Kick Off: “e-Security”

Bank
Informationssicherheit

Horst Walther

Frankfurt, 30. Oktober 2001

SiG

Agenda - Begrüßung, Ablauf des Kickoffs

Start	Thema	Person
15 Uhr 00	Begrüßung, Ablauf des Kickoffs	Auftraggeber
15 Uhr 10	Vorstellung der Teilnehmer	Projektteam
15 Uhr 20	Ergebnisse der Projektvorbereitungsphase	Auftraggeber
15 Uhr 30	Systematische Einordnung der Projektaufgaben	Horst Walther
15 Uhr 45	Teilprojekte und Unteraufträge	Auftraggeber
16 Uhr 15	Verfahren des Projektmanagements	Horst Walther
16 Uhr 30	--- Ende der Veranstaltung ---	

Projektziel - Was wollen wir erreichen?

Mit Projektende soll Folgendes erreicht worden sein ...

- Es besteht **globale Evidenz** über die technische Qualität der **Internetzugänge**.
- Die Internetzugänge der Bank werden laufend auf **Schwachstellen überprüft**.
- Es ist die technische Basis für die sichere Kommunikation in **geschlossenen Benutzergruppen** geschaffen.
- Es existiert eine elektronisch abrufbare Liste der **e-Business Applikationen**. Ihre Nutzung ist weltweit bekannt.
- Die globalen *Security* ***Requirements*** an das e-Business sind dokumentiert.
- Komponenten der e-Business Architektur werden nur nach **Sicherheitsfreigabe** implementiert. Diese ist ein obligatorischer Schritt in dem global gültigen **application deployment process**.
- Es ist ein Prozess für die **Behandlung von Sicherheitsvorfällen** implementiert.
- Die **verbleibenden Risiken** sind bekannt, priorisiert und Maßnahmen geplant.

Auslöser - Warum machen wir das Projekt?

- Intern festgestellte Sicherheitslücken
  - Mangelhafte Auskunftsfähigkeit (z.B. Patch-Level)
  - Im 1. Workshop zusammengetragene Anforderungen.
- Hinweise externer Auditoren
  - Fragen nach den Gründen unterschiedlicher Verschlüsselungsstärken konnten nicht beantwortet werden.
- Deutsche Bundesbank
  - Regularien aus „*Electronic Banking aus bankenaufsichtlicher Perspektive*“

Rahmenbedingungen - Was müssen wir beachten?

- Globale Gültigkeit – Die Ergebnisse sind weltweit gültig.
- Die relevanten Regularien der Bank müssen beachtet werden ...
  - HB 001 – e-Business-Handbuch
  - HB 002 - Richtlinien zur Informationssicherheit
  - HB 003 - Mindeststandards für bankweite Projektarbeit

Tagesziel - Was wollen wir heute erreichen?

Am Ende der heutigen Veranstaltung sollen bekannt sein...

- die Projekt**ziele**,
- die **Arbeitspakete**
- **Teilprojekte** und **Unteraufträge**
- die Projekt**phasen** und **Meilensteine**,
- die *Ownership* der Arbeitspakete,
- die **Projektorganisation** und die **Verfahren** des Projektmanagements.

Agenda - Vorstellung der Teilnehmer

Start	Thema	Person
15 Uhr 00	Begrüßung, Ablauf des Kickoffs	Auftraggeber
15 Uhr 10	Vorstellung der Teilnehmer	Projektteam
15 Uhr 20	Ergebnisse der Projektvorbereitungsphase	Auftraggeber
15 Uhr 30	Systematische Einordnung der Projektaufgaben	Horst Walther
15 Uhr 45	Teilprojekte und Unteraufträge	Auftraggeber
16 Uhr 15	Verfahren des Projektmanagements	Horst Walther
16 Uhr 30	--- Ende der Veranstaltung ---	

Die Projektteilnehmer stellen sich vor ...

- Aus welchen Unternehmen, Einheiten kommen Sie?
- Welche Rolle nehmen Sie im Projekt wahr? (Projektarbeit, Projektleitung, Projektverantwortung, Review ...)
- An welchen inhaltlichen Schwerpunkten möchten Sie mitwirken?
- Welchen spezifischen Interessenschwerpunkt werden Sie vertreten?

Agenda - Ergebnisse der Projektvorbereitungsphase

Start	Thema	Person
15 Uhr 00	Begrüßung, Ablauf des Kickoffs	Auftraggeber
15 Uhr 10	Vorstellung der Teilnehmer	Projektteam
15 Uhr 20	Ergebnisse der Projektvorbereitungsphase	Auftraggeber
15 Uhr 30	Systematische Einordnung der Projektaufgaben	Horst Walther
15 Uhr 45	Teilprojekte und Unteraufträge	Auftraggeber
16 Uhr 15	Verfahren des Projektmanagements	Horst Walther
16 Uhr 30	--- Ende der Veranstaltung ---	

Up front – Aktivitäten I

- Experten- und Lieferantengespräche (25.05 - 18.06.01)
- Zwei Projektdefinitionsworkshops
  - 20.06.2001 und 17.07.2001
- Projektmeetings mit auftraggebenden Abteilungen
- Drei Auftragsbesprechungen mit dem Zertifikatsanbieter
  - Produktvorstellung
  - InAuftraggeberation + Test
  - Bewertung
  - Auftragsvergabe (zwei Gespräche vor Ort)
- InAuftraggeberation der *Bank Private Onsite*
- Projektbesprechungen mit dem Auftraggeber
  - 12.10. 2001 und 22.10.2001
- Anbieterauswahl / Auftragsbesprechung mit Scanning-Anbieter

Up front – Aktivitäten II

- Eingebundene Abteilungen der Bank und Bank Systems ...
  - Bank Systems (Bankbasissysteme / Ausland / Security)
  - Bank Systems (e-Solutions)
  - Bank Systems (Engineering)
  - Bank London (Information Security)
  - Bank Frankfurt (IT-Revision)
  - Bank Frankfurt (e-Business Group)
  - Bank (IT-Strategie)

Agenda - Systematische Einordnung der Projektaufgaben

Start	Thema	Person
15 Uhr 00	Begrüßung, Ablauf des Kickoffs	Auftraggeber
15 Uhr 10	Vorstellung der Teilnehmer	Projektteam
15 Uhr 20	Ergebnisse der Projektvorbereitungsphase	Auftraggeber
15 Uhr 30	Systematische Einordnung der Projektaufgaben	Horst Walther
15 Uhr 45	Teilprojekte und Unteraufträge	Auftraggeber
16 Uhr 15	Verfahren des Projektmanagements	Horst Walther
16 Uhr 30	--- Ende der Veranstaltung ---	

Ziele und Maßnahmen

Um unsere Sicherheitsziele zu erreichen müssen wir drei Schutzaufgaben wahrnehmen.

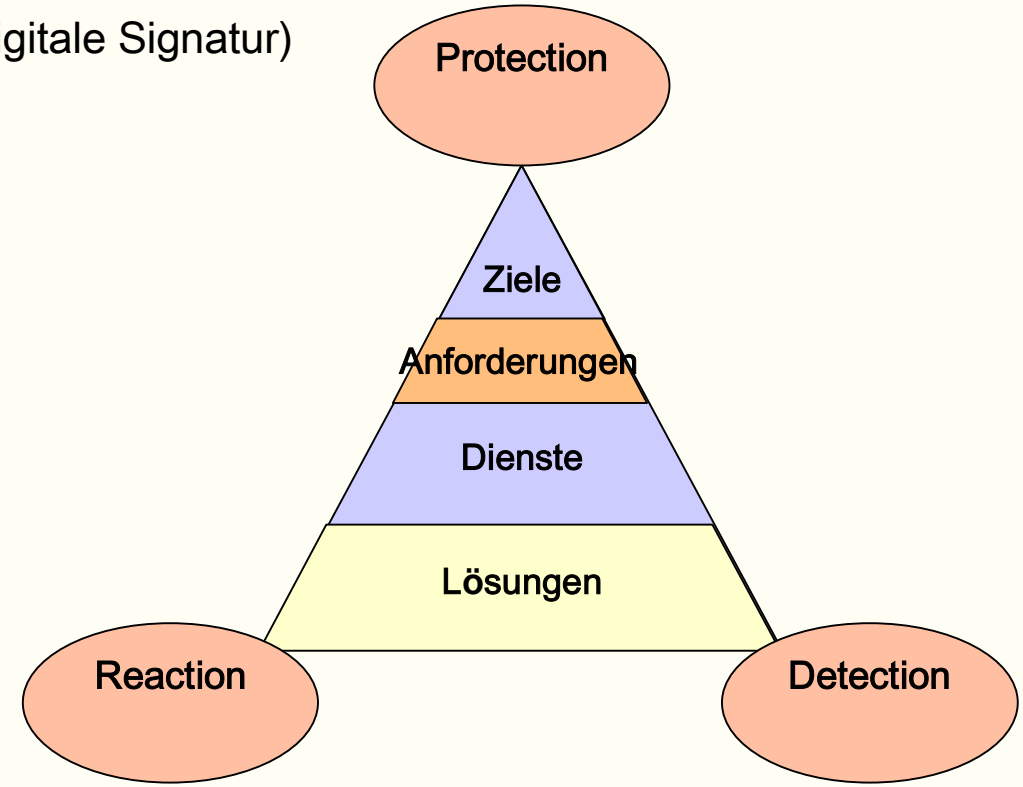
Sicherheitsziele	Schutzaufgaben

▸ Authentizität
▸ Integrität
▸ Verbindlichkeit
▸ Verfügbarkeit
▸ Vertraulichkeit
	■ *Protection*
	  ▸ vorbeugende Schutzmaßnahmen
	■ *Detection*
	  ▸ Aufdecken von Schutzverletzungen
	■ *Reaction*
	  ▸ Gegenmaßnahmen bei Schutzverletzungen

Maßnahmen und Dienste

Die Aufgaben werden durch generische IT-Sicherheitsdienste ermöglicht ...

- Protection
  - Administration
  - Authentifikation (Digitale Signatur)
  - Autorisierung
  - Datenträgerschutz
  - Dokumentation
  - Identifikation
  - Notfallplanung
  - Verschlüsselung
  - Zugangsschutz
- Detection
  - Protokollierung
  - Überwachung
- Reaction
  - Untersuchung



Generische IT-Sicherheitsdienste I

- Administration
  - Funktionen zur Verwaltung sicherheitstechnischer Einstellungen für die verwendete Hardware und Software
- Authentisierung
  - Funktionen zur Überprüfung der Echtheit bzw. Korrektheit von Identifikations-Informationen (z.B.: durch Digitale Signatur, dem elektronischen Gegenstück der handschriftlichen Unterschrift, deren rechtliche Stellung in entsprechenden Gesetzen auf Bundes- und EU-Ebene geregelt ist)s.
- Autorisierung
  - Funktionen zur Prüfung von Zugriffsberechtigungen (inkl. Segregation of duties, d.h.: Explizite Trennung von Rechten, deren Ausübung durch eine Person Konflikte verursachen kann.)
- Datenträgerschutz
  - Funktionen, die den Zugang zu Informationen auf der physikalischen Datenträger-Ebene kontrollieren
- Dokumentation
  - Gesamtheit aller in Schriftform niedergelegten Regeln und Richtlinien zur Sicherheit von IT-Systemen und Daten
- Identifikation
  - Funktionen, die verschiedenen Systemelementen (Benutzern, Ressourcen, Rechnern) eindeutige Merkmale zuordnen
- Notfallmanagement
  - Vorgehensweisen und technische Einrichtungen, um die Auswirkungen von IT-Problemsituationen zu beherrschen

Generische IT-Sicherheitsdienste II

- Management von Sicherheitsvorfällen
  - Vorgehensweisen und technische Einrichtungen, um die Auswirkungen von IT-Problemsituationen zu beherrschen
- Protokollierung
  - Funktionen zur (passiven) Aufzeichnung von Aktivitäten der Systemelemente
- Überwachung
  - Funktionen, mit denen Systemeinstellungen und Aktivitäten von Systemelementen aktiv kontrolliert und getestet werden können
- Untersuchung
  - Vorgehensweisen, die bei festgestellten Sicherheitsvorkommnissen zum Einsatz kommen
- Verschlüsselung
  - Funktionen, die sowohl ruhende als auch bewegte Daten mit kryptographischen Methoden absichern
- Zugangsschutz
  - Vorgehensweisen und technische Einrichtungen, um die physische Erreichbarkeit von Systemen zu steuern

Lösungen I

#.	Generischer IT-Sicherheitsdienst	Lösung
1.	Administration	s. eProvisioning-Projekt, Netzwerkkonsolidierung
2.	Authentication	Authentication Layer, Softwarezertifikate, Hardwarezertifikate (Identrus, EU Signatur)
3.	Autorisierung	Benutzergruppen, zentral. Autorisierungssystem, Rollen Segregation of Duties
4.	Datenträgerschutz	...
5.	Dokumentation	Online Evidenz e-Business Applikationen und Systemevidenz, HB001-Regeln für e-Business Security, Dokumentation der Komponenten der Sicherheitsarchitektur (aktuell, online verfügbar)
6.	Identifikation	Authentication Layer, Zertifikate
7.	Management von Sicherheitsvorfällen	Incidenthandling / Eskalationsverfahren

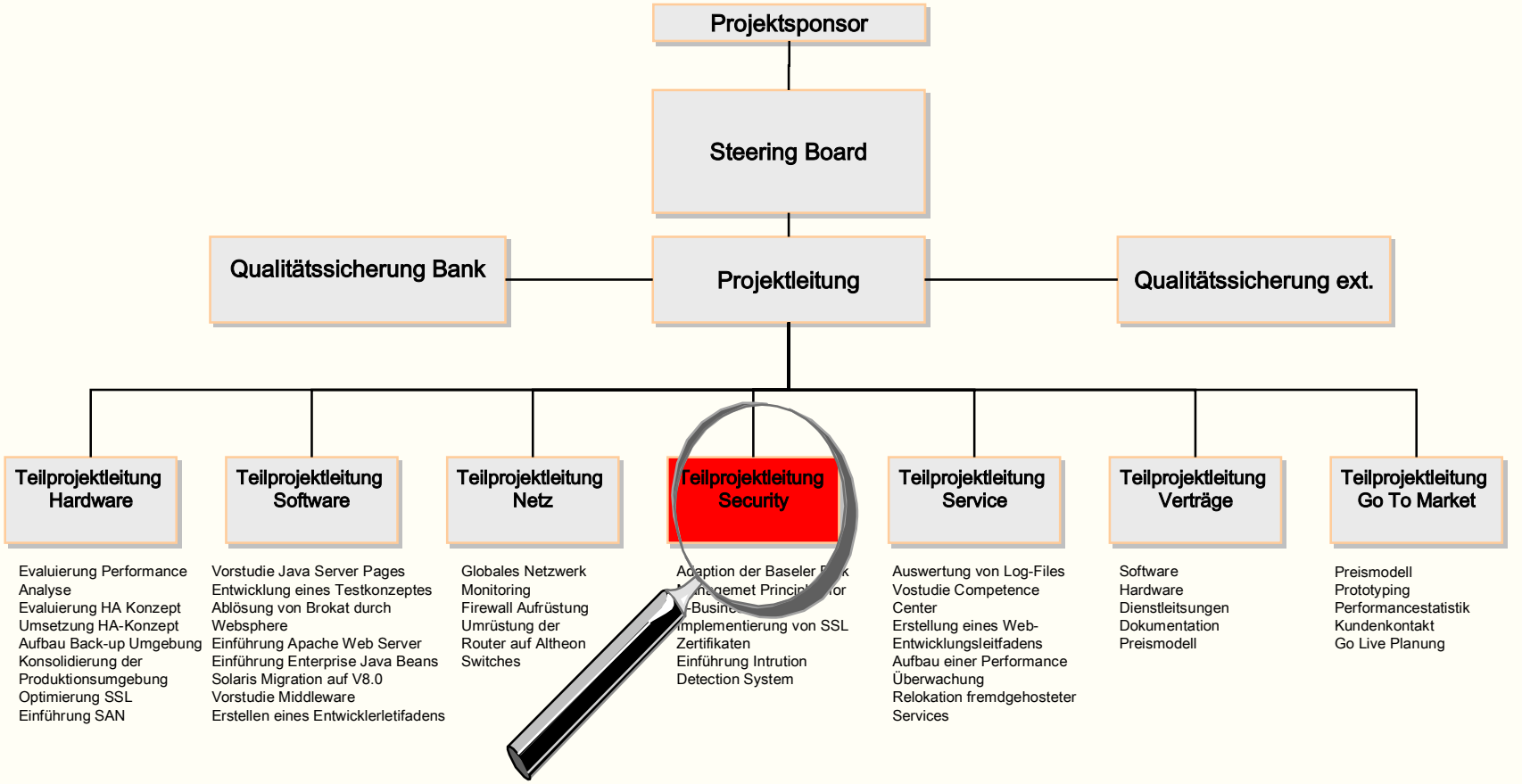
Lösungen II

#.	Generischer IT-Sicherheitsdienst	Lösung
8.	Protokollierung	Systemlogging Mechanismen, IDS
		...
10.	Überwachung	Sicherheits-Check, IDS
11.	Untersuchung	Managed Security Monitoring Services
12.	Verschlüsselung	SSL, X.509 Zertifikate (ggf. SAP Zertifikate)
13.	Zugangsschutz	...

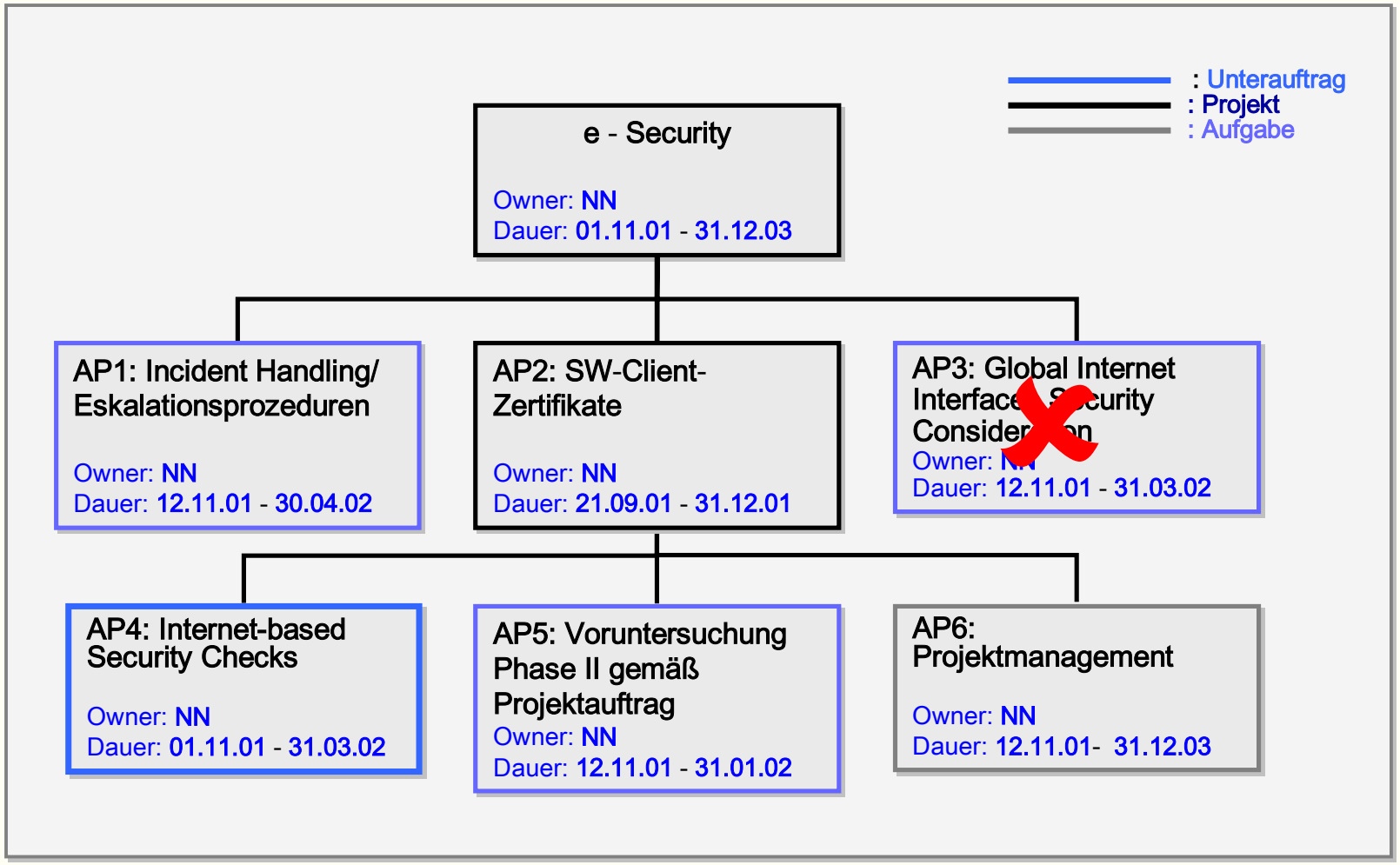
Agenda - Teilprojekte und Unteraufträge

Start	Thema	Person
15 Uhr 00	Begrüßung, Ablauf des Kickoffs	Auftraggeber
15 Uhr 10	Vorstellung der Teilnehmer	Projektteam
15 Uhr 20	Ergebnisse der Projektvorbereitungsphase	Auftraggeber
15 Uhr 30	Systematische Einordnung der Projektaufgaben	Horst Walther
15 Uhr 45	Teilprojekte und Unteraufträge	Auftraggeber
16 Uhr 15	Verfahren des Projektmanagements	Horst Walther
16 Uhr 30	--- Ende der Veranstaltung ---	

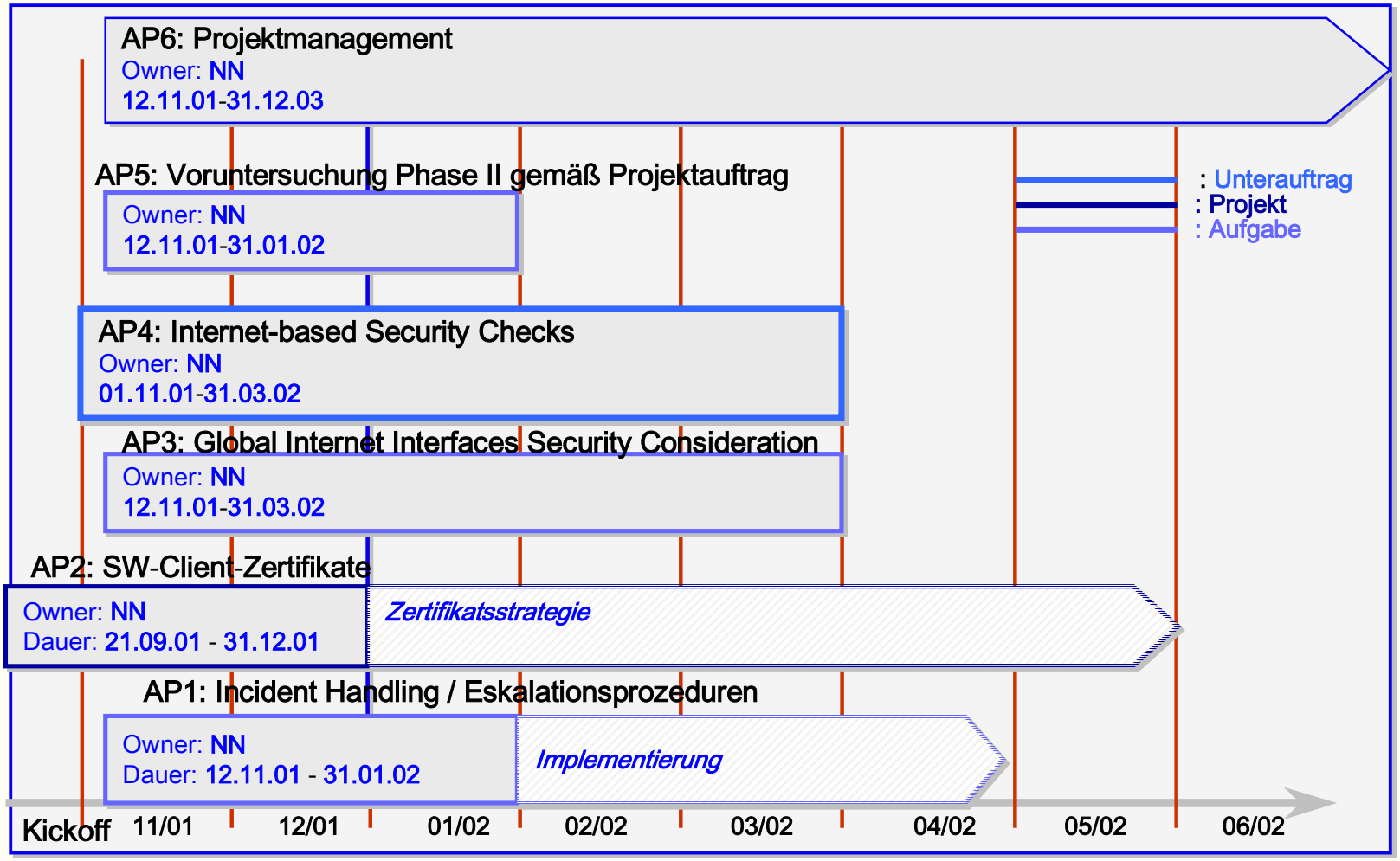
Einbindung von e-Security



Arbeitspakete - *work breakdown structure*



Zeitliche Abfolge der Arbeitspakete



AP1: Incident Handling/ Eskalationsprozeduren

- Beschreibung
  - Erfassen und Auswerten der bekannten Regularien für Incident Handling / Eskalationsprozeduren.
  - Definition von Eskalationsprozeduren / Incident Handling im Falle von IT-Sicherheitsverletzungen.
  - Abstimmung mit den zuständigen Stellen der Bank und ihrer Tochtergesellschaften.
- Ergebnis
  - Dokumentierte und abgestimmte Prozessdefinitionen für IT-Sicherheitsalarmfälle.

AP2: SW-Client-Zertifikate

- Beschreibung
  - Evaluierung des Einsatzes SW - Client Zertifikaten für die Nutzung zur Kommunikation im Internet.
- Ziel
  - Eine Bank-eigene PKI unter Nutzung der Zertifikatsdienstleistung des Anbieters.
- Aufgaben
  - Absprache mit dem Anbieter
  - Durchführen von Labortests
  - Entscheidung und Entwurf der Lösung
  - Erstellen der Dokumentation
  - Erstellen einer Policy
  - Durchführen eines Piloten
  - Abstimmen und Definieren der erforderlichen Prozesse
  - Überprüfen und Abstimmen des Ergebnisses.

AP3: Global Internet Interfaces Security Consideration I

- Beschreibung
  - Schaffen von Evidenz über die Sicherheitssituation an 50 Standorten.
  - Konzept der Absicherung der weltweiten Bank Internetzübergänge.
    - Reduktion auf sicher zu gestaltende Zugänge
    - Vereinheitlichung von Technologie und Administration
    - Betrachtung auch extern „gehosteter“ Infrastruktur.
- Ergebnis
  - Aufstellung der Internetübergänge der Bank weltweit (Lokationen, Provider, ...)
  - Dokumentation des Bedrohungspotentials
  - Maßnahmenempfehlung

AP3: Global Internet Interfaces Security Consideration II

- Vorbehalt ...
  - Entscheidung im e-Kernteam am 31.10.2001
- Schritte ...
  - Evidenzerstellung ...
    - Erstellen einer Checklist (Excel oder Web–basiert): Bank-Systemhaus
    - Versenden mit Begleitbrief an 50 Ansprechpartner: Auftraggeber
    - Auswerten auf Sicherheitsmängel hin: Bank-Systemhaus

  ... Bis zum Jahresende 2001 ...
  - Mängelbeseitigung
    - Erarbeiten der Maßnahmenempfehlung zur Mängelbeseitigung
    - Versenden einer Aufforderung zur Mängelbeseitigung (Bei Bedarf) : Sponsor
    - Eskalieren (bei Bedarf) : Auftraggeber

AP4: Internet-based Security Checks I

- Beschreibung
  - Externe Sicherheits-Checks der Bank Internet-Umgebung
- Erwartetes Ergebnis
  - regelmäßiger Bericht über festgestellte Schwachstellen der Bank-Internetumgebung
  - Je nach Auftrag bis zu 7 x 24 Stunden Supportbereitschaft im Incident-Fall
  - Sicherheitswarnungen und Maßnahmen zur Behebung
- Status:
  - Bis zum 29. Oktober 2001 lagen gute Angebote vor

AP4: Internet-based Security Checks II

- Zwei Angebote werden nicht weiter betrachtet
- Zwischen zwei Angeboten werden wir wählen ...
- Weitere Beschlüsse ...
  - Die Reports (incl. Mgt. Summary) werden an den Auftraggeber
  - Die Scanning Termine werden unregelmäßig festgelegt.
  - Den Datensicherungsbeauftragen informieren
- Schritte ...
  - Gespräche führen, um präzisere Angebote zu erhalten: Auftraggeber
  - Testbeauftragung: Scan durch beide Anbieter an einem Tag (07:11): Auftraggeber
  - Entscheidungsvorschlag z.Kt. an Sponsor senden.: Auftraggeber

AP5: Voruntersuchung Phase II gemäß Projektauftrag I

- Folgende Punkte werden untersucht und bewertet ...
  - User Administration
  - System Administration
  - Security Monitoring /Auditing / Incident Recognition
  - Backup / Restore / Archivierung
  - Handbuch 001
  - Architekturen für die sichere Authentifizierung
  - Update Prozesse (Sicherheitspatches, Virenschutz)
  - Outsourcing Security
  - Untersuchung der Verwendbarkeit von SAP Zertifikaten
  - Internet Explorer Konfiguration
  - Untersuchung „gehärteter“ Betriebssysteme z.B. Pitbull / secure IIS
  - Untersuchung von EAM Infrastrukturlösungen für die sichere Verwaltung von E-Commerce-Portalen (Extranet Access-Markt (EAM)) z.B. Netegrity SiteMinder-Plattform
  - Sicherheitsfreigabeprozess für den Einsatz von e-Business Applikationen
  - Einsatz von Checksummenprogrammen
  - Untersuchung der e Business der Ausfallsicherheitskonzepte
  - Erstellung Application Hoster Questionaire.

Projektrahmen

- Aufwand:
  - AP1: Incident Handling, 40 PT
  - AP2: SW-Client Zertifikate, 60 PT
  - AP3: Global Internet Interfaces Security Consideration, 80 PT
  - AP4: Internet based Security Checks, operativer Betrieb, wöchentliche Tests
  - AP5: Voruntersuchungsaktivitäten, 40 PT
  - AP6: PM, ca. 50 PT (bis 31.03.02)
- Laufzeit: ca. 25 Monate

Agenda - Verfahren des Projektmanagements

Start	Thema	Person
15 Uhr 00	Begrüßung, Ablauf des Kickoffs	Auftraggeber
15 Uhr 10	Vorstellung der Teilnehmer	Projektteam
15 Uhr 20	Ergebnisse der Projektvorbereitungsphase	Auftraggeber
15 Uhr 30	Systematische Einordnung der Projektaufgaben	Horst Walther
15 Uhr 45	Teilprojekte und Unteraufträge	Auftraggeber
16 Uhr 15	Verfahren des Projektmanagements	Horst Walther
16 Uhr 30	--- Ende der Veranstaltung ---	

AP6: Projektmanagement

- Projektakte - Wie werden die Projektergebnisse dokumentiert und kommuniziert ?
- Berichtswesen - Wer wann an wen?
- Qualitätssicherung - Wie ist sie organisiert ?
- Projektbesprechungen - Wer trifft sich wann und wo?
- Standards - Welche Bank-Standards sind zu beachten?

Projektakte – für die Ablage der Ergebnisse

- Projektergebnisse werden in einer **Projekte-Akte** abgelegt.
- **Ergebnisse** der Projektarbeit werden erst nach einem - erfolgreich durchlaufenen - internen Review zu Projektergebnissen.
- Auf die Projektakte erhalten das **Projektteam** und der **Reviewerkreis** Schreibzugriff.
- Sie können sich **Repliken** halten.
- **Projektergebnisse** kann nur der PL (bzw. sein Stellvertreter) gültig oder ungültig setzen. Er kann sie weder ändern noch löschen.
- Den aktuellen Reviewern werden die zu beurteilenden Dokumente zugestellt (**Bringschuld**), für die Teammitglieder sind sie **Holschuld**.
- **PM-Dokumente** werden ebenfalls in der Projektakte abgelegt.
  - Protokolle, Projektberichte, Planungen, Soll- / Ist-Vergleiche

Berichtswesen - Wer wann an wem?

- Wochenberichte - Die Projektmitarbeiter berichten an den PL.
- Turnus ist wöchentlich (jeweils Montag Mittag)
- Es sind die Bank-Formulare zu verwenden
  - Formulare werden gestellt
- Der PL konsolidiert die Wochenberichte und erstellt einen monatlichen Statusbericht.
- Die Statusberichte werden zusätzlich als pdf-Dokument in der Projektakte abgelegt.

Qualitätssicherung - Wie ist sie organisiert?

- Projektergebnisse werden in Reviews geprüft und freigegeben.
- Es sind 2 Arten von Reviews vorgesehen ...
  - **Interne** Reviews - innerhalb des Projektteams
  - **Projektreviews** - im Kreis der je AP nominierten Reviewer für die Abnahme von Projektergebnissen.
  - **Reviewer** für Projektreviews sind je Arbeitspaket benannte Experten.
- In den Projektreview werden Dokumente ...
  - bei Abwesenheit von Mängeln **freigegeben**
  - Bei Anwesenheit leichter Mängel mit **Nachbesserungsauflagen** freigegeben
  - Bei Anwesenheit schwerer Mängel **zurückgewiesen**
- Nach erstmalig erfolgreich durchlaufenem Review erhält ein Dokument die Versionsnummer 1.0.
- Reviewmeetings werden protokolliert
  - Dokumentation der Reviews in der **Projektakte**
  - **Versandt** an die Teilnehmer und Projektteam

Projektbesprechungen - Wer wann und wo?

- Projekt jour fixe - Jeden Donnerstag, 14:00 -16:00
- Teilnehmer sind die jeweils aktiven Mitarbeiter im Projektteam und ggf. geladene Gäste.
- Ort ist Besprechungsraum 100, Oberstraße 19
- Es wird ein Protokoll angefertigt, an die Teilnehmer versandt und in der Projektakte gespeichert
- Der PL kann einen Projekt jour fixe bei Mangel an Bedarf absagen.

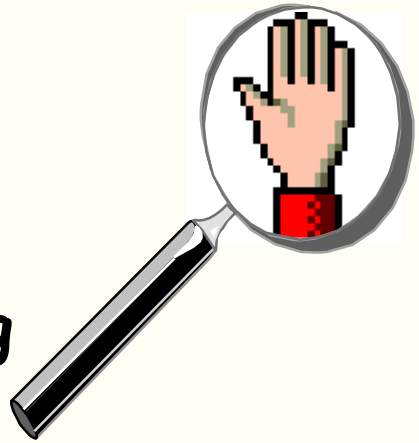
Standards - Welche sind zu beachten?

- Das Projekt orientiert sich am „Handbuch 003„
- Die Ergebnisse werden im Format von Microsoft Office 97 oder Office 2000 erarbeitet
- Die Ergebnisse werden im PDF-Format publiziert.
- Die Projektakte zur Ablage von Projektergebnissen und Projektmanagementdokumentation ist eine Lotus Domino Dokumentenbank.
- Zur Kommunikation verwenden wir Internet-Mail oder Lotus NOTES (Text, RTF, HTML)
- Über das Internet versandte Dokumente werden mittels PGP (Pretty Good Privacy) verschlüsselt. Die öffentlichen Schlüssel aller Projektbeteiligten werden in der Projektakte abgelegt.

Agenda - Ende der Veranstaltung

Start	Thema	Person
15 Uhr 00	Begrüßung, Ablauf des Kickoffs	Auftraggeber
15 Uhr 10	Vorstellung der Teilnehmer	Projektteam
15 Uhr 20	Ergebnisse der Projektvorbereitungsphase	Auftraggeber
15 Uhr 30	Systematische Einordnung der Projektaufgaben	Horst Walther
15 Uhr 45	Teilprojekte und Unteraufträge	Auftraggeber
16 Uhr 15	Verfahren des Projektmanagements	Horst Walther
16 Uhr 30	--- Ende der Veranstaltung ---	

Achtung Anhang



Hier kommen die berüchtigten back-up-Folien ...