Informationssicherheit nach DIN ISO 27001 auf Basis IT-Grundschutz
Customized Baustein KIDICAP P5

Datum

10.05.2012

Gesellschaft für Innovative Personalwirtschaftssysteme mbH

In Zusammenarbeit mit:
HiSolutions AG
Information Security Consulting
Bouchéstraße 12
12435 Berlin
GERMANY

Dokumenten-Status

Projektname		Projektnummer	
Erstellung Grundschutzbaustein KIDICAP P5		nn-nnn	
Dokumenten Titel		Dokumenten Dateiname	
Customized Baustein KIDICAP P5		Baustein KIDICAP v0.93.doc	
Autor	Seiten	Version	Verfasst am:
Wolfgang Witerzens witerzens@hisolutions.com	16	Final v1.0	25. November 2011

Versionsverlauf

Datum Veränderung	Version	Beschreibung	verändert durch
9. Mai 2011	0.1	Erster Entwurf	Wolfgang Witerzens
26. Juli 2011	0.2	Qualitätssicherung	Robert Manuel Beck
05. August 2011	0.8	QS	Wilhelm Dolle
16. August 2011	0.9	Finaler Entwurf	Wolfgang Witerzens
25.November 2011	1.0	Finale Version	Wolfgang Witerzens

Inhaltsverzeichnis

1 Einleitung

1.1 Hintergrund

Die Anwendung KIDICAP P5 konsolidiert Funktionen für die Gehaltsabrechnung, die Personalverwaltung und das Dienstreisemanagement. Im Rahmen der Integration der Anwendung in eine IT-Infrastruktur ist es unerlässlich, angemessene Sicherheitsmaßnahmen umzusetzen. Eine mögliche Grundlage hierfür bietet die IT-Grundschutz-Vorgehensweise des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Innerhalb der Grundschutzkataloge des BSI existiert jedoch kein vorgefertigter Baustein für die Software KIDICAP P5. Zur vollständigen Modellierung von Informationsverbünden kann dies aber notwendig sein.

Dieser Customized Baustein wurde mit Hilfe der angepassten Gefährdungen und Maßnahmen aus „CB 5.93 Anwendungssoftware aus Eigenentwicklung“ modelliert. Die Nummerierung der verwendeten Maßnahmen wurde nicht verändert. Einzelne Maßnahmen sind für die Anwendbarkeit auf eigenentwickelte Software modifiziert worden. Um die Veränderung dieser Maßnahmen zu kennzeichnen, wurden ihre Bezeichner mit einem * versehen.

1.2 Ziel

Der vorliegende Baustein für KIDICAP P5 der Gesellschaft für Innovative Personalwirtschafts-systeme mbH (GIP) wurde unter Zuhilfenahme der Standardmaßnahmen der Grundschutzkataloge erstellt.

Kernfunktionalität von KIDICAP P5 ist die Engine zur Personalabrechnung (KIDICAP PPay) inklusive funktionaler AddOns (eAkte, Contentmanagement, HCM-Apps) auf deren Betrieb der vorliegende Baustein zielt.

Die Besonderheit an KIDICAP P5 liegt im Betrieb und im Einsatzumfeld, da die Software einen Großrechner vorraussetzt, welcher in der Regel nur in größeren Rechenzentren vorhanden ist. KIDICAP P5-Systeme werden in der Regel nicht von Grund auf neu implementiert oder stillgelegt, sondern in den bestehenden Installationen um neue Kunden und Arbeitgeber erweitert. Der Betrieb der Software erfolgt dabei meist im Rahmen von Outsourcing. Die sichere Implementierung und Betrieb ist in professionellen KIDICAP-Rechenzentren gegeben. Der vorliegende Baustein soll dazu einen Leitfaden geben.

2 Customized Baustein KIDICAP P5

2.1 Beschreibung KIDICAP P5

Alle Prozesse integriert

KIDICAP P5 bietet allen Beteiligten eine effiziente Unterstützung in der gesamten Wertschöpfungskette der Personalwirtschaft. Alle Ereignisse, die in der Laufbahn eines Mitarbeiters oder in mitarbeiterübergreifenden Prozessen auftreten, können im jeweiligen Modul von KIDICAP P5 einfach abgebildet werden. Dabei berücksichtigt das System sowohl zentral organisierte Aufgaben des Personalmanagements (Personalverwaltung, Personalplanung und -controlling) als auch dezentrale Prozesse, wie etwa das Einbeziehen der Führungskräfte und Mitarbeiter in Aufgaben und Prozesse der Personalarbeit.

Abb.: Lösungen für die gesamte Prozess- und Wertschöpfungskette der Personalwirtschaft

KIDICAP P5 ist speziell für die Anforderungen und Bedürfnisse des öffentlichen Dienstes, der Kirchenorganisationen und des Gesundheitswesens entwickelt. Die funktionale Tiefe der Software führt zu einem hohen Nutzungsgrad im Public Sector.

Modularer Softwareaufbau

Zu den Hauptaufgaben von KIDICAP P5 zählen Personalverwaltung, Personalplanung und -controlling, -abrechnung, Self Services sowie Prozesskommunikation. Um den Benutzerrollen in den Aufgabenfeldern bestmöglich zu entsprechen, ist KIDCAP P5 in drei Engines gegliedert:

- Personalverwaltung
- Personalabrechnung
- Dienstreiseabrechnung

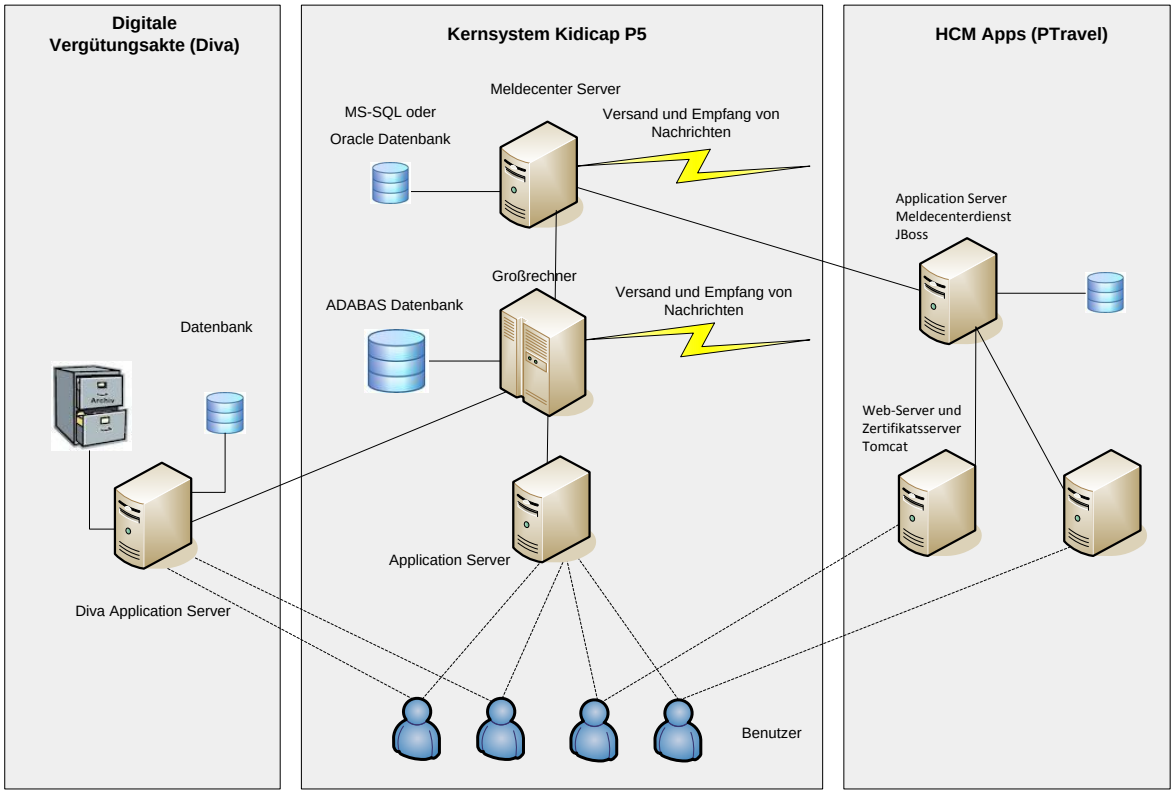
Ergänzt wird die Funktionalität der drei Engines durch sogenannte AddOns: Die elektronische Personalakte, ein Contentmanagementsystem und weitere HCM-Funktionsbausteine komplettieren die Softwareanwendung und führen zur weiteren Produktivitätssteigerung und Automatisierung der Arbeitsabläufe.

Web-Services, Business-Integratoren und Schnittstellen ermöglichen die einfache Kommunikation z.B. mit ERP-, Spezial-, DMS-oder Archivsystemen.

Das System ist rollenbasiert aufgebaut und bedient die rollenspezifischen Anforderungen der Anwender. Jeder Beteiligte im personalwirtschaftlichen Prozess wird gemäß seinem Benutzerprofil unterstützt. Die mehrschichtige KIDICAP P5-Architektur ermöglicht mit Web-Clients und Portalintegrationen einen Einsatz in den unterschiedlichsten Varianten.

Technischer Überblick

KIDICAP P5 kann innerhalb mehrerer möglicher Betreibermodelle betrieben werden. Zwischen Application Service Providing (ASP) und Full Service Providing (FSP) können alle Service-Ebenen abgebildet werden. In jedem Fall wird in einem ServiceCenter die Software installiert und die Datenbank eingerichtet. Nachfolgende Skizze zeigt den typischen Aufbau eines KIDICAP P5 Systems:



Vorraussetzung für das KIDICAP P5 Kernsystem ist eine ADABAS Datenbank auf einem Großrechner mit OS/390 oder VSE. Das System selbst ist in der von der Software AG entwickelten Programmiersprache NATURAL geschrieben und setzt direkt auf eine ADABAS Datenbank auf.

Die Benutzer kommunizieren dabei über einen Application Server mit dem Großrechner, bzw. KIDICAP P5. Sowohl die Clientssoftware, als auch die Software für den Application Server sind betriebssystemunabhängig in Java geschrieben. Darüber hinaus ist es auch möglich das System für den Zugriff über einen Citrix Terminal Server zu konfigurieren.

Neben dem reinen Benutzerzugriff gibt es für den Versand und Empfang einen sogenannten Meldecenter Server, welcher neben einer Schnittstelle am Großrechner auch zusätzlich Meldungen an externe Einheiten wie z.B. eGovernment, Finanzamt, Krankenkassen, Renten-, AV-

Versicherung verschicken kann. Die Serversoftware ist dabei ebenfalls, wie beim Application Server, betriebssystemunabhängig in Java geschrieben. Zusätzlich benötigt der Meldecenter Server eine MS-SQL oder Oracle Datenbank.

Die technische Struktur der digitalen Vergütungsakte, oder auch eAkte genannt, besteht aus einem Application Server, einem Archivsystem und einem Datenbank Server. Im Rahmen der Archivierung wird dabei der AFP Druckstrom des Großrechners abgegriffen, über eine Konvertierungskomponente nach verschiedenen Kriterien aufbereitet, in pdf/a konvertiert und im Archivsystem abgelegt. Bedingt durch die platformunabhängigkeit der Software kann das System auf allen gängigen Betriebssystemen und Datenbanken betrieben werden.

Der Teilbereich HCM Apps, der z.B. das Thema Reisekostenabrechnung in PTravel abdeckt besteht aus einem Web-Server und ftp-Server für den direkten Kontakt mit den Benutzern, sowie einem Application Server und einer Datenbank für die Verarbeitung im Hintergrund. Bedingt durch die platformunabhängigkeit der Software kann auch hier das System auf allen gängigen Betriebssystemen und Datenbanken betrieben werden.

2.2 Gefährdungslage

Der vorliegende Abschnitt behandelt grundsätzliche Gefährdungen der Software KIDICAP P5.

Generell hängt die Gefährdungslage von KIDICAP P5 vom Einsatzszenario ab. Ein Personalwirtschaftssystem in einem isolierten Behörden- oder Unternehmensnetz ist in der Regel weniger gefährdet als ein System, das über eine Reihe an externen Schnittstellen verfügt oder sogar an das Internet angeschlossen ist.

Folgende typische Gefährdungen werden angenommen:

2.2.1 Höhere Gewalt

G 1.1	Personalausfall
G 1.2	Ausfall von IT-Systemen

2.2.2 Organisatorische Mängel

G 2.7	Unerlaubte Ausübung von Rechten
G 2.22	Fehlende Auswertung von Protokolldaten
G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
G 2.27	Fehlende oder unzureichende Dokumentation
G 2.28	Verstöße gegen das Urheberrecht
G 2.29	Softwaretest mit Produktionsdaten
G 2.66	Unzureichendes Sicherheitsmanagement
G 2.69*	Fehlende oder unzureichende Planung des Einsatzes der Software Die Planung des Einsatzes spielt eine wichtige Rolle für einen ordnungsgemäßen Betrieb eine Software. Die Planung sollte mindestens folgende Aspekte berücksichtigen: Die Planung der Zugriffsmöglichkeiten auf die Software ist ein Kernthema für die

	Systemsicherheit. Weiterhin ist die Planung der Administration der Software ein wichtiges Thema. Insbesondere die Art des Zugriffs, z.B. über eine Webanwendung oder über die Kommandozeile, kann von entscheidender Bedeutung für die Sicherheit sein. Bei fehlender oder fehlerhafter Planung der Administrationsaufgaben besteht die Gefahr, dass das System unsicher oder unzulänglich administriert wird. Darüber hinaus können sich bei fehlender oder unzureichender Planung auch folgende Probleme ergeben: • Der Administrationszugriff auf das System kann unzureichend gesichert sein, • die Systemperformance zu gering sein und • es kann zu Datenverlusten kommen, sofern Replikation und Backup nicht ausreichend berücksichtigt wurden.
G 2.87	Verwendung unsicherer Protokolle in öffentlichen Netzen
G 2.97*	Unzureichende Notfallplanung für die Software Eine unzureichende Planung für Notfälle kann Probleme, die beim Betrieb der Software auftreten, wesentlich verschlimmern und Ausfallzeiten verlängern. Zusätzlich zu allgemeinen Fehlern, die oft im Bereich Notfallvorsorge gemacht werden, können bei Applikationen einige spezielle Fehler passieren, die eine schnelle Reaktion auf Zwischenfälle sehr erschweren oder gar unmöglich machen können. Einige dieser Fehler werden im Folgenden beschrieben. • Wird nach einem Notfall (etwa einem Hackereinbruch) eine Neuinstallation der Software nötig, so kann es zu erheblichen Verzögerungen führen, wenn die bei der Installation verwendeten Pakete (Quelltexte oder Distributionspakete) nicht mehr verfügbar sind. Sind die Installationspakete zwar verfügbar, aber beispielsweise auf dem betroffenen Rechner selbst und nicht auf einem anderen Rechner oder einem schreibgeschützten Datenträger gespeichert, so müssen sie nach einem Hackereinbruch als unsicher angesehen werden. • Existiert keine oder nur eine unzureichende Dokumentation der Konfiguration, so kann es sehr schwierig sein, nach einem Notfall überhaupt wieder eine funktionierende Konfiguration herzustellen. Schlechte Dokumentation kann auch dazu führen, dass Konfigurationsfehler zunächst nicht entdeckt werden und bei auftretenden Problemen eine aufwendige Fehlersuche erforderlich wird. • Bei der Systemwiederherstellung nach einem Notfall kann es wünschenswert sein, einen älteren Stand der Konfiguration wieder herzustellen. Wird für die Konfigurationsdateien keine Versionsverwaltung durchgeführt, so kann dies schwierig oder gar unmöglich sein.

2.2.3 Menschliche Fehlhandlungen

G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
G 3.3	Nichtbeachtung von IT-Sicherheitmaßnahmen
G 3.8	Fehlerhafte Nutzung von IT-Systemen

G 3.9	Fehlerhafte Administration von IT-Systemen
G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten
G 3.38	Konfigurations- und Bedienungsfehler
G 3.43	Ungeeigneter Umgang mit Passwörtern

2.2.4 Technisches Versagen

G 4.8	Bekanntwerden von Softwareschwachstellen

2.2.5 Vorsätzliche Handlungen

G 5.2	Manipulation an Informationen oder Software
G 5.9	Unberechtigte IT-Nutzung
G 5.19	Missbrauch von Benutzerrechten
G 5.21	Trojanische Pferde
G 5.23	Schadprogramme
G 5.28	Verhinderung von Diensten
G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
G 5.85	Integritätsverlust schützenswerter Informationen

2.3 Maßnahmenempfehlungen

Wie unter 2.1 beschrieben setzt KIDICAP P5 auf eine bestehende Umgebung mit einzelnen Komponenten auf. Für die Absicherung dieser Basiskomponenten können die folgenden Bausteine herangezogen werden:

Systeme

B 3.107 S/390- und zSeries-Mainframe

B 3.201 Allgemeiner Client

B 3.101 Allgemeiner Server

Netze

B 4.1 Heterogene Netze

B 4.2 Netz- und Systemmanagement

B 4.4 VPN

Anwendungen

B 5.4 Webserver

B 5.7 Datenbanken

Für die erfolgreiche Implementierung sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der strategischen Entscheidung, über Planung, Konzeption und Installation bis zum Betrieb. Nicht vergessen werden darf dabei die ordnungsgemäße Aussonderung eines Systems, wenn das Ende der Betriebsphase erreicht wird.

Parallel zur Betriebsphase muss die Notfallvorsorge sicherstellen, dass der Betrieb auch im Notfall aufrecht erhalten werden kann. Informationssicherheitsmanagement und Revision stellen sicher, dass das Regelwerk auch eingehalten wird.

Die Schritte, die dabei zu durchlaufen sind sowie die Maßnahmen, die in den jeweiligen Phasen beachtet werden sollten, sind im Folgenden aufgeführt:

2.3.1 Planung und Konzeption

M 2.1	Festlegung von Verantwortlichkeiten und Regelungen
M 2.5	Aufgabenverteilung und Funktionstrennung
M 2.11	Regelung des Passwortgebrauchs
M 2.173*	Erstellung eines Software-Sicherheitskonzepts Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement Verantwortlich für Umsetzung: Leiter IT, Administrator Vor dem Einrichten einer Software sollte in einem Sicherheitskonzept beschrieben werden, welche Sicherheitsmaßnahmen in welchem Umfang umzusetzen sind. Anhand der in der Sicherheitsstrategie festgelegten Anforderungen kann dann regelmäßig überprüft werden, ob die getroffenen Maßnahmen ausreichend sind. In der Sicherheitsstrategie sollten die folgenden Fragen beantwortet werden: • Welche Dienste soll die Software anbieten? • Wer ist für die Konfiguration und den Betrieb verantwortlich? • Welche anderen Systeme und welche Netzverbindungen sind für den sicheren Betrieb der Software wichtig? Können zeitweise Störungen oder Ausfälle dieser Systeme gegebenenfalls überbrückt werden? • Wie werden die Verantwortlichen geschult, insbesondere hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen? • Welche Zugriffsbeschränkungen auf die Software sollen realisiert werden (siehe auch M 2.175 Aufbau eines Application Server)? **Vorgehen bei Sicherheitsvorfällen** In der Sicherheitsstrategie müssen auch Reaktionen auf bestimmte software-spezifische Sicherheitsvorfälle festgelegt werden (siehe auch Baustein B 1.8 Behandlung von Sicherheitsvorfällen). **Hackerangriff** Es sollte beschrieben werden, was beim Verdacht auf einen Hackerangriff auf die Software zu tun ist. Wichtig ist vor allem die Frage, wann das System notfalls vom Netz genommen werden muss und wer die

	Entscheidung dazu trifft. Teil einer Sicherheitsstrategie muss auch die regelmäßige Informationsbeschaffung über potentielle Sicherheitslücken sein, um rechtzeitig Vorsorge dagegen treffen zu können. (Siehe M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems.) Ergänzende Kontrollfragen: • Existiert eine Sicherheitsstrategie für den Betrieb der Software? • Werden die getroffenen Regelungen regelmäßig überprüft und gegebenenfalls angepasst?
M 2.256	Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb

2.3.2 Umsetzung

M 2.8	Vergabe von Zugriffsrechten
M 2.30	Regelung für die Einrichtung von Benutzern / Benutzergruppen
M 2.31	Dokumentation der zugelassenen Benutzer und Rechteprofile
M 3.3	Vertretungsregelungen
M 3.37*	Schulung der KIDICAP P5 Administratoren Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragter Um KIDICAP P5 korrekt und sicher administrieren zu können, ist eine Schulung der verantwortlichen Administratoren unumgänglich. Schon kleine Konfigurationsfehler können dazu führen, dass Sicherheitslücken entstehen. Besonders die korrekte Konfiguration von Zugangsbeschränkungen erfordert gute Kenntnisse der vorhandenen Möglichkeiten und ihrer Beschränkungen. Aufgrund der starken Interaktion zwischen den Sicherheitsmechanismen von KIDICAP P5, der ADABAS Datenbank und des zugrundeliegenden RACF bzw OS/390 Betriebssystems müssen den Administratoren des Systems auch die Sicherheitsmechanismen des Betriebssystems bekannt sein. Dies gilt auch dann, wenn die KIDICAP-Administratoren nicht gleichzeitig auch für die Administration des Betriebssystems zuständig sind. Neben den Aspekten der allgemeinen Betriebssystemsicherheit sollten folgende Aspekte Gegenstand der Schulung sein: • Konfigurationsmöglichkeiten von KIDCAP P5, Syntax der Konfigurationsdateien. • Mechanismen der Benutzerauthentisierung, Einsatzgebiete, Vor- und Nachteile der einzelnen Mechanismen. • Einrichten und Verwalten von Zugangsbeschränkungen in KIDICAP P5. • Zusammenspiel der Konfiguration von Zugangsbeschränkungen in der ADABAS Datenbank mit Zugriffsberechtigungen auf Betriebssystem- und Dateiebene.

	• Möglichkeiten zur Aufteilung von Kompetenzen zwischen den Server-Administratoren und "Redakteuren", Entwicklung von Rechte- und Rollenkonzepten. • Möglichkeiten zur Abbildung eines "organisatorischen" Rechte- und Rollenkonzepts mit Hilfe der Benutzer- und Rollenverwaltung des Betriebssystems. • Maßnahmen zur Sicherstellung der Verfügbarkeit von KIDICAP P5. • Datensicherung von KIDICAP P5. Ergänzende Kontrollfragen: • Sind die Administratoren auf den Umgang mit KIDICAP P5 vorbereitet und insbesondere in sicherheitsrelevanten Aspekten geschult? • Sind die Administratoren im Umgang mit dem genutzten Betriebssystem und seinen sicherheitsrelevanten Aspekten geschult?
M 3.52*	Schulung von KIDICAP P5 Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT Verantwortlich für Umsetzung: Administrator, Benutzer, Vorgesetzte KIDICAP P5 ist sowohl in der Administration und im Betrieb als auch in der Benutzung komplex. Alle Personen, die mit KIDICAP P5 arbeiten, müssen daher zwingend geschult werden. Dies gilt in besonderem Maße für Administratoren. (siehe M 3.37) Die Schulungsinhalte sind dem Nutzungsspektrum der zu schulenden Personen anzupassen. Ein Teil der Schulung sollte immer auch sicherheitsrelevante Themen ansprechen, so dass eine Sensibilisierung für den sicheren Umgang mit KIDICAP P5 erfolgt. Es empfiehlt sich, in regelmäßigen Abständen das Bewusstsein für die Sicherheit aufzufrischen (Security-Awareness-Programm) und auf veränderte oder neue Situationen, Mechanismen oder Verfahren hinzuweisen. Generell ist es wichtig, dass das Sicherheitsbewusstsein im Lauf der Zeit von einer rein informellen Einstellung zu einer proaktiven verändert wird. Ergänzende Kontrollfragen: • Sind Benutzer im Umgang mit dem KIDICAP P5 geschult worden? • Sind die Administratoren geschult worden? • Nutzen Administratoren regelmäßig die Online-Informationen, um sich über neue Technologien - auch bezüglich der Sicherheit - zu informieren?
M 5.88	Vereinbarung über Datenaustausch mit Dritten
Z 1.1	ADABAS Sicherheitseinstellungen ADABAS Datenbanken stellen Sicherheitsmechanismen zur Verfügung um vor unautorisierten Zugriff auf ADABAS Dateien zu schützen. Die Sicherheit wird dabei durch einen Passwort-Schutz und der verschlüsselten Speicherung von Dateien gewährleistet. Passwörter liefern einen Schutz auf Dateiebene, Datenfeldebene und Datenwertebene. Diese Sicherheitsoptionen werden innerhalb des Security Tools

	ADASCR definiert und werden in der ADABAS Security Systemdatei gespeichert. Für den Zugriff auf passwortgeschützte ADABAS Dateien muss zwingend ein Passwort eingegeben werden. Jedem Datenfeld in einer ADABAS Datei kann bis zu 15 Ebenen lesen und update Berechtigungen zugeordnet werden. Ein Benutzerpasswort spezifiziert die Berechtigung für das Datenfeld und ADABAS bestimmt automatisch, ob der Benutzer für die Funktion autorisiert ist. Wenn die Berechtigungsstufe eines Benutzerpassworts größer oder gleich dem Berechtigungslevel der Datei ist, wird der Zugriff erlaubt. Jede ADABAS Datei kann auf individueller Feldebene geschützt werden. In diesem Fall spezifiziert das Passwort Werteinschränkungen auf Einträge, die ausgewählt, gelesen und aktualisiert werden können. Mit Hilfe eines Zifferncodes kann unter Benutzung des ADACMP Tools bei der Erstellung einer ADABAS Datei diese verschlüsselt werden. Es ist zu prüfen, in welchen Bereichen der ADABAS Datenbank eine Verschlüsselung sinnvoll ist, ohne dass diese den Betrieb, beispielsweise durch Performanceeinbußen, behindert. Ergänzende Kontrollfragen: • Sind die kritischen Bereiche der ADABAS Datenbank identifiziert? • Ist für die kritische Bereiche die Verschlüsselung, bzw. der Passwortschutz eingeschaltet worden?
Z 1.2	NATURAL Sicherheitseinstellungen NATURAL stellt ein optionales Sicherheitssystem zur Verfügung, welches den Zugriff und die Benutzung der NATURAL-Umgebung einschränkt und steuert. Damit kann auch die Benutzung des gesamten Systems, einzelner Programme und Funktionen und der Zugriff auf das NATURAL Data Definition Module (DDM) eingeschränkt werden. Sicherheit wird dabei durch die Definition von Objekten und deren Beziehung zwischen den Objekten hergestellt. Es gibt drei Objekte, die für den Zugriff auf Daten durch DDMs mit dem SAS/ACCESS Interface notwendig sind: Benutzer, Libraries und Dateien. **Benutzer** …können Menschen, Computer oder Gruppen von beiden sein. Mit Hilfe eines Identifiers werden Benutzer durch das NATURAL Security-System identifiziert ind die Aktivitäten während einer Session kontrolliert. **Bibliotheken** …enthalten eine Gruppe von Programmen, Objektmodulen oder beides. Innerhalb der Bibliotheken werden ADABAS Passwörter oder Zifferncodes gespeichert, um es NATURAL Programmen zu ermöglichen mit dem ADABAS Sicherheitssystem zusammenzuarbeiten. **Dateien** sind NATURAL DDMs basierend auf ADABAS Dateien. Zwischen diesen Objekten werden Beziehungen, so genannte Links, definiert. Diese Links legen die Zugriffsrechte der Benutzer und Bibliotheken. Sämtliche Objekte werden in der NATURAL Security System Datei gespeichert, die auf die gleiche Weise mit einem Passwort oder einem Zifferncode geschützt werden kann, da sie eine ADABAS Datei ist. Es ist empfehlenswert zu prüfen, welche Bereiche der NATURAL-Umgebung

	gegen unautorisierte Änderungen geschützt werden sollten. Dies kann zum Beispiel im Hinblick auf Schutz des Produktivsystems sinnvoll sein. Ergänzende Kontrollfragen: • Sind die kritischen Bereiche der NATURAL-Umgebung identifiziert? • Ist für die kritische Bereiche die Verschlüsselung, bzw. der Passwortschutz eingeschaltet worden?

2.3.3 Betrieb

Wesentliche Bestandteile des Betriebs sind die Dokumentation von Änderungen und die laufende Kontrolle die Protokolldateien.

M 2.64	Kontrolle der Protokolldateien
M 4.210	Sicherer Betrieb des z/OS-Betriebssystems
M 4.211	Einsatz des z/OS-Sicherheitssystems RACF
M 2.35	Informationsbeschaffung über Sicherheitslücken des Systems

2.3.4 Aussonderung

M 2.320	Geregelte Außerbetriebnahme eines Servers

2.3.5 Notfallvorsorge

Wesentliche Bestandteil der Notfallvorsorge sind regelmäßige Backups und und ein Notfallplan, der aktuell ist und regelmäßig getestet wird. Im besonderen sind die folgenden Maßnahmen wichtig:

M 6.1	Erstellung einer Übersicht über Verfügbarkeitsanforderungen
M 6.22	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
M 6.88*	Erstellen eines Notfallplans für KIDICAP P5 Verantwortlich für Initiierung: Leiter IT, Informationssicherheitsmanagement Verantwortlich für Umsetzung: Administrator Der teilweise oder komplette Ausfall von KIDICAP kann in vielen Fällen gravierende Auswirkungen haben. So kann das System etwa wesentlicher Bestandteil innerbetrieblicher Arbeitsabläufe oder E-Government-Systems sein. Ein Ausfall der Anwendung hat auch den Ausfall des Gesamtsystems zur Folge. Meist ist das System mit andern Partern vernetzt, so dass ein Ausfall oder eine Störung auch schnell öffentlich bekannt wird. Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind. Folgende Aspekte müssen dabei berücksichtigt werden: • Die Notfallplanung für KIDICAP muss in den existierenden Notfallplan

	integriert werden (siehe Baustein B 1.3 Notfallmanagement). • Durch einen Systemausfall kann es auch zu Datenverlusten kommen. Daher ist ein Datensicherungskonzept für die Anwendung zu erstellen, das in das existierende Datensicherungskonzept integriert werden sollte (siehe auch Baustein B 1.4 Datensicherungskonzept). Hierin sollte nicht nur KIDICAP selbst, sondern auch das Gesamtsystem, innerhalb dessen die Anwendung eingesetzt wird, berücksichtigt werden. Dazu gehören unter Umständen Datenbanken, Applikationsserver oder Proxy-Installationen zur Lastverteilung. • Bestehen besondere Anforderungen an die Verfügbarkeit des Systems, so sollten benötigte Komponenten redundant ausgelegt werden. Beispielsweise kann der Applikationsserver oder der Nachrichtenserver redundant ausgelegt werden. • Die Anbindung an KIDICAP setzt eine funktionierende WAN oder Internet-Anbindung voraus. Bei bestimmten Konfigurationen ist auch ein korrekt funktionierender DNS-Server nötig. Ein Ausfall dieser Komponenten muss daher ebenfalls in Betracht gezogen werden. • Wird SSL eingesetzt, so muss beim Wiederanlauf des Systems auch der private Schlüssel des SSL-Zertifikates zugreifbar sein. Da dieser durch ein Passwort geschützt sein sollte, muss dieses sicher hinterlegt sein, damit es für den Wiederanlauf verfügbar ist (siehe auch M 2.22 Hinterlegen des Passwortes). • Die Systemkonfiguration ist zu dokumentieren. Wichtige Aufgaben müssen so beschrieben sein, dass das Gesamtsystem im Notfall auch ohne vorherige Kenntnis dieser Systemkonfiguration wiederhergestellt werden kann. • Es muss ein Wiederanlaufplan erstellt werden, der das geregelte Hochfahren des Systems gewährleistet. Ergänzende Kontrollfragen: • Existiert ein Notfallplan für den Ausfall von KIDICAP P5? • Gibt es entsprechende Notfallpläne für die anderen Systeme, die zum Betrieb von KIDICAP benötigt werden? • Existieren Notfallpläne für den Ausfall der Internet-Anbindung, falls das System im Internet genutzt wird? • Existiert ein Datensicherungskonzept für die Anwendung?
M 6.93	Notfallvorsorge für z/OS-Systeme
M 6.118	Überprüfung und Aufrechterhaltung der Notfallmaßnahmen
M 6.119	Dokumentation im Notfallmanagement-Prozess

2.4 Kreuzreferenztabelle

Maßnahme/ Gefährdung		G 1.1	G 1.2	G 2.7	G 2.22	G 2.26	G 2.27	G 2.28	G 2.29	G 2.66	G 2.69*	G 2.87	G 2.97*	G 3.1	G 3.3	G 3.8	G 3.9	G 3.16	G 3.38	G 3.43	G 4.8	G 5.2	G 5.9	G 5.19	G 5.21	G 5.23	G 5.28	G 5.71	G 5.85
M 2.1	(A)				X	X	X			X	X		X								X								
M 2.5	(A)			X																			X						
M 2.8	(A)			X										X				X				X	X	X					
M 2.11	(A)			X																X									
M 2.30	(A)			X														X											
M 2.31	(A)						X																	X					
M 2.35	(A)																				X								
M 2.64	(A)				X																	X	X	X					
M 2.173*	(A)									X																			
M 2.256	(A)				X	X	X			X	X																		
M 2.320	(A)																						X					X	
M 3.3	(A)	X																											
M 3.37*	(A)								X								X	X	X										
M 3.52*	(A)							X						X	X	X			X	X									
M 4.210	(A)			X																		X	X	X	X	X	X	X	X
M 4.211	(A)			X																		X	X	X	X	X	X	X	X
M 5.88	(A)						X				X	X																X	
M 6.1	(A)		X										X																
M 6.22	(B)		X										X	X		X			X										
M 6.88*	(A)		X										X																
M 6.93	(A)		X										X																
M 6.118	(B)		X										X																
M 6.119	(A)		X				X						X																
Z 1.1	(Z)																					X	X	X	X	X		X	X
Z 1.2	(Z)																					X	X	X	X	X		X	X