eSI - Der elektronische Sicherheitsinspektor

Unterstützung für eine kontinuierliche Überprüfung von

IT-Sicherheitsmaßnahmen in Unternehmensnetzen

Heinz Sarbinowski

sarbi@sit.fraunhofer.de

Fraunhofer Institut
Sichere Telekooperation

Inhalt

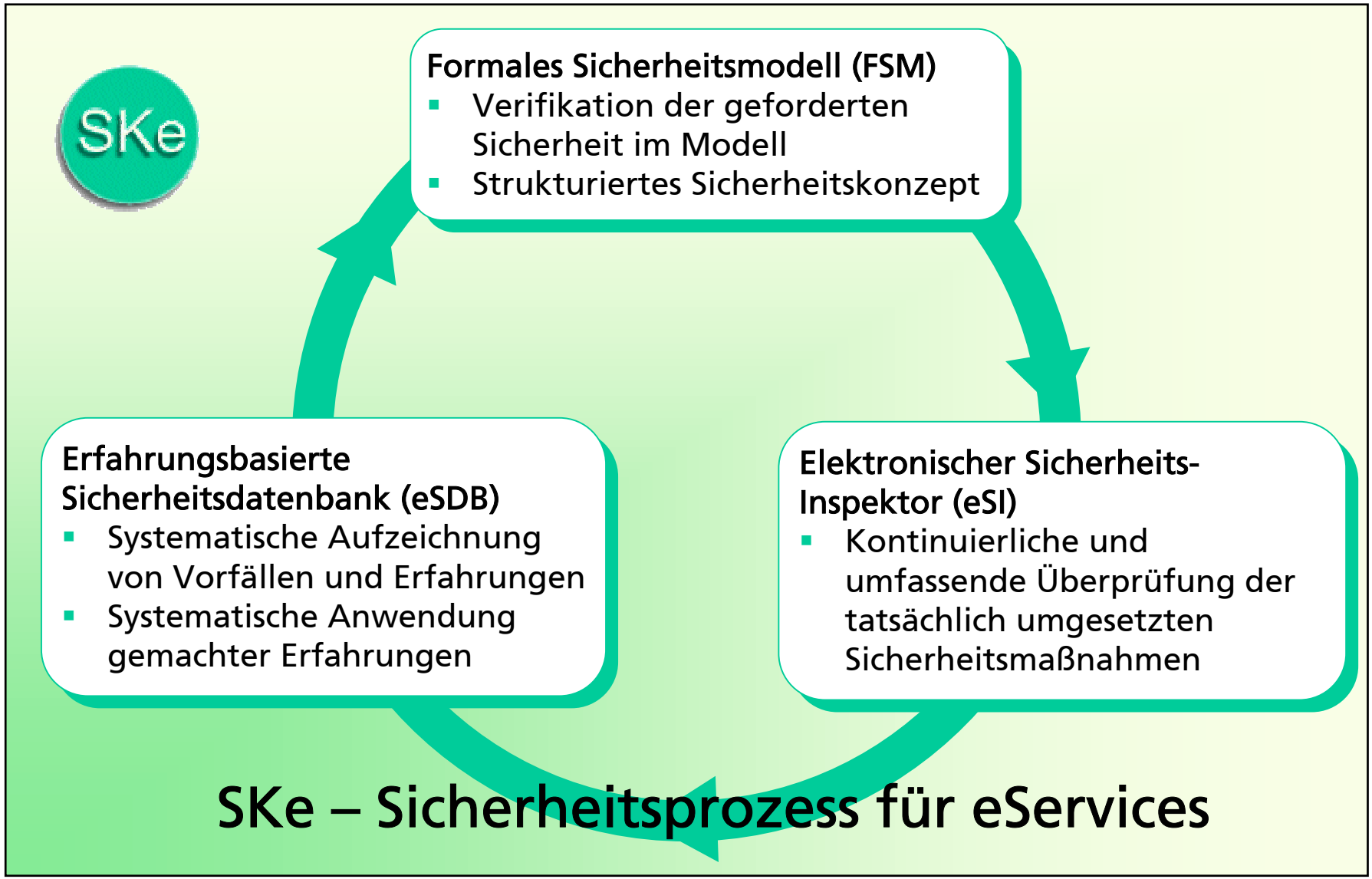
- eSI im Projekt SKe
- IT-Sicherheitsmaßnahmen
- Vorgehensmodell zur automatisierten Überprüfung
- eSI Komponenten / Funktionen
- eSI Maßnahmenüberprüfungen

Fraunhofer Institut
Sichere Telekooperation

eSI im Projekt SKe

- SKe „Durchgängige Sicherheitskonzeption mit dynamischen Kontrollmechanismen für eService-Prozesse“
  - BMBF Förderprojekt im Programm „Leben und Arbeiten in einer vernetzten Welt“ (Mai 2001 bis Dezember 2003)
  - Formales Sicherheitsmodell, Angriffsimulator, strukturiertes Sicherheitskonzept
  - elektronischer Sicherheitsinspektor eSI
  - Erfahrungsbasierte Sicherheitsdatenbank, Aufzeichnen von Vorfällen, Diagnose von Vorfällen, Handlungsempfehlungen

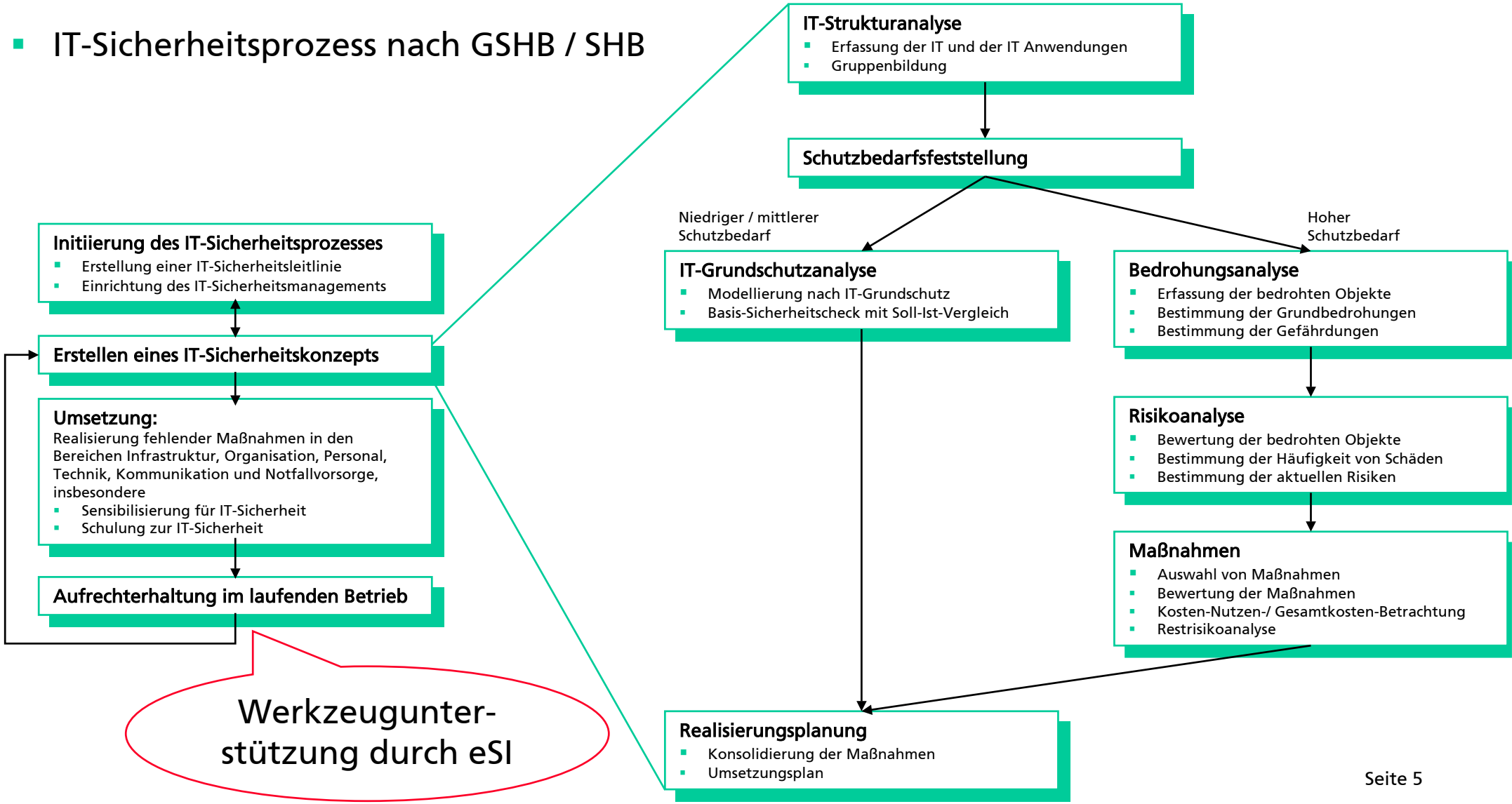
eSI im Projekt SKe



Fraunhofer Institut Sichere Telekooperation

IT-Sicherheitsmaßnahmen

- IT-Sicherheitsprozess nach GSHB / SHB



SIT
Fraunhofer Institut Sichere Telekooperation

IT-Sicherheitsmaßnahmen

Werkzeugeinordnung des eSI

Werkzeuge für:

- Erstellen von Sicherheitskonzepten (GSTOOL, „textorientiert“)
- Umsetzung von IT-Sicherheitsmaßnahmen
  - Teils händisch, teils Werkzeug-unterstützt
  - Teils automatisierte Umsetzung bei Produkt-bezogener Konfiguration (Policy enforcement: Windows Richtlinien, ePolicy Orchestrator)
- Überprüfung auf Schwachstellen (Vulnerability scanner: „Baseline Security Scanner“, Nessus)
  - Bekannte Programmfehler (bugs) in Standardprodukten (Server, PCs, E-Mail...)
  - Bekannte Konfigurationsfehler in Standardprodukten (Server, PCs, E-Mail...)
- Überprüfung von IT-Sicherheitsmaßnahmen (Sicherheitsaudit,...)

IT-Sicherheitsmaßnahmen

Werkzeugeinordnung des eSI (1)

- Security Audit 2003/2004
  - Checklisten für Interviews, Begehungen, Security Scans

    „Jede Checkliste enthält außer den durchzuführenden Arbeiten ein Bewertungsschema, um den Erfüllungsgrad jeder Prüfung zu messen. Zusätzlich gibt es k.o.-Kriterien, ohne deren Bestehen das Fazit einer Prüfung „durchgefallen" lautet."
  - Werkzeuge
    - Portscanner: nmap (Unix), MingSweeper (Windows)
    - Security Scanner: nessus (Unix), LANguard Network Security Scanner (Windows), N-Stealth (Windows-Tool für den Scan von Webservern)
    - Integritäts-Checker: AIDE (Unix), Tiger (Unix)
    - Prüfung von Passwörtern: LC4 (Windows), Crack (Unix)
    - Registry-Tools: doeskey (Windows)

IT-Sicherheitsmaßnahmen

earbeiten

rüfungskatalog Internet-PC

eferenz: BSI-Baustein 5.8

ame des Erstellers: Datum:

Nr.	Durchzuführende Arbeit	e?	Testmethode	k.o.	Prio	EG	verantwortlich	Bemerkungen	Unterformulare	B R
1	Kontrolle der Aufstellung eines IT-Systems (Interview und Begehung erforderlich)	☐	☐ Interview ☐ Begehung		3				Löschen Öffnen Neu anlegen	M
2	Kontrolle der Konzeption von Internet-PCs	☐	☐ Interview	K.O.	1				Löschen Öffnen Neu anlegen	M
3	Kontrolle der Richtlinien für die Nutzung von Internet-PCs	☐	☐ Interview		2				Löschen Öffnen Neu anlegen	M
4	Kontrolle der Schulung vor Programmnutzung	☐	☐ Interview		1				Löschen Öffnen Neu anlegen	M
5	Kontrolle der Schulung zu IT-Sicherheitsmaßnahmen	☐	☐ Interview		1				Löschen Öffnen Neu anlegen	M
6	Kontrolle des regelmäßiges Einsatzes eines Virensuchprogramms	☐	☐ Interview		1				Löschen Öffnen Neu anlegen	M
7	Kontrolle von PC-Sicherheitsprodukten	☐	☐ Interview ☐ Penetrationstest		1				Löschen Öffnen Neu anlegen	M
8	Kontrolle der Prüfung eingehender Dateien auf Makro-Viren	☐	☐ Interview		1				Löschen Öffnen Neu anlegen	M
9	Kontrolle der sicheren Installation von Internet-PCs	☐	☐ Interview ☐ Begehung	K.O.	1				Löschen Öffnen Neu anlegen	M
10	Kontrolle des sicheren Betriebs von Internet-PCs	☐	☐ Interview		2				Löschen Öffnen Neu anlegen	M

GI-SECMGT 040206

Fraunhofer SIT Institut Sichere Telekooperation

IT-Sicherheitsmaßnahmen

Werkzeugeinordnung des eSI (2)

- Prüfschema für Auditoren (BSI, Qualifizierung/Zertifizierung nach IT-Grundschutz)
  - Überprüfung „nach Aktenlage“ (Referenzdokumente)
  - Inspektion vor Ort
    - ...„Der Auditor überprüft vor Ort die Umsetzung aller Maßnahmen des Bausteins „IT-Sicherheitsmanagement“ für den IT-Verbund.“
    - Zusätzlich zur Überprüfung des Management-Bausteines sind Stichproben aus den fünf Schichten "Übergeordnete Aspekte", "Infrastruktur", "IT-Systeme", "Netze" und "Anwendungen" zu wählen.“
    - „Die Prüfung der einzelnen Maßnahmen sollte direkt am Zielobjekt erfolgen, nicht nur anhand der Papierlage. Bei technischen Maßnahmen bedeutet dies eine Demonstration durch den jeweils zuständigen Administrator oder Vertreter. Der Auditor sollte nicht selbst in das System eingreifen.“...

IT-Sicherheitsmaßnahmen

Wer kontrolliert die Einhaltung der IT-Sicherheitsmaßnahmen?

- Überhaupt kontrolliert
- Der Sicherheitsbeauftragte
- Sicherheitsrevision / Auditing
- Gelegentlich / einmal im Jahr
- Stichprobenartig
- Checkliste „textorientiert“

IT-Sicherheitsmaßnahmen

Der elektronische Sicherheitsinspektor (eSI)

kontrolliert die Einhaltung der IT-Sicherheitsmaßnahmen

Mit Hilfe von elektronischen Checklisten kann eine derartige Überprüfung

- kontinuierlich und
- umfassend (nicht nur Stichproben)

automatisiert durchgeführt werden

Fraunhofer Institut
Sichere Telekooperation

IT-Sicherheitsmaßnahmen

Welche Maßnahmen sind automatisiert überprüfbar?

- Generell: nur technisch überprüfbare Maßnahmen
  - Organisatorische Maßnahmen (Richtlinien) im Einzelfall
    - „Auf den Arbeitsplatzrechnern dürfen keine privaten Programme installiert werden“: eher ja
    - „Die Mitarbeiter sind über die aktuellen Datenschutzrichtlinien zu informieren“: eher nein
  - Technische Maßnahmen: grundsätzlich ja
  - Qualität der Prüfergebnisse (Messstellen, Prüfwerkzeuge)
- Aufwand für die Überprüfung ist abzuwägen
  - Beim Prüfwerkzeug-Hersteller
    - Standard- / Individualfälle, Aktualisierung
  - Beim Unternehmen
    - Werkzeugeinsatz, Konfigurationsmanagement / Inventarisierung, spezielle Messstellen

SIT
Fraunhofer Institut
Sichere Telekooperation

IT-Sicherheitsmaßnahmen

Prüfverfahren für Maßnahmen

- „Verhaltensprüfung“ des Objekts (tut es, was es tun soll?)
- Konfigurationsprüfung (korrekte Konfiguration bewirkt korrektes Verhalten)

Prüfwerkzeugimplemetierung

- Zentrale Implementierung (etwa Portscanner)
- Verteilte Implementierung (etwa zentraler Abruf der Messwerte von lokal installierten „Agenten“)

IT-Sicherheitsmaßnahmen

Welche Maßnahmen werden vom eSI überprüft?

- „Standard“-Maßnahmen
  - Grundschutzhandbuch
  - SANS Top 20
- Individuelle Maßnahmen
  - Unternehmens- / Anwendungsspezifisch

Generell: nur technisch überprüfbare Maßnahmen

Vorgehensmodell zur automatisierten Überprüfung

Schritt 1

- Person prüft mit Hilfe eines „Standard- / Spezialwerkzeuges“ die korrekte Umsetzung / Einhaltung einer Maßnahme
  - Gliederung in zu prüfende Teilmaßnahmen
  - Kriterien für Umsetzung bestimmen (zu prüfende Messwerte, „Messstellen“, „Qualität“)
  - Werkzeug auswählen
  - Bedienung lernen
  - Prüfauftrag eingeben
  - Prüfergebnisse interpretieren und auswerten

Vorgehensmodell zur automatisierten Überprüfung

Schritt 1

Wissen über
- den Umgang mit Sicherheitsmaßnahmen
- die Prüfung von Umsetzungszuständen
- Umgang mit Prüfwerkzeugen
- die Interpretation der Prüfergebnisse und der Auswertungsergebnisse

Sicherheitsbeauftragter
Sicherheitsaudit /-revision

Prüfwerkzeug

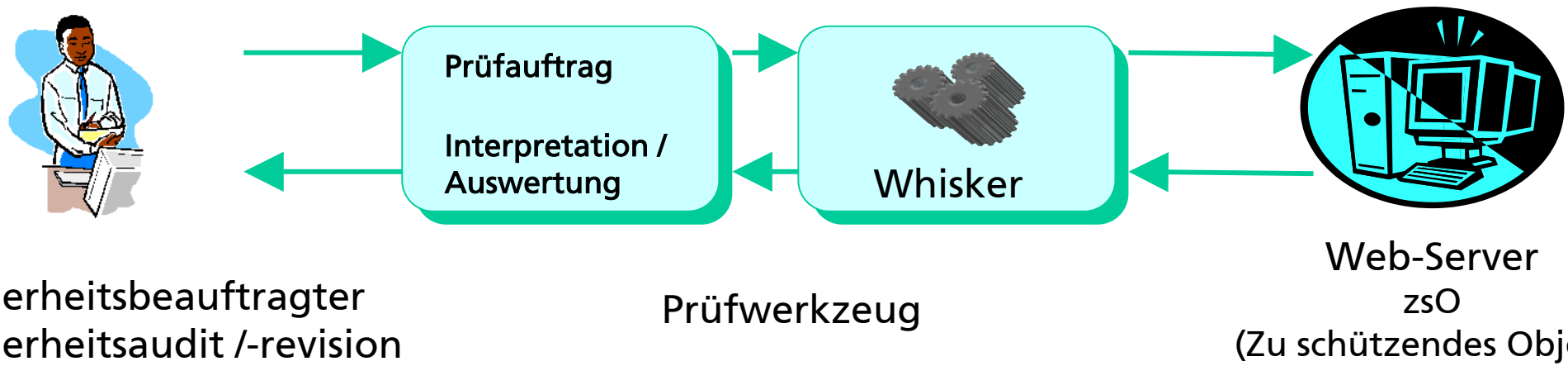
Web-Server
zsO
(Zu schützendes Objekt)

Fraunhofer Institut
Sichere Telekooperation

Vorgehensmodell zur automatisierten Überprüfung

Schritt 2

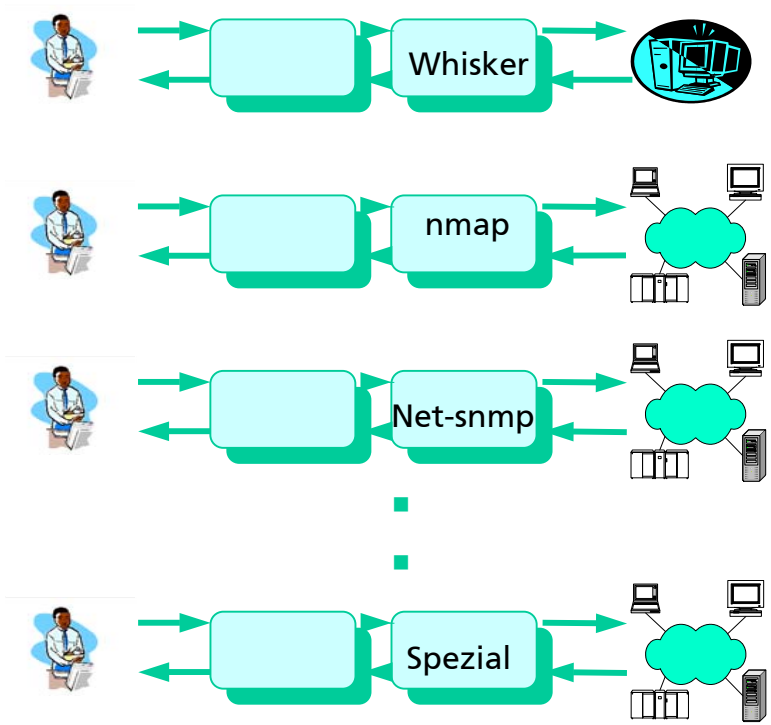
- Prüfauftrag automatisieren (welche Maßnahme, welches Objekt, wann...)
- Automatisierte Interpretation und Auswertung der Ergebnisse



Vorgehensmodell zur automatisierten Überprüfung

Schritt 3

- Viele Werkzeuge für unterschiedlichste Prüfzwecke / Maßnahmen

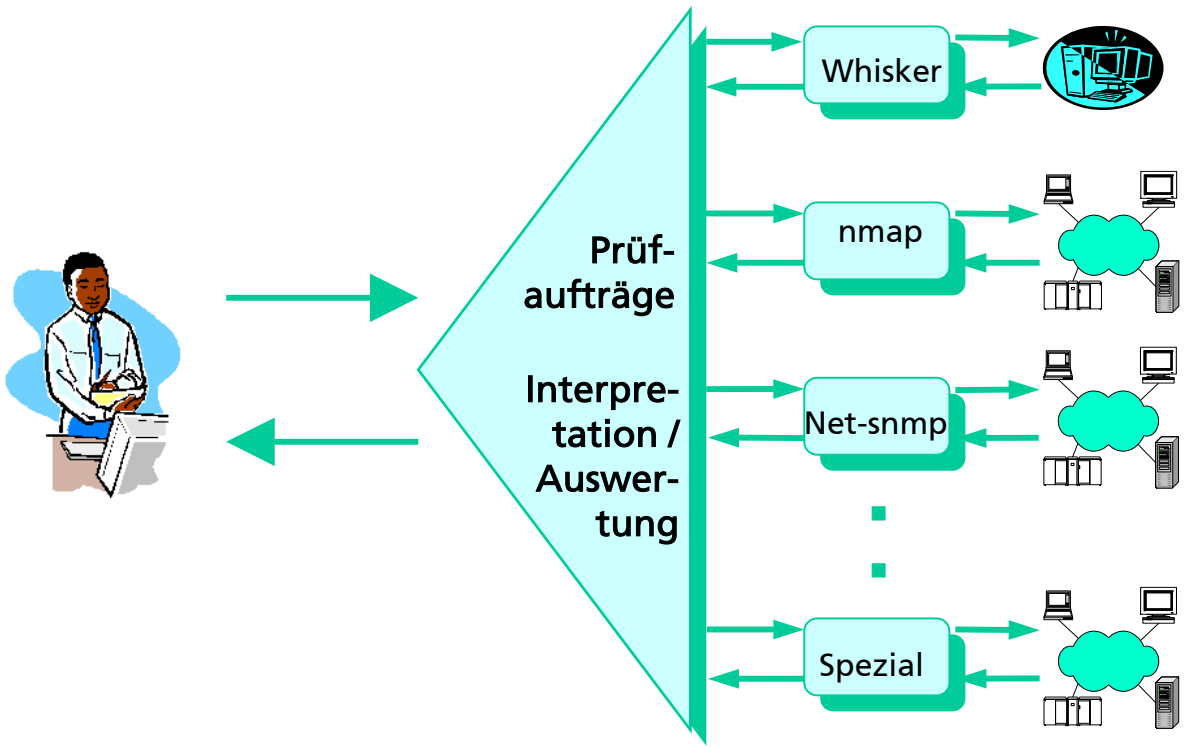


Fraunhofer Institut Sichere Telekooperation

Vorgehensmodell zur automatisierten Überprüfung

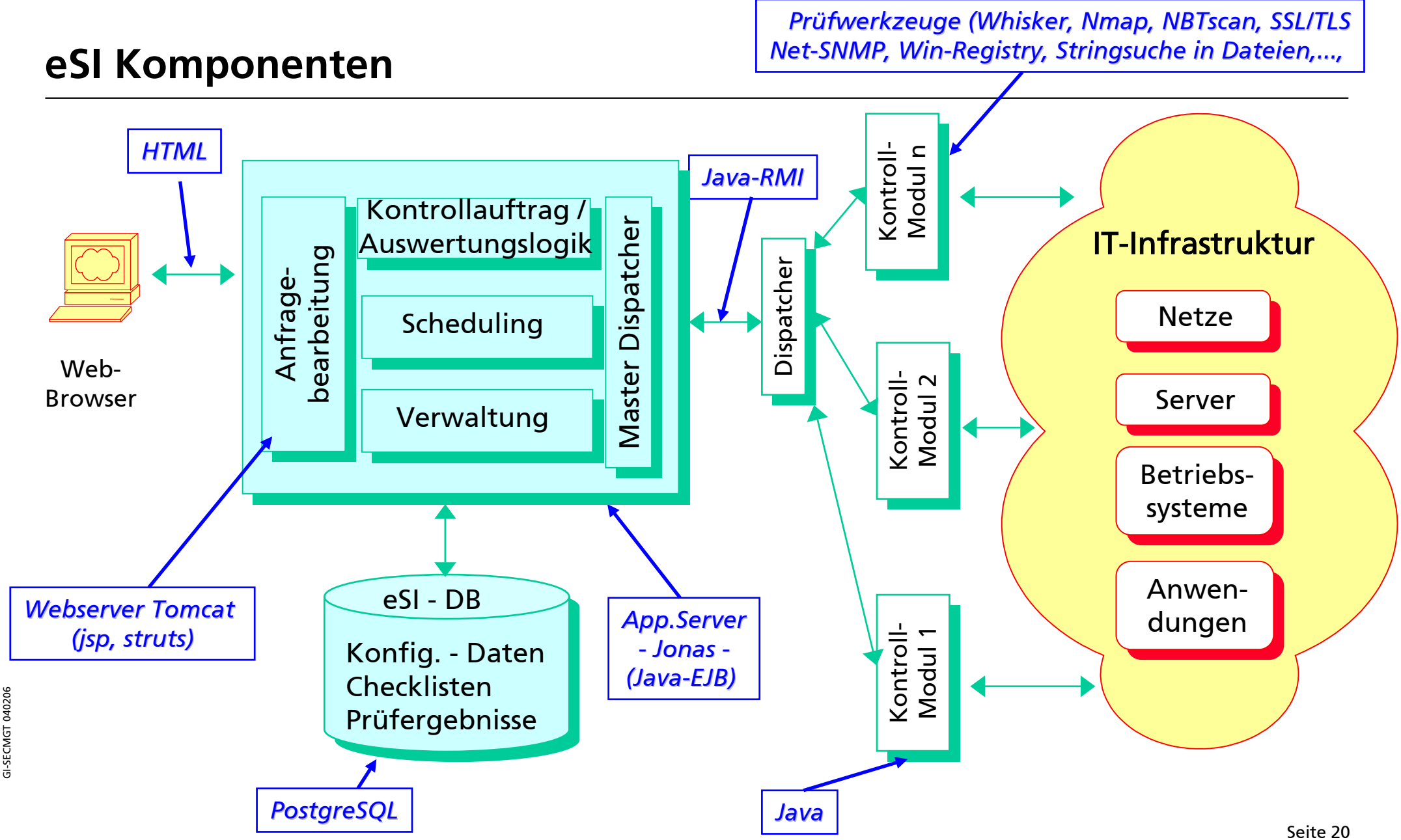
Schritt 4

- Ein Zugangspunkt und einheitliche Bedienung für alle Prüfwerkzeuge



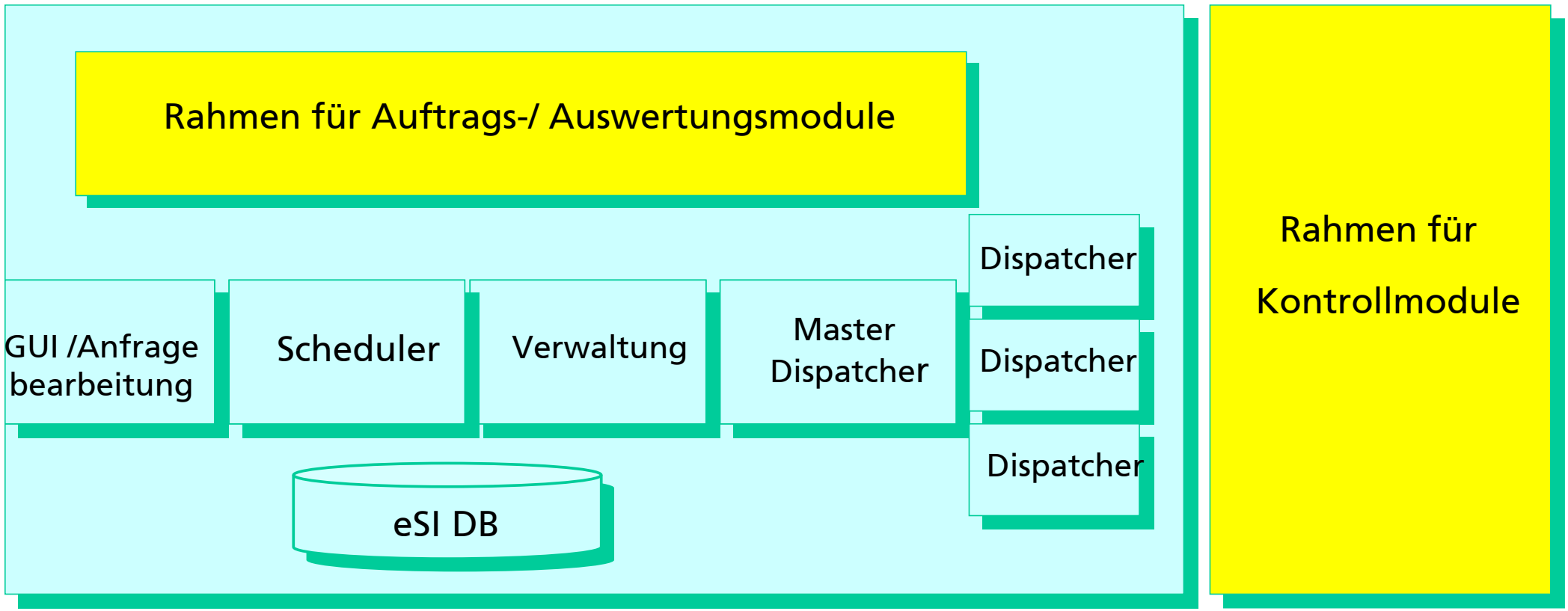
SIT
Fraunhofer Institut
Sichere Telekooperation

eSI Komponenten



eSI Komponenten (2)

eSI Basis-
und Erweiterungskomponenten

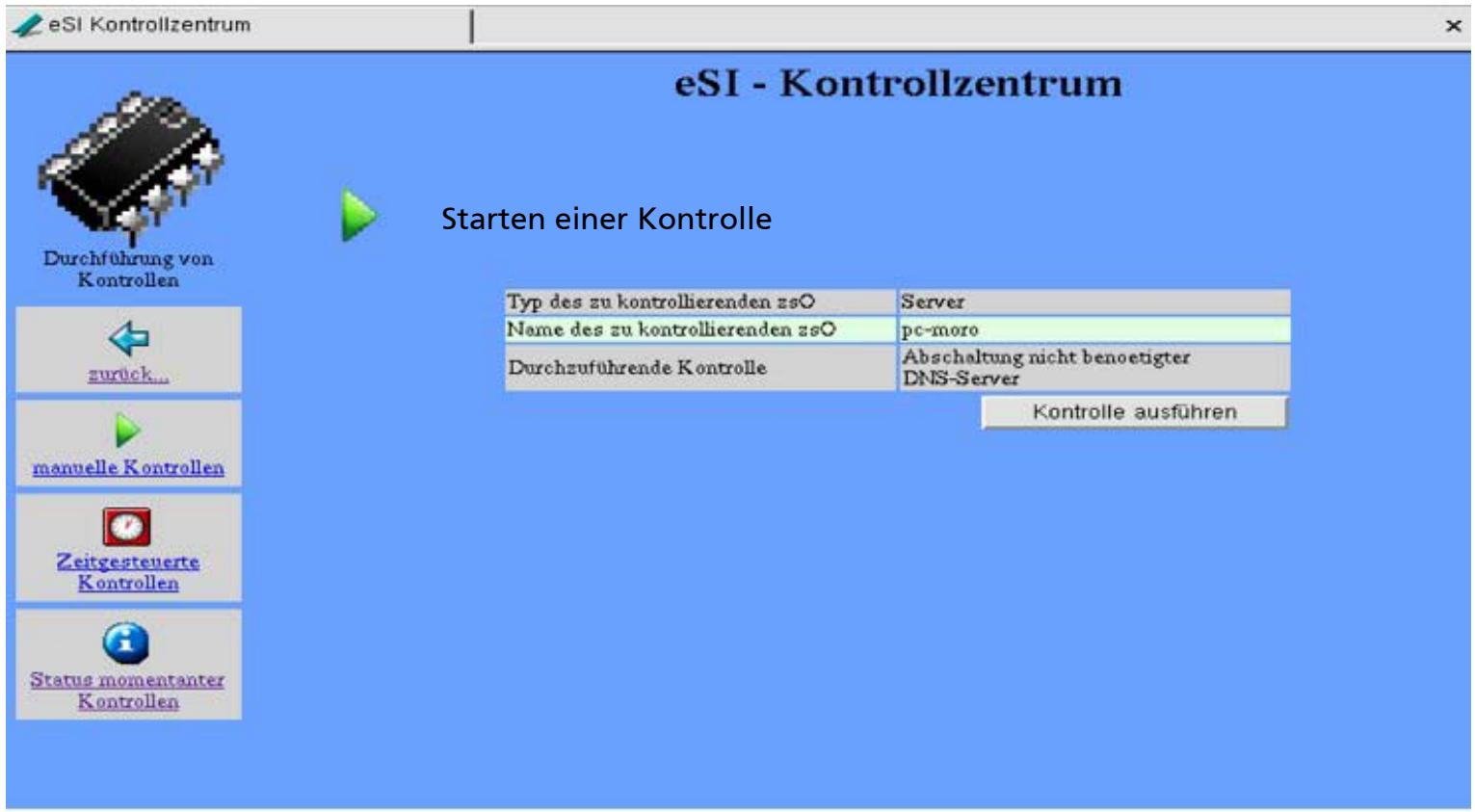


Fraunhofer Institut Sichere Telekooperation

eSI Maßnahmenüberprüfungen

Ablauf einer Überprüfung

1. Auswahl von Maßnahme und Objekt am GUI

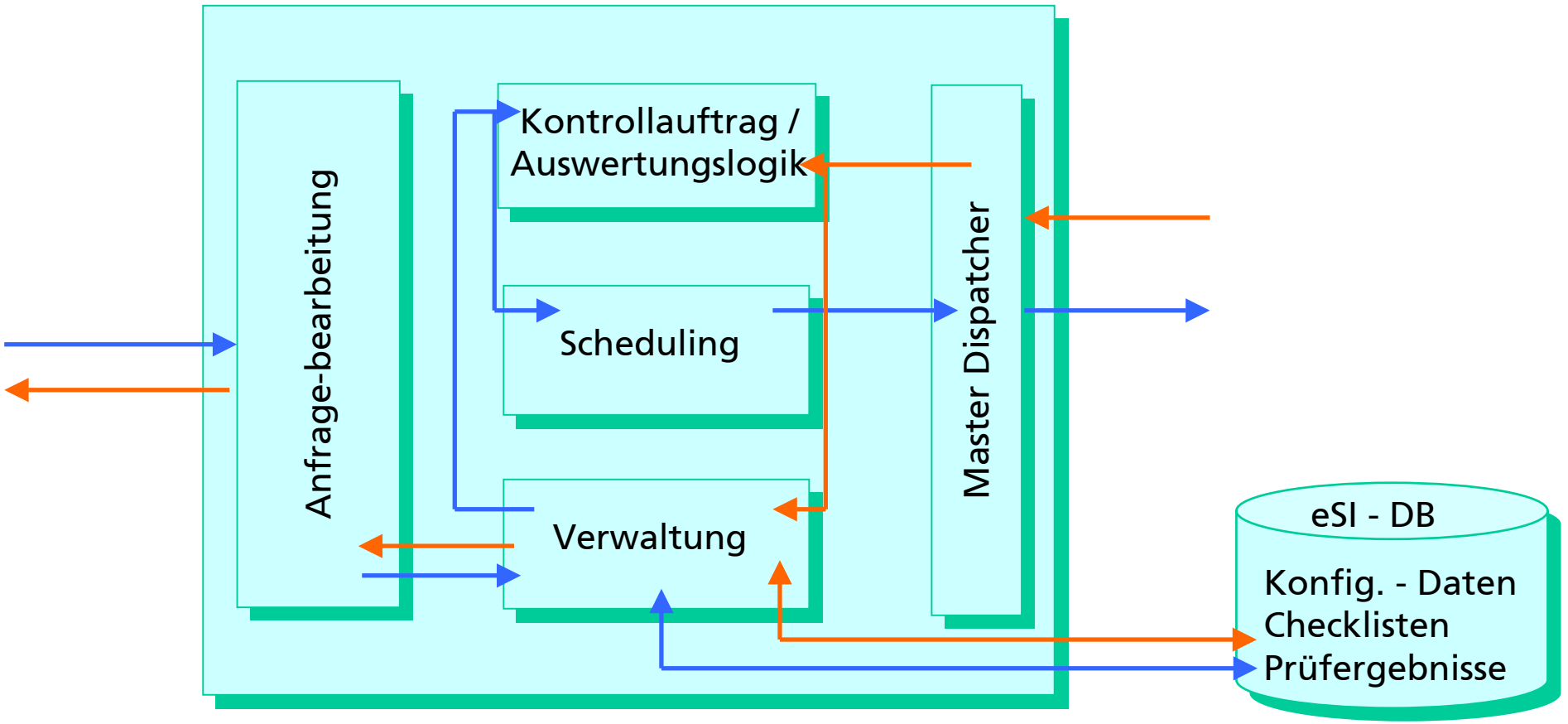


Fraunhofer Institut Sichere Telekooperation

eSI Maßnahmenüberprüfungen

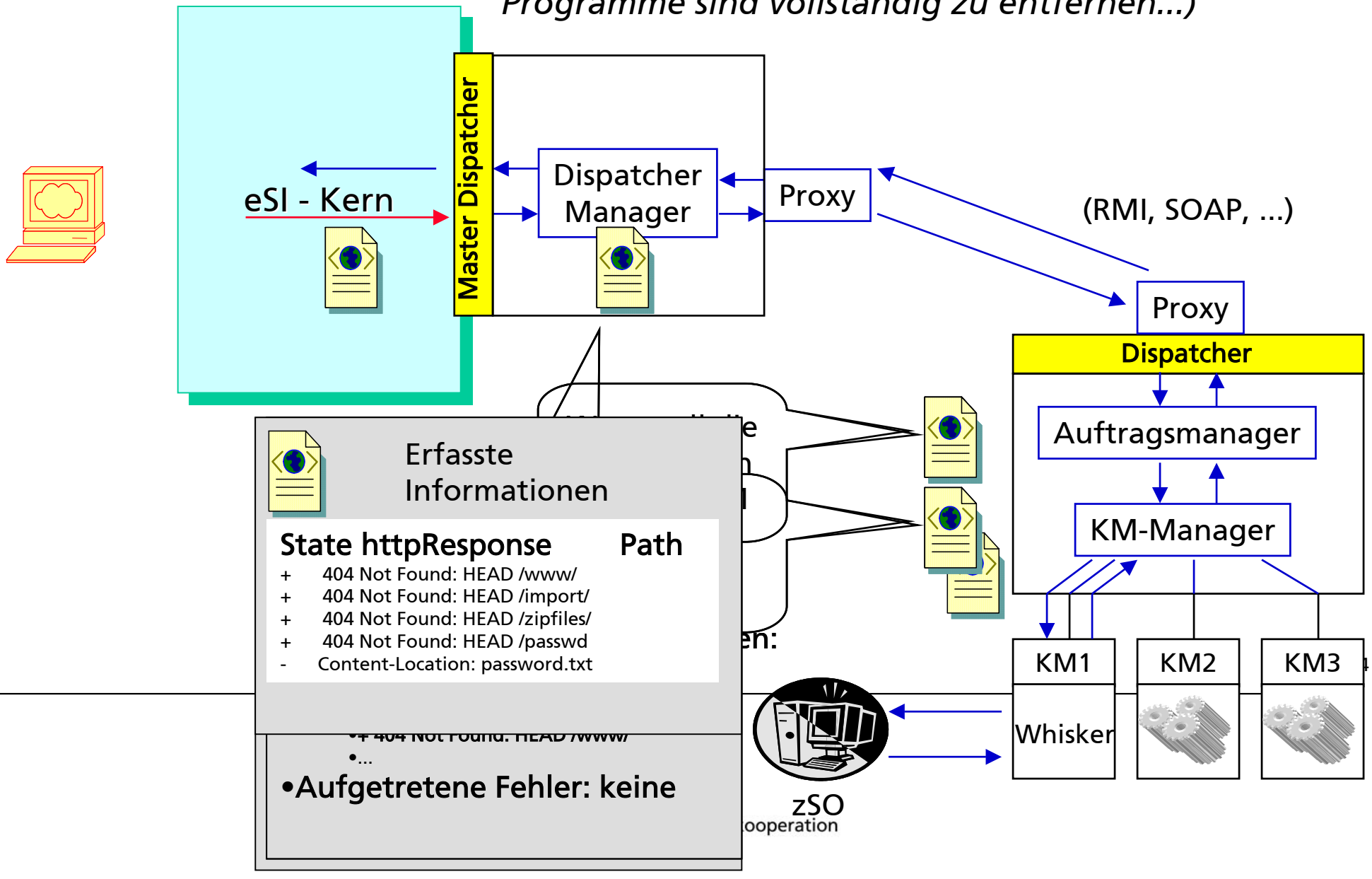
Ablauf einer Überprüfung

2. Ablauf innerhalb des eSI-Kerns



eSI Maßnahmenüberprüfungen

3. Ablauf Kontrollauftrag *(M 2.174 ... die vom Hersteller mitgelieferten CGI-Programme sind vollständig zu entfernen...)*



eSI Maßnahmenüberprüfungen

Einige Maßnahmen-Beispiele

„Abschalten von DNS“	GSHB M4.96 V07/99
„Ein Dienst pro Server“	GSHB M4.97 V07/99
„Standardscripte“ <=> MnNr.5	SANS G7 V2.504
„Port 111 (RPC) blockieren“	SANS U1 V3.21
„Problematische Parameter bei Samba“	GSHB M5.82 V10/00
„regelm. Aktualisierung d. Virensuchprogr.“	GSHB M4.3 V07/99
„transienter Betrieb des Virensuchprogramms“	GSHB M4.3 V07/99
„residenter Betrieb des Virensuchprogramms“	GSHB M4.3 V07/99
„Virenscannerkonfiguration nach Vorgabe“	Spezial-SKE M0.006
„»Verzeichnisinhalt auflisten« deaktivieren“	GSHB M2.174 V10/03
„Symbolische Links deaktivieren“	GSHB M2.174 V10/03
„IP-Forwarding deaktivieren“	GSHB M4.95 V07/99

SIT
Fraunhofer Institut
Sichere Telekooperation