Deutsche Bank
Information & Technology Risk Governance

Shared Assessments
Ein unternehmensübergreifender Ansatz zur Risikobewertung von Vendoren

November 2011

Leistung aus Leidenschaft

SHARED ASSESSMENTS

IT-Sicherheitsprüfungen für ein globales Unternehmen

Globale Präsenz der Deutsche Bank

70 Länder / 996 Auslandsniederlassungen

IT-Services sind in New York, London, Singapur und Frankfurt konzentriert

Support durch Partner in Near- und Offshore-Lokationen

Information & Technology Risk Governance

- erstellt mehr als 200 IT-Sicherheitsassessments für Outsourcings pro Jahr
- führt mehr als 20 Onsite-Reviews für strategische IT-Dienstleister pro Jahr durch
- stellt IT-Sicherheitsinformationen für Kunden der Bank bereit

Regulatorische Anforderungen als Treiber

BaFin

MaRisk Rundschreiben 11/2010
AT 9 Outsourcing

Bundesdatenschutzgesetz

FSA

FSA Handbook
SYSC 8 Outsourcing

Data Protection Act 1998

SR 00-17 (SPE): Guidance on the Risk Management of Outsourced Technology Services

Gramm-Leach-Bliley Act

MAS Monetary Authority of Singapore

Internet Banking and Technology Risk Management
8 Outsourcing Management
Guidelines for Outsourcing
Technology Questionnaire for Outsourcing

Cloud Computing

Erfahrungen aus der Praxis von IT-Sicherheits-prüfungen

Kundenspezifische Fragebogen • Kontrollen kundenspezifisch • Struktur nicht standardisiert	• Beantwortung aufwendig • Hohe Wahrscheinlichkeit zusätzlicher Aufwände für Dienstleister
SAS 70/SSAE 16 Type II • Dienstleister-spezifische Kontrollen • Struktur nicht standardisiert	• Aufwendige Prüfung • Hohe Wahrscheinlichkeit der Unvollständigkeit • Vereinzelt inadäquate Kontrollen
ISO 27001 Zertifizierung • Standardisierte Kontrollen • Dienstleister schränkt mit SOA Kontrollen ein	• Spezielle Aspekte der Kunde-Dienstleister-Beziehung nicht adressiert • Moderater Prüfungsaufwand

Bedarf nach Balance zwischen Kundenaufwand, Kundenanforderungen und Aufwand des Dienstleisters

Shared Assessments

Industriestandard-Organisation

- Vertreter von Kunden- und Dienstleistungsunternehmen
- Branchenübergreifend
- Steuerung durch Anwender
- Erfahrungsaustausch

Ziel

Erhöhung der Effizienz des Vendor-Risiko-Assessment-Prozesses auf Kunden- und Anbieterseite durch Standardisierung ohne Abstriche bei der Qualität der Prüfungen

Entwicklung

2005: Gründung durch BITS Financial Services Roundtable

2006: Version 1 der „Program Tools“

2009: Öffnung für weitere Branchen

2011: Meistbenutztes Standard-werkzeug für Vendor Assessments

Leistungen

- Standard Information Gathering Fragenkatalog
- Agreed Upon Procedures - Prüfungsverfahren
- Whitepapers
- Jährliche Konferenz
- Monatliches Mitgliederforum
- Organisation durch Sante Fe Group

Shared Assessments Programmteilnehmer

	Kunden	Dienstleister	Prüfungsunternehmen
Steering Committee	Goldman Sachs JPMorgan Chase The Bank of New York Mellon Deutsche Bank Target CVS Caremark AIG	Acxiom DriveSavers Data Recovery Early Warning Services Iron Mountain	
	Johnson & Johnson Bank of America Morgan Stanley US Bank Wilmington Trust DTCC	AT&T IBM TSYS First Data Recall Sungard Javitch, Block & Rathbone Yodlee EISI liveops RiskMetrics Group SEI Radian Deluxe Corp. EZ Shield Identity Protection ID Experts	BSI Group Deloitte KPMG PwC Ernst & Young Protivity ControlCase Evantix Churchill & Harriman Fishnet Security

Shared Assessments werden auch von Nichtmitgliedern genutzt

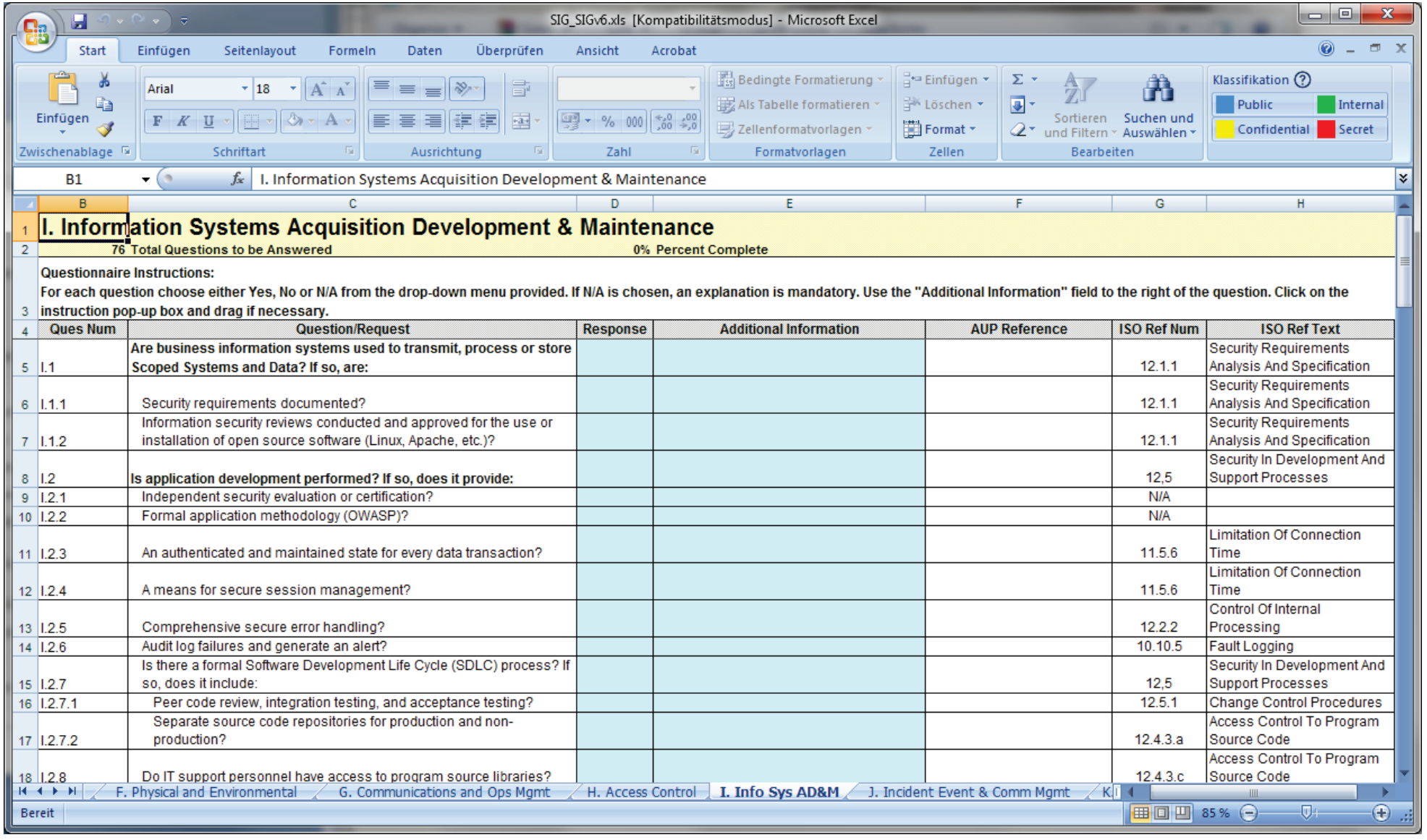
Standard Information Gathering - Fragenkatalog

Fragenkatalog

- Excel-basiertes Werkzeug
- sofort einsetzbar / pilotierbar
- SIG Lite für Basisprüfungen nutzbar
- Sektionsfragen reduzieren Beantwortungsaufwand
- ISO 27002 Kontrollreferenzen
- Feld für zusätzliche Informationen verfügbar
- Management-Werkzeug für Risikowichtung und Transformation alter Versionen verfügbar
- Lizenziert an GRC-Softwareprovider
- Version 6 aktuell

	Abschnitte	Fragen
	Business Information	
	SIG Lite	68
	Complete SIG	691
A	Risk Assessment and Treatment	14
B	Security Policy	48
C	Organizational Security	56
D	Asset Management	35
E	Human Resource Security	37
F	Physical and Environmental Security	129
G	Communications and Operations Management	72
H	Access Control	57
I	Information Systems Acquisition Development & Maintenance	76
J	Incident Event and Communications Management	32
K	Business Continuity and Disaster Recovery	58
L	Compliance	12
M	Additional Questions	
P	Privacy	65

Screenshot



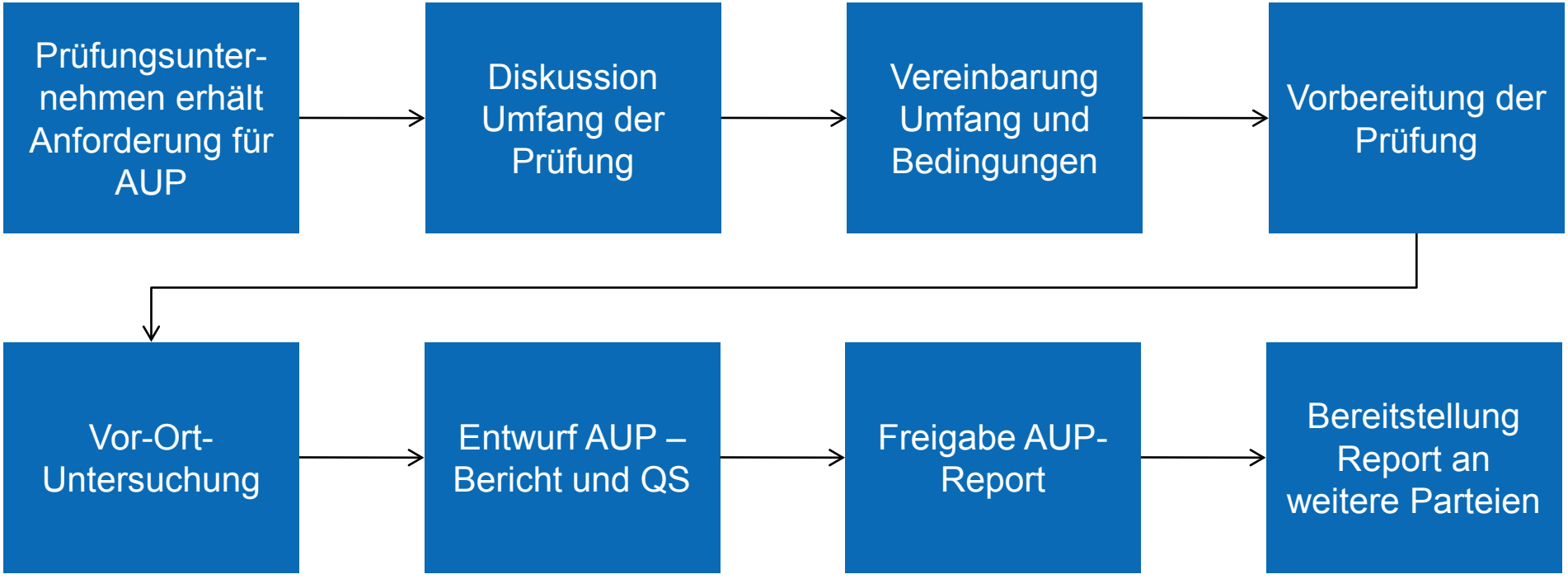
I. Information Systems Acquisition Development & Maintenance

76 Total Questions to be Answered — 0% Percent Complete

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text
I.1	**Are business information systems used to transmit, process or store Scoped Systems and Data? If so, are:**				12.1.1	Security Requirements Analysis And Specification
I.1.1	Security requirements documented?				12.1.1	Security Requirements Analysis And Specification
I.1.2	Information security reviews conducted and approved for the use or installation of open source software (Linux, Apache, etc.)?				12.1.1	Security Requirements Analysis And Specification
I.2	**Is application development performed? If so, does it provide:**				12,5	Security In Development And Support Processes
I.2.1	Independent security evaluation or certification?				N/A	
I.2.2	Formal application methodology (OWASP)?				N/A	
I.2.3	An authenticated and maintained state for every data transaction?				11.5.6	Limitation Of Connection Time
I.2.4	A means for secure session management?				11.5.6	Limitation Of Connection Time
I.2.5	Comprehensive secure error handling?				12.2.2	Control Of Internal Processing
I.2.6	Audit log failures and generate an alert?				10.10.5	Fault Logging
I.2.7	Is there a formal Software Development Life Cycle (SDLC) process? If so, does it include:				12,5	Security In Development And Support Processes
I.2.7.1	Peer code review, integration testing, and acceptance testing?				12.5.1	Change Control Procedures
I.2.7.2	Separate source code repositories for production and non-production?				12.4.3.a	Access Control To Program Source Code
I.2.8	Do IT support personnel have access to program source libraries?				12.4.3.c	Access Control To Program Source Code

Agreed Upon Procedures



Das AUP-Dokument beschreiben die Prozeduren für ein Vor-Ort-Prüfung eines Shared Assessments.

Vorteile des Shared Assessments Programm

Spezialisiertes Werkzeug für Risikoprüfungen von Dienstleistern

Entwickelt von Kunden und Dienstleistern

Praxiserprobt

Hohe Effizienz

Dienstleister: Einmalige Erfassung der Antworten

Kundenunternehmen: Automatisierung der Auswertung möglich

Support durch GRC-Werkzeuge

Schnelle Anpassung an aktuelle Entwicklungen

SIG Version 7 wird die Prüfung von Cloud-Computing-Dienstleistungen unterstützen

Shared Assessments Programm

Erfahrungsaustausch, Trainings, Mitgliederforum, Shared Assessments Konferenz