Stufe Dataport die Konzeption des ISMS umgesetzt hat. Das **Process Maturity Model** (PMM) ist ein Reifegradmodell, mit dem die definierten Prozesse untersucht und beurteilt

werden können, inwieweit sie in der Lage sind, die festgelegten Ziele zu erreichen. Dabei werden die Prozesse anhand ihrer Ausprägung einer bestimmten **Reifegradstufe** zugeordnet.

- **Reifestufe 0:** Incomplete (Der chaotische Prozess)
- **Reifestufe 1:** Performed (Der initiale Prozess)
- **Reifestufe 2:** Managed (Der definierte Prozess)
- **Reifestufe 3:** Established (Der standardisierte Prozess)
- **Reifestufe 4:** Predictable (Der vorhersagbare Prozess)
- **Reifestufe 5:** Optimizing (Der optimierte Prozess)

Wird das Reifegradmodell auf die Umsetzung des ISMS in der **Gesamtorganisation** von Dataport am **Standort Altenholz** angewandt, liegt die Einstufung zum Zeitpunkt der Begutachtung in **Abhängigkeit** von dem zu betrachtenden Organisationsbereich zwischen 1 und 4:

Für die **Kundenverfahren** „ZIAF“ und „Landesnetz“ wurde mit der Umsetzung der Implementierung des ISMS in die Organisationsstrukturen Dataports zuerst begonnen. Nach dem Reifegradmodell ist zum Zeitpunkt der Begutachtung für diese Fachverfahren die Stufe 4 erreicht. Weitere Kundenverfahren sind in der Umsetzung.

2.5 Werkzeuge für das ISMS

Zur Unterstützung des IT-Sicherheitsmanagements setzt Dataport im Wesentlichen zwei Werkzeuge ein. Die Bearbeitung von IT-Sicherheitsvorfällen, CERT-Meldungen und Notfällen wird im **Ticket-System** dokumentiert. Dies ermöglicht eine einfache Eskalation von Störungen aus dem Incident- und Problemmanagement, unterstützt die Klassifizierung und ermöglicht die Erstellung automatisierter Auswertungen über die bearbeiteten Vorfälle.

Die Umsetzung von IT-Sicherheitsmaßnahmen wird im **Grundschutztool** (GSTool) dokumentiert. Dabei werden die Stammdaten (z.B. Räume und Gebäude, IT-Systeme, Netze und Anwendungen) so erstellt, dass eine dezentrale Pflege der Maßnahmenumsetzung bei Dataport durch die IT-Sicherheitsmanager in der Linienorganisation möglich wird. Gleichzeitig können die gleichen Stammdaten in IT-Verbünden für Kunden organisiert werden. Dies ermöglicht die Erstellung kundenspezifischer Reports über die Umsetzung von Maßnahmen in deren IT-Verbünden.

3 Datenschutzrechtliche Bewertung

3.1 Prüfungsverlauf

Das Audit „**Konzeption** eines **Informationssicherheits-Managementsystems**“ wurde vom Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein (ULD) über mehrere Phasen begleitet.

Zunächst wurde in Zusammenarbeit mit Dataport eine umfassende **Bestandsaufnahme** über die aufbau- und ablauforganisatorischen Strukturen durchgeführt. Die Ergebnisse der Erhebung sowie Handlungsempfehlungen wurden in einem Bericht zugestellt. Auf der Grundlage des Berichts wurden die **Strukturen** des ISMS erarbeitet.

Die Anpassung der ursprünglichen Dokumentenlage an die derzeitigen Gegebenheiten unter Berücksichtigung aller organisatorischen, technischen und datenschutzrechtlichen Belange war aufwändig. Ebenso musste der technischen und organisatorischen Infrastruktur des **Rechenzentrums** Rechnung getragen werden.

In regelmäßigen Abständen fanden mit Dataport **Projektgruppensitzungen** statt, in denen die vom ULD festgestellten Sachverhalte diskutiert und Lösungen für die Verbesserung und Optimierung zur Erreichung der festgelegten Datenschutzziele erarbeitet wurden (vgl. Tz. 1).

Nach Abschluss aller Arbeiten und nach Erreichung der von Dataport festgelegten Ziele wurde vom ULD im Juli 2007 die **Begutachtungsphase** eingeleitet. Analysiert wurden insbesondere die zur **Konzeption** gehörigen Dokumente (siehe Anlagenverzeichnis). Die Funktionsweise des ISMS wurde darüber hinaus vor Ort mit den bereits umgesetzten aufbau- und ablauforganisatorischen Gegebenheiten stichprobenartig geprüft und abgeglichen.

3.2 Rechtliche Anforderungen

Dataport verarbeitet „eigene“ sowie personenbezogene Daten seiner Kunden in deren Auftrag. Darüber hinaus gewährleistet Dataport als Auftragnehmer die **Konformität** seiner Verarbeitungsprozesse mit den datenschutzrechtlichen Vorschriften.

Das **Landesdatenschutzgesetz** sowie die **Datenschutzverordnung** finden infolgedessen neben den bereichsspezifischen Vorschriften Anwendung. Die gesetzlichen Regelungen zur Datensicherheit verweisen auf den allgemeinen anerkannten Standard der IT-Sicherheit und auf die Anforderungen an ihre Dokumentation.

Die automatisierte Verarbeitung personenbezogener Daten erfordert technische und organisatorische Maßnahmen, die die Datensicherheit bzw. die Ordnungsmäßigkeit der Datenverarbeitung gewährleisten. Ein angemessenes IT-Sicherheitsniveau kann nur durch geplantes und organisiertes Vorgehen aller Beteiligten erreicht und aufrechterhalten werden. Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von Sicherheitsmaßnahmen ist eine systematische Vorgehensweise. Diese Planungs-, Lenkungs- und Kontrollaufgaben werden vom ISMS übernommen.

3.3 Konformität der BSI-Standards

Dataport hat die Konzeption des **ISMS** nach den BSI-Standards BSI 100-1, 100-2 und 100-3 erstellt. Dabei wurden die BSI-Sicherheitsmaßnahmen der anzuwendenden Bausteine

- B 1.0 IT-Sicherheitsmanagement,
- B 1.1 Organisation,
- B 1.2 Personal,
- B 1.8 Behandlung von Sicherheitsvorfällen und
- B 1.13 IT-Sicherheitssensibilisierung und -schulung

berücksichtigt. Das ISMS erfüllt die **grundlegenden** Anforderungen, insbesondere

- die Übernahme der Gesamtverantwortung für IT-Sicherheit durch die Leitungsebene,
- die Erstellung einer IT-Sicherheitsleitlinie,
- die Festlegung der IT-Sicherheitsziele und –strategie,
- der Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit sowie
- die Dokumentation des IT-Sicherheitsprozesses.

Die darüber hinaus gehenden für das ISMS maßgeblichen IT-Sicherheitsmaßnahmen befinden sich derzeit in der Umsetzung, so dass eine vollständige und wirk-

same **Installation des ISMS in die gesamte Organisationsstruktur von Dataport auf der Grundlage dieses Konzepts** realisiert werden kann.

3.4 Zusammenfassende Bewertung

Im Auditverfahren „**Konzeption eines Informationssicherheits-Managementsystems**“ wurde festgestellt, dass Dataport über eine rechts- und normenkonforme Konzeption verfügt, die die Kernelemente des ISMS aufbau- und ablauforganisatorisch beschreibt und praxistauglich umgesetzt werden kann. Die Praxistauglichkeit des Konzepts wird durch seine Implementierung für einzelne Fachverfahren bestätigt. Die Berücksichtigung **internationalen Sicherheitsstandards** BSI-Grundschutz unter Einbeziehung von ITIL gewährleistet ferner die Bestimmung von wirkungsvollen IT-Sicherheitsprozessen sowie die dafür erforderlichen IT-Sicherheitsmaßnahmen. Die **Leitungsebene** ist sensibilisiert und übernimmt Aufgaben und Pflichten bezüglich der Informationssicherheit. Von ihr werden bewusst folgende **Managementfunktionen** wahrgenommen:

- Übernahme der Gesamtverantwortung für IT-Sicherheit,
- Festlegung der Sicherheitsziele und Sicherheitsstrategie,
- Integration der IT-Sicherheit in die Dataport-Organisation mit Hilfe des ISMS.

Darüber hinaus wurden bei der Durchführung des Audits folgende „**datenschutzfreundliche**“ Aspekte als besonders erwähnenswert festgestellt:

1. Das ISMS gewährleistet dauerhaft ein hohes Gesamtsicherheitsniveau.
2. Die Datenverarbeitung wird unter den Aspekten der Verfügbarkeit, Vertraulichkeit, Integrität sowie der Ordnungsmäßigkeit in einer geregelten Aufbau- und Ablauforganisation überwacht.
3. Die Sicherheitsprozesse sind unter Berücksichtigung eines national anerkannten Sicherheitsstandards gestaltet.
4. Sicherheitsrelevante Ereignisse können über das IT-Sicherheitsvorfallmanagement rechtzeitig erkannt werden.
5. Die technischen und organisatorischen Abläufe des ISMS werden im IT-Sicherheits- und Datenschutz-Managementhandbuch vollständig beschrieben.

Die Prüfung hat ergeben, dass die zum Konzept gehörenden Dokumente des ISMS in Übereinstimmung mit dem nationalen Sicherheitsstandard des BSI gestaltet sind und keinen Anlass zu datenschutzrechtlichen Beanstandungen geben. Ferner hat die Prüfung gezeigt, dass das ISMS für einzelne Kundenverfahren bereits BSI-standardkonform implementiert ist.

Kiel, 27. August 2007

(Gutachter: Heiko Behrendt)