Sicher in der Cloud – Best Practice Sicherheitskonzept

Monika Kuberek | Universitätsbibliothek der TU Berlin

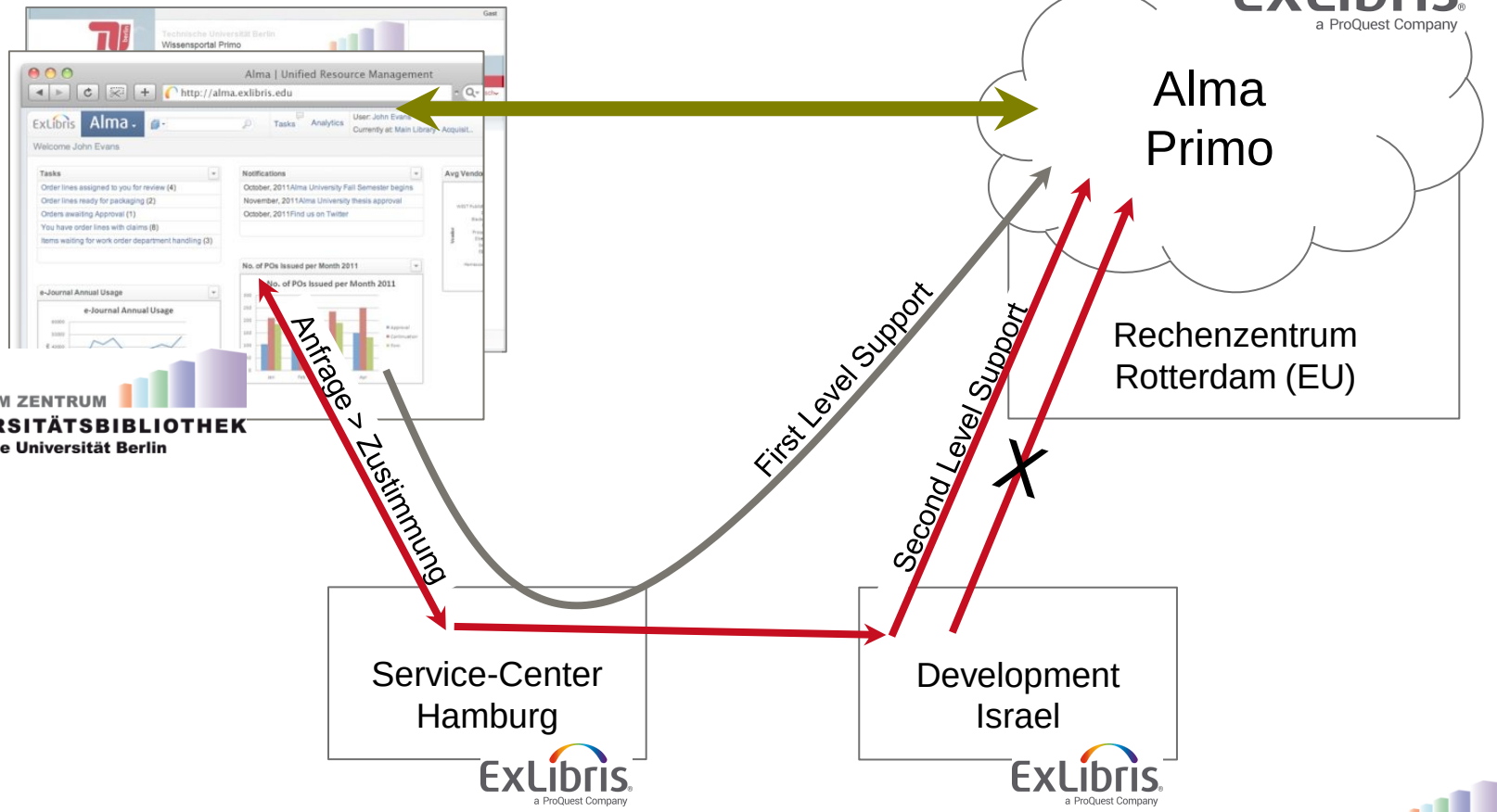
106. Bibliothekartag „Medien – Menschen – Märkte“ | 30.05. – 02.06.2017 in Frankfurt am Main

Alma und Primo in der Cloud

- Berliner Universitätsbibliotheken 2016
  - Umstieg von Aleph auf Alma
  - Wechsel von KOBV-Primo in die Cloud
- Ex Libris Private Cloud
- Servicemodell – Software as a Service (Saas)
  - Auslagerung sämtlicher Alma-/Primo-Komponenten
  - Zugriff der Bibliothek über das Internet
- Vertrag mit Ex Libris 2015
  - Einbindung der Behördlichen Datenschutzbeauftragten
  - Basis-Festlegungen für Cloud-Betrieb
  - Sicherheitskonzept im Vertrag festgeschrieben

➢ Begutachtung und Zustimmung zum Sicherheitskonzept durch Behördliche Datenschutzbeauftragte der Universitäten und Landesdatenschutzbeauftragte

Cloud-Betrieb – Grundkonstellationen



WISSEN IM ZENTRUM
UNIVERSITÄTSBIBLIOTHEK
Technische Universität Berlin

WISSEN IM ZENTRUM
UNIVERSITÄTSBIBLIOTHEK
Technische Universität Berlin

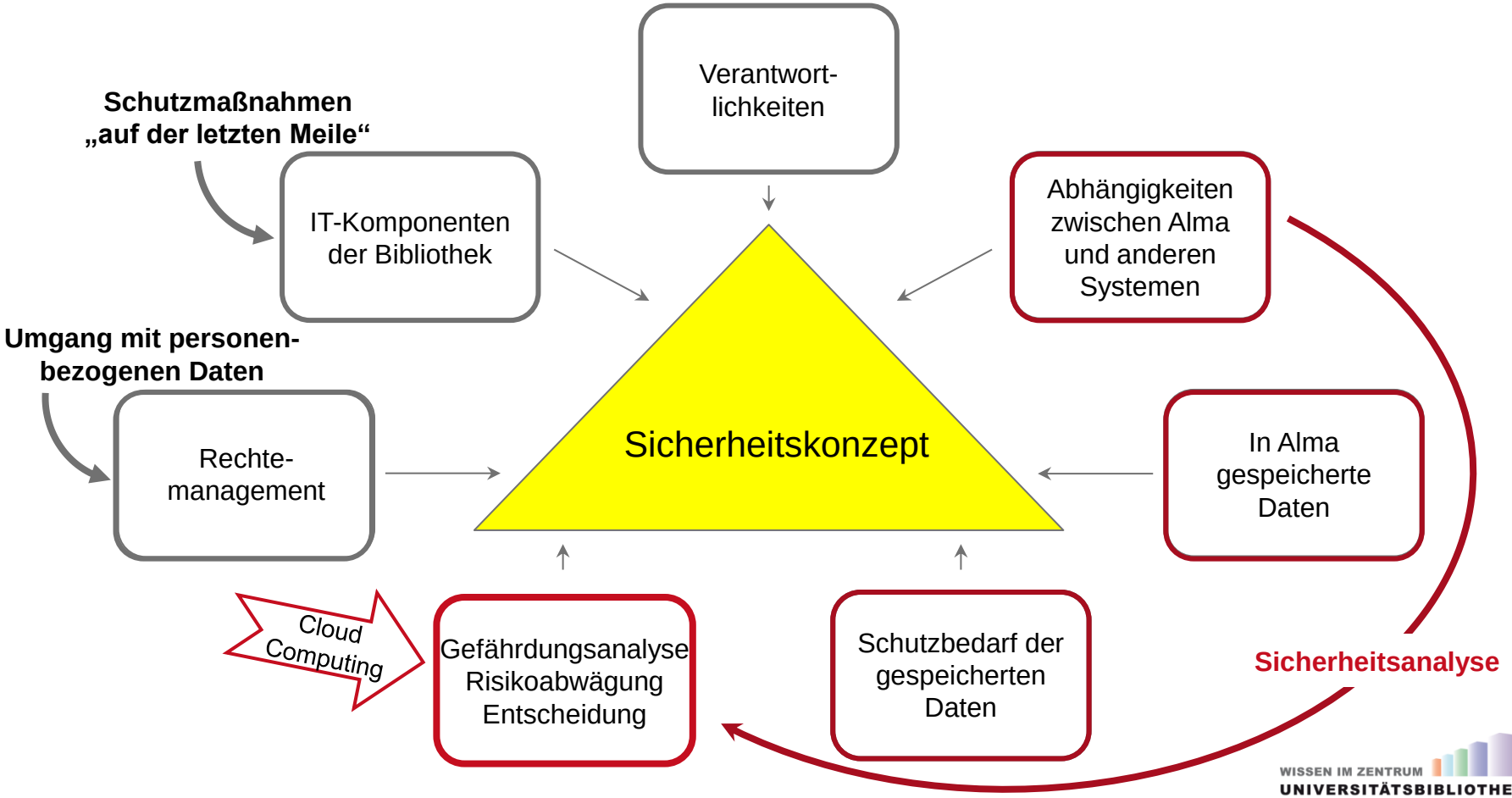
Sicherheitskonzept Alma | Sicherheitskonzept Primo

- Informationssicherheit > Datenschutz, Datensicherheit, …
- Ziele (gemäß § 5 Abs. 2 BlnDGS)
  - Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit, Transparenz
- Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zum Cloud Computing
  - „Dossier Anwender Management“

    https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Zielgruppen/Anwender/AnwenderManagement/AnwenderManagement.html?cms_pos=1
  - Eckpunktepapier: „Sicherheitsempfehlungen für Cloud-Computing-Anbieter – Mindestanforderungen für die Informationssicherheit“

    https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile&v=6

Sicherheitskonzept – einzelne Komponenten



Verantwortlichkeiten

- Gesamtverantwortung
  - Datenverarbeitende Stelle ist die Bibliothek. Die Gesamtverantwortung für das universitäre Bibliothekssystem trägt die Direktorin bzw. der Direktor der Bibliothek.
- Verantwortung für den IT-Betrieb der Bibliothek
  - Gesamtverantwortung für den Betrieb von Alma
  - Systembibliothekarische Administration von Alma
  - Administration der Mitarbeiter-Endgeräte
  - Administration der Benutzer-Endgeräte
- Verantwortung für Identitätsmanagement und Active Directory

➢ Feststellung der Verantwortlichkeiten für alle Betriebsbereiche der Bibliothek, die mit Alma in Zusammenhang stehen

Rechtemanagement

- Arten von BenutzerInnen in Alma
  - Alma-Definition: interne / externe BenutzerInnen
  - Unterscheidung Staff User / Patron
- Authentifizierung / Autorisierung
- Rollen- und Rechtekonzept
- Verwaltung der internen / externen BenutzerInnen
- Anonymisierung / Löschung von BenutzerInnen und Benutzerdaten

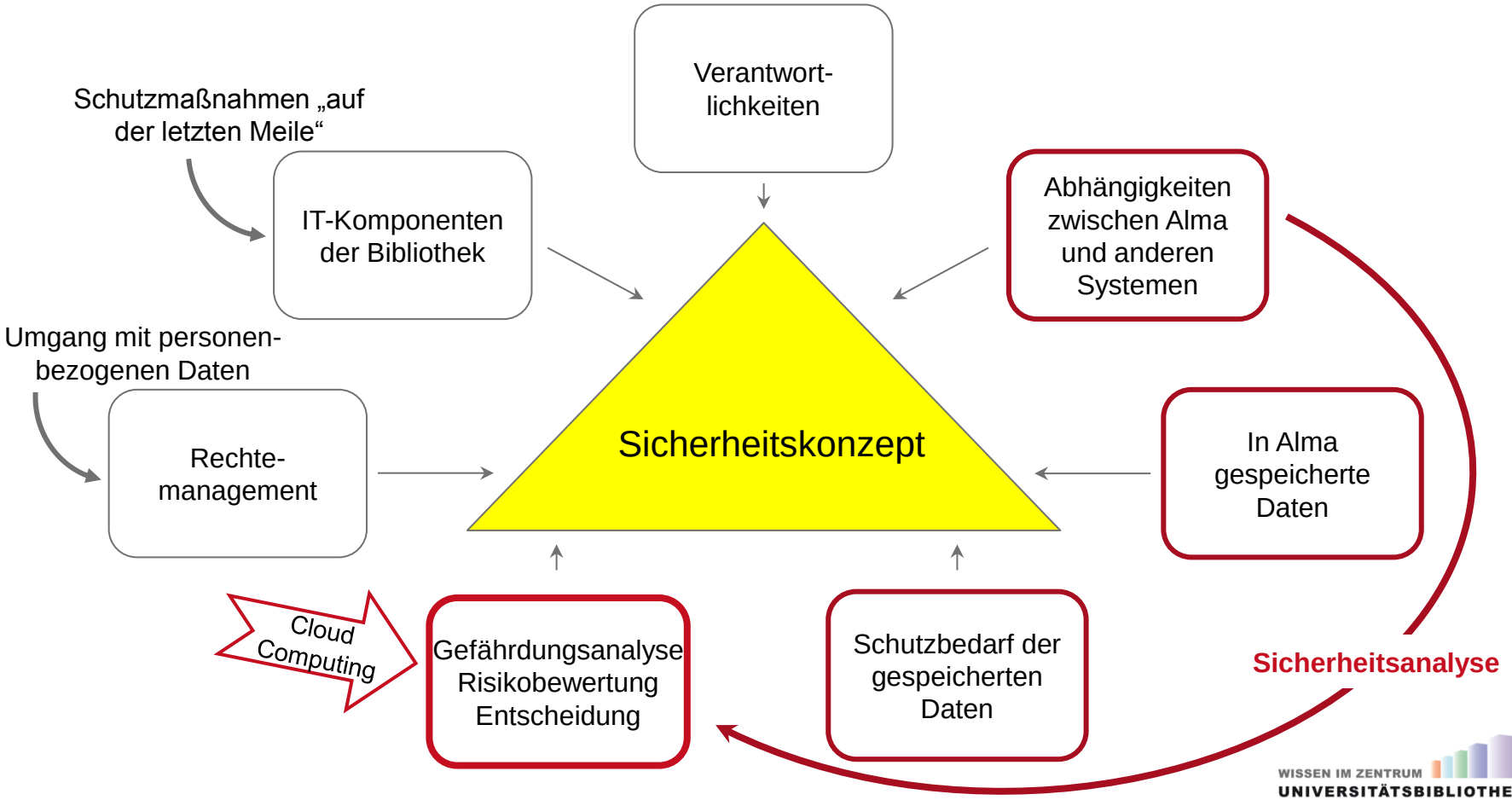
➢ Umgang mit personenbezogenen Daten in der Bibliothek

IT-Komponenten der Bibliothek

- Verbindung zum Dienstleister
- Beschreibung der Einzelkomponenten und Schutzmaßnahmen
  - PCs / Terminals der MitarbeiterInnen und Peripheriegeräte
  - Thekenarbeitsplätze
  - Benutzerterminals
  - Verbuchungsautomaten
  - Rechnernetz für MitarbeiterInnen und Benutzungsbereich
  - Identitätsmanagement und Active Directory
- Organisatorische Maßnahmen
  - z.B. Paßwortrichtlinien des Rechenzentrums

➢ Schutzmaßnahmen „auf der letzten Meile“

Sicherheitskonzept – einzelne Komponenten



Abhängigkeiten zwischen Alma und anderen Systemen

- Aus welchen Systemen erhält Alma Daten?
  - Primo, Verbuchungsautomaten, Fernleihsystem, B3Kat …
- An welche Systeme liefert Alma Daten?
  - Primo, Fernleihsystem, Mailrelay, IT-Umgebung Einzelarbeitsplätze …
- Was passiert, wenn Alma bzw. das andere System nicht zur Verfügung steht?
  - z.B.: Fallen die Verbuchungsautomaten aus, kann die Ausleihe/Rückgabe nur an den Theken erfolgen.
  - bzw.: Steht Alma nicht zur Verfügung, kann die Bibliothek weder aktive noch passive Fernleihbestellungen durchführen.

➢ Feststellung der generellen Abhängigkeiten und ihrer Relevanz für die Nutzerservices und den Betrieb der Bibliothek

In Alma gespeicherte Daten

- Unterscheidung der Datenarten
  - ➢ Bibliographische Daten, Etatdaten, Lieferantendaten, Erwerbungsdaten, Benutzerdaten, Ausleihdaten, Gebührendaten, Kommunikationsdaten
- Unterscheidung
  a) durch die Bibliothek erhoben
  b) maschinelle Übertragung: aus anderen Systemen eingespielt, aus Alma exportiert
- Beschreibung der Daten
  a) Art der Daten, Inhalte, Erforderlichkeit, Datenaustausch, Speicherdauer, Löschung/ Anonymisierung, Zugriffsrechte
  b) Art der Daten, Quell-/Zielsystem, Inhalte, Erforderlichkeit, Speicherdauer, Datenschutz im Quell-/Zielsystem, Verantwortlich

➢ Analyse der Datenarten und der datenschutzrechtlichen Belange

In Alma gespeicherte Daten

– Beispiel

5.1 Durch die UBs erhobene und in Alma gespeicherte Daten

	1. Daten	2. Inhalte	3. Erforderlichkeit	4. Daten-austausch/ mit wem	5. Speicherdauer	6. Anonymisierung/ Löschung	7. Zugriffsrechte
5	Benutzer-daten (Internal User)	Institution Benutzer-ID, E-Mail-Adresse	Für die Abwicklung der Benutzerdienste, für Mahnungen und Rückforderungen notwendig.	Primo der UB der TUB	Mind. 12 bis max. 24 Monate nach der letzten Kontoaktivität oder auf Verlangen des/der Benutzer_in, sofern das Konto ausgeglichen ist	Anonymisierung in Alma nach der in Spalte 5 angegebenen Frist bzw. nach Ausgleich des Benutzerkontos Löschung der in Alma deaktivierten Benutzerkonten im Active Directory der UB der TUB einmal pro Monat	alle für die Benutzung autorisierten Mitarbeiter_innen der UB

Schutzbedarf der gespeicherten Daten

- Hinsichtlich: Vertraulichkeit, Verfügbarkeit, Integrität
- Auswirkungen des Verlusts von Vertraulichkeit / Verfügbarkeit / Integrität
  - Beeinträchtigung des informationellen Selbstbestimmungsrechts
  - Verstoß gegen Gesetze, Vorschriften, Verträge
  - Beeinträchtigung der Aufgabenerfüllung
  - Negative Außenwirkung der Einrichtung
  - Finanzielle Auswirkungen
- Einordnung in Schutzbedarfsstufen
  - niedrig, mittel, hoch
- Feststellung des Schutzbedarfs für die verschiedenen Datenarten
  - Bibliographische Daten, Etatdaten, …

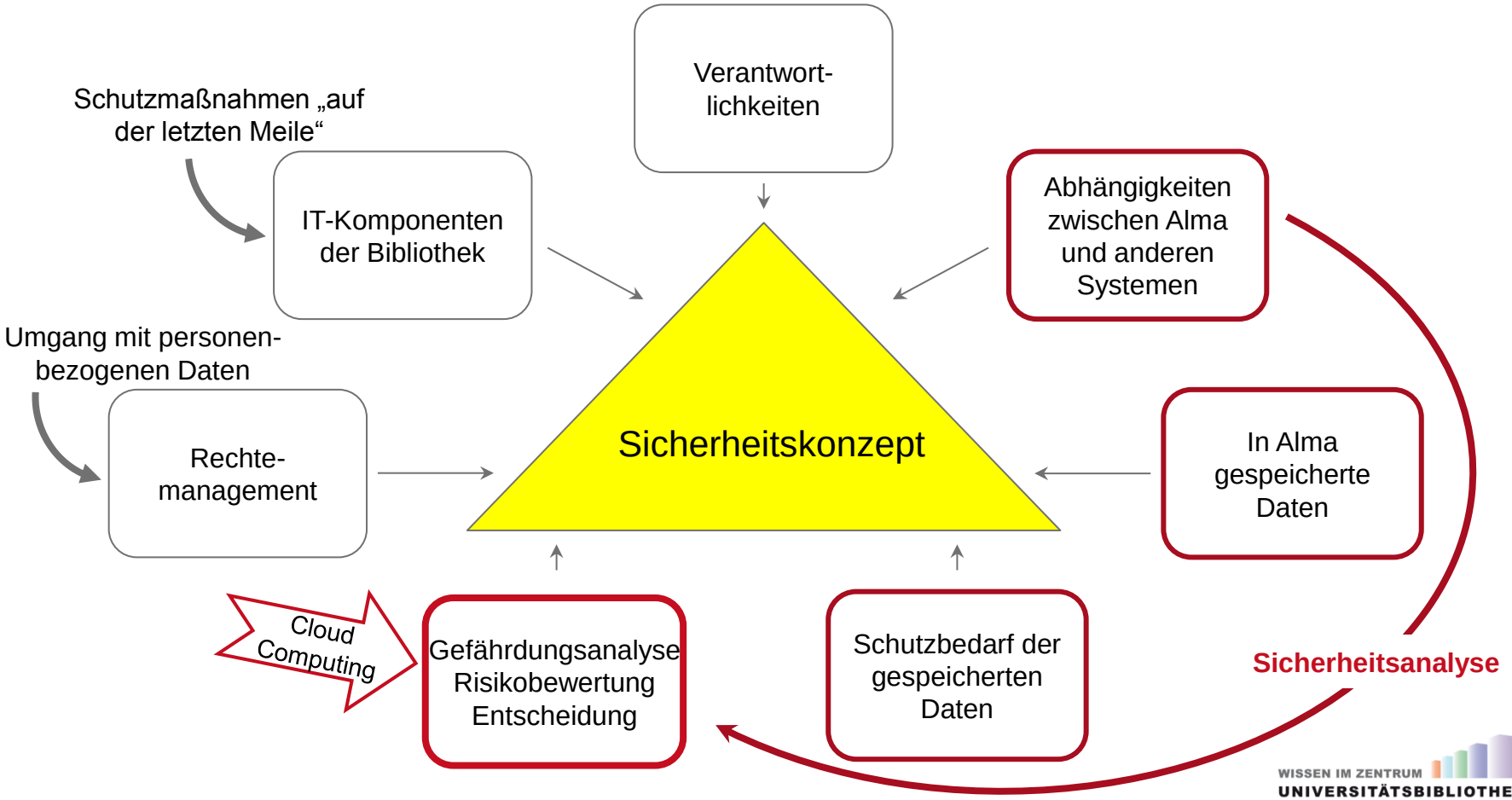
➢ Schutzbedarf für alle Daten ist hoch

Schutzbedarf der gespeicherten Daten

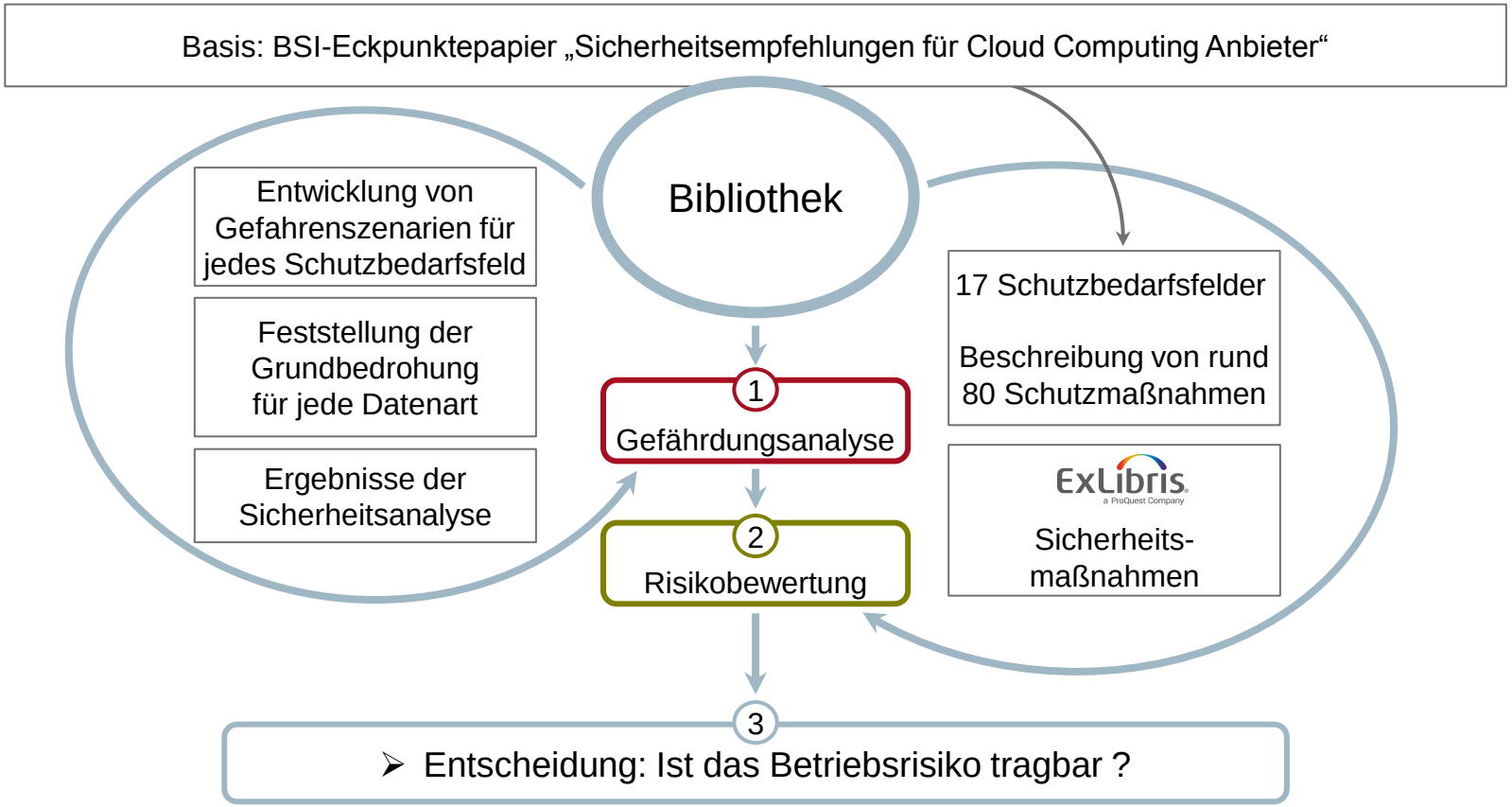
– Beispiel

	Daten	Vertraulichkeit	Verfügbarkeit	Integrität	Schutzbedarf (Stufe)
1	Biblio-graphische Daten	Daten sind frei zugänglich (lesend). Schutzbedarf niedrig	Die Daten sollen 7x24 verfügbar sein. Kurzzeitige Ausfälle sind vertretbar. Ausfälle beeinträchtigen das Ansehen der Einrichtung in geringem Maß. Da die Mitarbeiter_innen nicht handeln können, entsteht hoher materieller Schaden. Schutzbedarf hoch	Die Daten müssen korrekt sein, da sie den Nachweis für den Besitz der Bibliothek darstellen. Die Verletzung der Integrität in einzelnen Daten hat geringe Folgen. Der Verlust der Daten insgesamt ist für den Betrieb der Bibliothek katastrophal. Schutzbedarf hoch	hoch

Sicherheitskonzept – einzelne Komponenten



Gefährdungsanalyse – Risikobewertung – Entscheidung

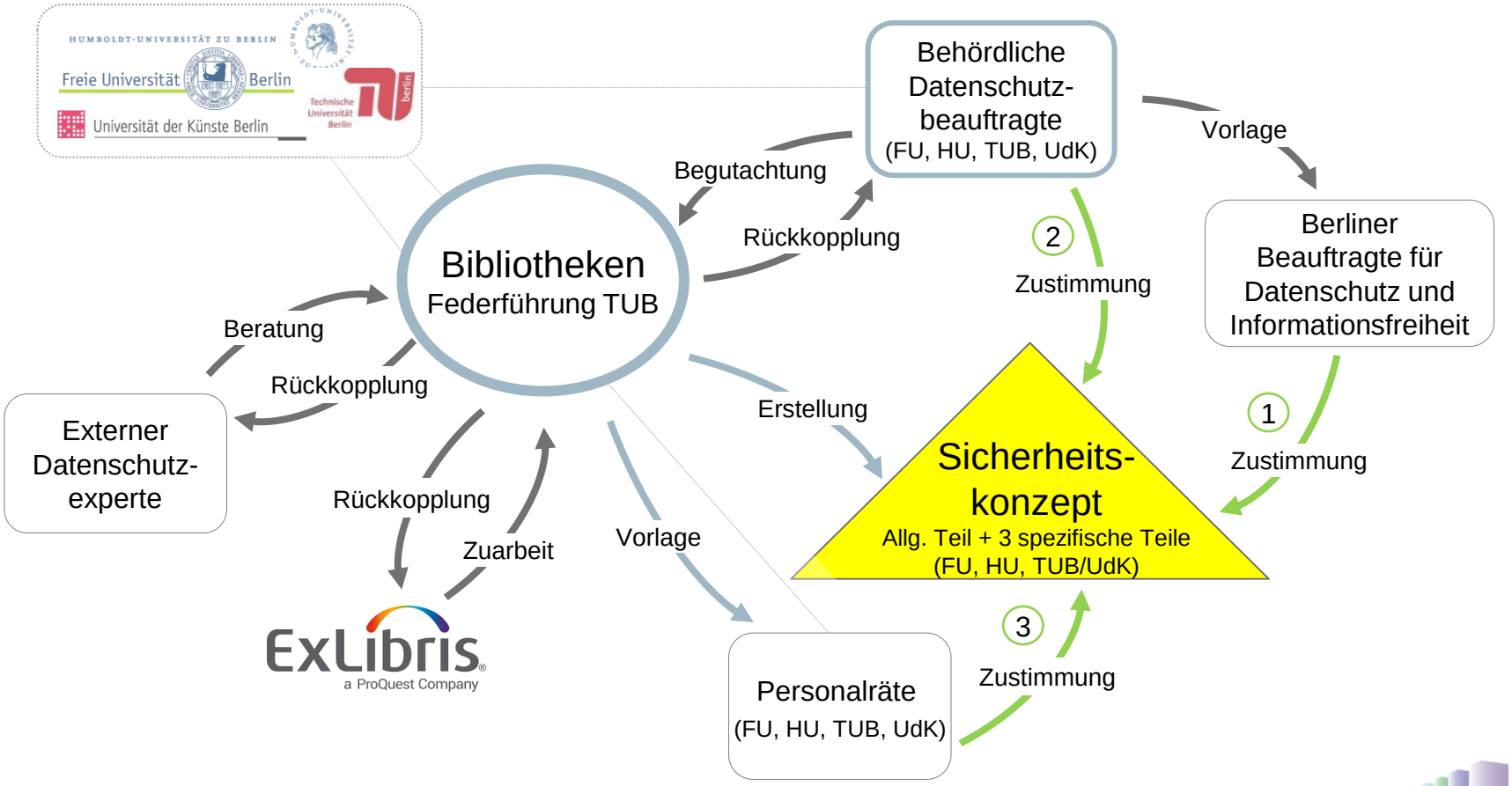


Gefährdungsanalyse – Risikobewertung – Entscheidung

Beispiel

Gefahrenszenarium und korrespondierende Maßnahmen	Grundbedrohung: Vertraulichkeit Verfügbarkeit Integrität	Grundbedrohung: hohe Vertraulichkeit	Grundbedrohung: hohe Verfügbarkeit	Bedrohte Daten	Sicherheitsmaßnahmen im Einzelnen	Risikobewertung unter Einbeziehung der Sicherheitsmaßnahmen
C. Server-Sicherheit Mögliche Gefährdungen ergeben sich z.B. durch: Angriffe wie Rechteüberschreitungen von Nutzern, Login-Fehlversuche oder Schadsoftware (z.B. Trojanische Pferde)						Das verbleibende Risiko erscheint als so gering, dass das Betriebsrisiko hinsichtlich der genannten Gefährdung als tragbar erscheint.
Maßnahmen:						
12 Technische Maßnahmen zum Schutz des Hosts (Host Firewalls, regelmäßige Integritätsüberprüfungen, Host-based Intrusion Detection Systems)	x			1-8	Sicherheitsmaßnahmen Ex Libris	
13 Sichere Grund-Konfiguration des Hosts (z.B. Einsatz gehärteter Betriebssysteme, Deaktivierung unnötiger Dienste, etc.)	x			1-8	Sicherheitsmaßnahmen Ex Libris	
14 Einsatz zertifizierter Hypervisoren (Common Criteria mindestens EAL 4)		x		5,6,7,8	Sicherheitsmaßnahmen Ex Libris	
			x	1-8		

Sicherheitskonzept – Beteiligte



Danke für Ihre Aufmerksamkeit!

Monika Kuberek

monika.kuberek@tu-berlin.de