

Leistungsbeschreibung

„IT-Audit mit Schwerpunkt Kosten, IT-Betrieb und Webentwicklung“

16.07.2026

Der Auftraggeber ist ein gemeinnütziger eingetragener Verein mit Sitz an der Humboldt-Universität zu Berlin (nachfolgend „HU“). Er nutzt für den Betrieb seiner IT auf Basis einer Kooperationsvereinbarung anteilig die technische Infrastruktur der Humboldt-Universität zu Berlin, insbesondere Gebäudeverkabelung, Netzkomponenten, Internetzugang sowie zentrale E-Mail- und Kommunikationsdienste.

Das IT-Team des Auftraggebers stellt einerseits die Arbeitsfähigkeit der Mitarbeiter*innen sicher. Hierzu gehören insbesondere Arbeitsplatz-IT, Support, Nutzer*innenverwaltung, Endgeräte, Server (Betrieb durch HU), Fachanwendungen sowie die Betreuung interner Dienste. Zu diesem Aufgabenbereich zählen 3 Mitarbeiter*innen. Andererseits ist ein wesentlicher Teil des IT-Teams mit der Entwicklung von Webanwendungen befasst, die zum Teil über Zuwendungen finanziert werden (9 von 12 Programmierer*innen). Diese Webanwendungen werden unter einer Open-Source-Lizenz veröffentlicht. Die Anwendungen dienen vor allem dem computerbasierten Testen von Schüler*innen und werden von dem Arbeitsbereich VERA und IQB-Bildungstrends vordringlich genutzt. Aufgrund der Veröffentlichung unter einer Open-Source-Lizenz können die Webanwendungen auch von den Ländern genutzt werden.

1 Grundlagen für die Erbringung der Leistungen

- Der Auftraggeber steht mit einem IT-Controlling und der Dokumentation von Prozessen und Verantwortlichkeiten am Anfang. Prüfungen und Analysen werden sich daher vor allem auf Interviews stützen müssen.
- Die Leistung umfasst mindestens eine Dokumentenprüfung, die Auswertung relevanter Kosten-, Vertrags-, Lizenz-, Entwicklungs- und Betriebsunterlagen sowie strukturierte Interviews mit relevanten Ansprechpartnerinnen und Ansprechpartnern des IQB. Die Dokumentenprüfung wird nicht mehr als 50 Dokumente mit einem Umfang von jeweils 10 Seiten umfassen. Abweichungen von bis zu 10% sind möglich.
- Die Leistungen der IT werden für bis zu 200 Beschäftigte des Auftraggebers ausgeführt.
- Prüfungen von IT-Systemen der HU oder gemeinsam genutzter Infrastruktur sind nicht Bestandteil der Leistung.
- Die Prüfung in den Bereichen der Informationssicherheit bilden die Voraussetzung für die anschließende Sicherheitsprüfung anhand eines Sicherheitsstandards nach BSI-Grundschutz-Kompendium bilden. Sie arbeiten insbesondere Sicherheitslücken heraus. Die anschließende Sicherheitsprüfung ist nicht Gegenstand dieser Leistungsbeschreibung.
- Als Ergebnis ist ein schriftlicher Auditbericht zu erstellen. Dieser stellt den Prüfungsumfang, Methodik, Feststellungen, Risiken, Kostenstrukturen, Wirtschaftlichkeitsbewertung und Empfehlungen nachvollziehbar dar. Alle Aspekte, die die Informationssicherheit betreffen, müssen in einem separaten Berichtsteil dargestellt werden.
- Die Empfehlungen sind in priorisierten Maßnahmenlisten entsprechend der beiden Berichtsteile zusammenzufassen. Für jede Maßnahme werden nach Möglichkeit Nutzen, Umsetzungsaufwand, Einspar- oder Effizienzpotenzial, Risiken einer Nichtumsetzung und zeitliche Priorität angegeben.
- Die Ergebnisse sind dem Auftraggeber in einem Abschlussgespräch vorzustellen.

2 Zu erbringende Leistungen

Gegenstand der ausgeschriebenen Leistung ist die Durchführung eines unabhängigen IT-Audits der vom IQB verantworteten IT-Strukturen, IT-Prozesse, Kostenstrukturen, Sicherheitsmaßnahmen sowie der Prozesse der Webentwicklung. Das Audit dient der Qualitätsentwicklung. Ziel des Audits ist es, Transparenz über Leistungsumfang, Ressourceneinsatz, Kosten, Verantwortlichkeiten, Risiken und Optimierungspotenziale der IT des Auftraggebers zu schaffen, zu analysieren und zu bewerten. Der Auftragnehmer hat daher priorisierte Maßnahmenlisten (vgl. Ziffer 1, 7. Spiegelstrich) für die Prüfbereiche zu erarbeiten.

Ein besonderer Schwerpunkt des Audits liegt auf der Kostenanalyse und Wirtschaftlichkeitsbewertung. Dabei müssen die Kosten¹ des IT-Betriebs, der Arbeitsplatzunterstützung und der Systembetreuung erhoben, strukturiert und bewertet werden. Zu untersuchen ist insbesondere, ob und wenn ja, welche Kostentreiber erkennbar sind, ob Doppelstrukturen oder vermeidbare Aufwände vorliegen und welche Einspar-, Konsolidierungs- oder Effizienzpotenziale bestehen.

Ein weiterer Schwerpunkt liegt auf den Prozessen der Webentwicklung. Zu prüfen sind insbesondere Organisation, Rollen, Anforderungsmanagement, Priorisierung, Entwicklungsprozesse, Qualitätssicherung, Testverfahren, Release- und Deploymentprozesse, Dokumentation, Wartbarkeit, Open-Source-Governance, IT-Sicherheit auch im Entwicklungsprozess sowie der Umgang mit Abhängigkeiten und Sicherheitsupdates. Dabei werden auch bewertet, ob die Entwicklungsprozesse den Anforderungen an Zuverlässigkeit, Datenschutz, IT-Sicherheit, Transparenz und langfristige Nutzbarkeit der Anwendungen für computerbasierte Tests durch Externe angemessen Rechnung tragen.

Der Auftragnehmer hat die nachfolgenden Prüfbereiche systematisch zu untersuchen. Für jeden Prüfbereich sind die relevanten Unterlagen auszuwerten, geeignete Interviews mit den zuständigen Personen zu führen, die Feststellungen nachvollziehbar zu dokumentieren, Risiken und Verbesserungspotenziale zu bewerten sowie konkrete Handlungsempfehlungen in Form eines priorisierten Maßnahmenkatalogs abzuleiten.

2.1 Prüfbereich „IT-Organisation, Rollen und Zuständigkeiten“

Der Auftragnehmer hat die Organisation der IT des IQB zu erfassen und zu bewerten. Dazu gehören insbesondere die Aufgabenverteilung innerhalb des IT-Teams, die Zuordnung von Verantwortlichkeiten, Vertretungsregelungen, Entscheidungswegen, Eskalationswegen sowie Schnittstellen zu Fachbereichen, Verwaltung, Institutsleitung und externen Dienstleistern. Der Auftragnehmer hat zu prüfen, ob Rollen und Zuständigkeiten klar dokumentiert, angemessen verteilt und für die bestehenden Aufgaben ausreichend dimensioniert sind. Dabei ist auch zu bewerten, ob die Organisation geeignet ist, sowohl den laufenden IT-Betrieb als auch die Pflege der Webanwendungen dauerhaft sicherzustellen.

2.2 Prüfbereich „Abgrenzung der Verantwortlichkeiten zwischen IQB und Humboldt-Universität zu Berlin“

Der Auftragnehmer hat bestehende Abhängigkeiten, Schnittstellen, Abstimmungsprozesse, Servicevereinbarungen und Verantwortungsgrenzen zu analysieren und zu bewerten, die durch die geteilten Zuständigkeiten von der HU und dem Auftraggeber entstehen. Dabei ist insbesondere zu prüfen, ob Zuständigkeiten, Kostenanteile, Reaktionszeiten und Risiken hinreichend transparent geregelt

¹ Da die Softwareentwicklung im Rahmen von Projektförderungen finanziert wird, ist dieser Bereich bei der Auswertung der Kosten nicht Gegenstand der Leistung.

sind. Dazu zählen insbesondere Gebäudeverkabelung, Netzwerkinfrastruktur, Internetzugang, E-Mail-Dienste und weitere zentrale Dienste. Der Auftraggeber wird hierzu die Zuständigkeiten der HU darstellen. Als grundlegendes Dokument steht dem Auftragnehmer hierfür das IT-Konzept zur Verfügung, das von der IT des Auftraggebers im zweijährigen Rhythmus überarbeitet wird.

2.3 Prüfbereich „Leistungen des IT-Teams zur Sicherstellung der Arbeitsfähigkeit“

Der Auftragnehmer hat zu untersuchen, welche Leistungen das IT-Team zur Sicherstellung der Arbeitsfähigkeit der Mitarbeiter*innen erbringt. Dazu gehören insbesondere Arbeitsplatz-IT, Endgeräteverwaltung, Benutzerkonten, Berechtigungen, Support, Softwarebereitstellung, Drucker, Telefonie, Dateiablagen und interne Fachanwendungen. Der Auftragnehmer hat zu bewerten, ob diese Leistungen angemessen organisiert, dokumentiert, priorisiert und mit ausreichenden Ressourcen hinterlegt sind. Außerdem sind Qualität, Reaktionsfähigkeit, Ausfallsicherheit und mögliche Effizienzpotenziale im IT-Support zu beurteilen. Als grundlegendes Dokument steht dem Auftragnehmer hierfür das IT-Konzept zur Verfügung.

2.4 Prüfbereich „IT-Kosten, Kostentransparenz und Wirtschaftlichkeit“

Der Auftragnehmer hat die IT-Kosten des Auftraggebers zu erheben, zu strukturieren und zu bewerten. Dabei sind insbesondere Kosten für Personal, Hardware, Software, Lizenzen, Wartung, Support, externe Dienstleistungen und Cloud-Dienste (Hosting) zu berücksichtigen. Dabei sind auch technische Abhängigkeiten, Betriebskosten, Lebenszyklen und absehbare Ersatz- oder Modernisierungsbedarfe zu berücksichtigen. Ziel ist eine Bewertung der Wirtschaftlichkeit sowie die Identifikation von Einspar-, Konsolidierungs- und Steuerungspotenzialen. Grundlage der Bewertung sind die Kostenübersichten der letzten 5 Jahre, die als detaillierte Tabellen (Excel) durch den Auftraggeber bereitgestellt werden sowie das von der IT erstellte IT-Konzept, in dem eine Finanzplanung über 5 Jahre enthalten ist, die die IT im Rahmen der Aufstellung des Doppelhaushalts des Auftraggebers jeweils erstellt.

2.5 Prüfbereich „Informationssicherheit und technische Schutzmaßnahmen“

Der Auftragnehmer hat die bestehenden technischen und organisatorischen Maßnahmen zur Informationssicherheit zu bewerten. Dazu gehören insbesondere Benutzer- und Berechtigungsmanagement, Authentifizierungsverfahren, administrative Zugriffe, Patch- und Schwachstellenmanagement, Virenschutz, Protokollierung, Monitoring, Netzwerksicherheit und Schutz besonders sensibler Daten. Der Auftragnehmer hat zu prüfen, ob die Maßnahmen dem Schutzbedarf der verarbeiteten Informationen entsprechen und ob wesentliche Risiken bestehen. Die Prüfung berücksichtigt sowohl den allgemeinen IT-Betrieb als auch die Entwicklung, Bereitstellung und Nutzung der Webanwendungen.

2.6 Prüfbereich „Backup, Wiederherstellung und Notfallvorsorge“

Der Auftragnehmer hat die bestehenden Backup-, Wiederherstellungs- und Notfallkonzepte zu prüfen. Dabei ist zu bewerten, welche Systeme und Daten gesichert werden, in welchen Intervallen Sicherungen erfolgen, wie Wiederherstellungen getestet werden und welche Verantwortlichkeiten im Notfall bestehen. Der Auftragnehmer hat zu untersuchen, ob die bestehenden Maßnahmen geeignet sind, den Betrieb des IQB und die Verfügbarkeit wesentlicher Anwendungen innerhalb angemessener Zeit wiederherzustellen.

2.7 Prüfbereich „Prozesse der Webentwicklung“

Der Auftragnehmer hat die Prozesse zur Entwicklung der Webanwendungen des Auftraggebers umfassend zu analysieren. Dazu gehören Anforderungsaufnahme, Priorisierung, Planung, Aufwandschätzung, Umsetzung, Code Reviews, Qualitätssicherung, Testmanagement, Dokumentation, Releaseplanung und Deployment. Der Auftragnehmer hat zu bewerten, ob die Prozesse nachvollziehbar, effizient, sicher und geeignet sind, qualitativ hochwertige und wartbare Anwendungen

bereitzustellen. Dabei ist auch zu prüfen, ob Zuständigkeiten, Entscheidungswege und Übergaben zwischen Entwicklung, Betrieb und Nutzenden klar geregelt sind.

2.8 Prüfbereich „Nutzung durch die Länder und Anforderungen des computerbasierten Testens“

Der Auftragnehmer hat zu berücksichtigen, dass die Webanwendungen dem computerbasierten Testen von Schüler*innen dienen. Er hat zu prüfen, ob die Entwicklungs-, Betriebs- und Supportprozesse den besonderen Anforderungen dieses Einsatzbereichs angemessen Rechnung tragen. Dazu gehören insbesondere Verfügbarkeit, Belastbarkeit, Datenschutz, Datensicherheit, IT-Sicherheit, Supportfähigkeit und langfristige Wartbarkeit.

2.9 Priorisierte Maßnahmen und Ergebnisdarstellung

Der Auftragnehmer hat die Ergebnisse des Audits in einem schriftlichen Bericht zusammenzufassen. Für jeden Prüfbereich sind Feststellungen, Risiken, Kostenaspekte und Verbesserungspotenziale darzustellen. Die Empfehlungen sind in einer priorisierten Maßnahmenliste aufzubereiten. Für jede Maßnahme werden mindestens Ziel, Nutzen, geschätzter Umsetzungsaufwand, Dringlichkeit, mögliche Einspar- oder Effizienzpotenziale sowie Risiken einer Nichtumsetzung beschrieben. Die Ergebnisse zum Prüfbereich IT-Sicherheit sind in einem separaten Berichtsteil darzustellen.

2.10 Datenschutz und Verschwiegenheit

Der Auftragnehmer muss gewährleisten, dass die Anforderungen an den Datenschutz, insbesondere der EU-Datenschutz-Grundverordnung jederzeit beachtet wird. Die interne Datenstruktur (Netzwerke) des Auftragnehmers muss jederzeit den datenschutzrechtlichen Anforderungen entsprechen. Dokumente, Unterlagen und Interviewmitschriften hat der Auftragnehmer sechs Monate nach Vertragsende aufzubewahren. Danach muss der Auftragnehmer eine fachgerechte, d.h. datenschutzrechtlich abgesicherte Entsorgung der Originaldateien und -ausdrucke (digitale und ausgedruckte Unterlagen) sowie eventuell noch vorhandener Kopien durchführen.

Die Vernichtung der Materialien ist jeweils zu dokumentieren und dem Auftraggeber nachzuweisen.

Alle mit der Ausführung beschäftigten Mitarbeiter*innen müssen sich schriftlich zur vertraulichen Behandlung aller auftragsbezogenen Informationen einschließlich sämtlicher Dokumente, Unterlagen und Interviews verpflichten und eine Verschwiegenheitserklärung unterzeichnen.

3 Zeitplan und Ablauf

Das IT-Audit wird innerhalb eines Zeitraums von voraussichtlich zehn bis zwölf Wochen nach Auftragserteilung durchgeführt. Der Auftragnehmer hat mit dem Angebot einen konkreten Projekt- und Zeitplan vorzulegen, aus dem die vorgesehenen Arbeitsschritte, Meilensteine, Mitwirkungspflichten des IQB sowie die geplanten Termine für Zwischen- und Endergebnisse hervorgehen.

Der Ablauf umfasst mindestens folgende Phasen:

Phase	Zeitraum	Inhalt
1. Projektstart und Kick-off	Woche 1	Abstimmung von Zielsetzung, Prüfungsumfang, Ansprechpartnerinnen und Ansprechpartnern, Kommunikationswegen, benötigten Unterlagen sowie Terminplanung.
2. Dokumenten- und Datenanforderung	Woche 1 bis 2	Anforderung und Sichtung relevanter Unterlagen, insbesondere Kostenübersichten, Verträge, Lizenzinformationen, Organisationsunterlagen, Systemdokumentationen, Prozessbeschreibungen und Sicherheitskonzepte.

3. Ist-Aufnahme und Interviews	Woche 2 bis 5	Durchführung strukturierter Interviews mit relevanten Personen aus IT, Verwaltung, Leitung, Softwareentwicklung und gegebenenfalls weiteren Fachbereichen. Erfassung der IT-Organisation und Kostenstrukturen.
4. Analyse und Bewertung	Woche 3 bis 7	Auswertung der erhobenen Informationen. Bewertung von Wirtschaftlichkeit, Kostentransparenz, IT-Betrieb, Informationssicherheit, Infrastruktur und Schnittstellen zur Humboldt-Universität zu Berlin.
5. Zwischenstand/Zwischengespräch	ca. Woche 6 oder 7	Vorstellung vorläufiger Feststellungen, Klärung offener Fragen und Abstimmung weiterer Prüfungsschwerpunkte. Der Auftragnehmer hat wesentliche erste Erkenntnisse, erkennbare Risiken und noch offene Informationsbedarfe darzustellen.
6. Berichtsentwurf	Woche 8 bis 9	Erstellung eines schriftlichen Berichtsentwurfs mit Feststellungen, Risikobewertung, Kostenanalyse, Bewertung der Entwicklungsprozesse und priorisierte Maßnahmen. Der Berichtsentwurf muss die Ergebnisse zum Prüfbereich IT-Sicherheit als separaten Teil darstellen.
7. Kommentierung durch das IQB	Woche 9 bis 10	Möglichkeit des IQB, sachliche Hinweise, Korrekturen und Ergänzungen zum Berichtsentwurf einzubringen. Der Auftragnehmer hat diese zu prüfen und nachvollziehbar zu berücksichtigen.
8. Abschlussbericht und Ergebnispräsentation	Woche 10 bis 11	Vorlage des finalen Auditberichts einschließlich Management-Zusammenfassung und priorisierter Maßnahmenliste. Präsentation der Ergebnisse in einem Abschlussgespräch mit dem IQB.

Der Abschlussbericht hat spätestens bis zum 03.12.2026 vorzuliegen.

Der Auftragnehmer hat den Zeitplan in Abstimmung mit dem Auftraggeber so zu gestalten, dass die Belastung der Mitarbeiter*innen des Auftraggebers durch Interviews, Rückfragen und Unterlagenbereitstellung angemessen begrenzt wird. Verzögerungen, die sich aus fehlenden Unterlagen, notwendigen Abstimmungen mit der Humboldt-Universität zu Berlin oder zusätzlichen Prüfbedarfen ergeben, sind frühzeitig anzuzeigen und mit dem Auftraggeber abzustimmen.

Abweichungen vom vorgesehenen Zeitplan sind nur nach vorheriger Abstimmung mit dem Auftraggeber zulässig. Der finale Auditbericht ist spätestens zum 03.12.2026 vorzulegen, sofern keine anderweitige Vereinbarung getroffen wird.

Der Auftraggeber prüft den vom Auftragnehmer vorgelegten Berichtsentwurf innerhalb von zwei Wochen auf sachliche Richtigkeit und Vollständigkeit der zugrunde gelegten Informationen. Etwaige Hinweise, Korrekturen oder Ergänzungen sind dem Auftragnehmer innerhalb dieser Frist mitzuteilen, die der Auftragnehmer umzusetzen hat. Erfolgt innerhalb der vereinbarten Frist keine Rückmeldung, gilt der Entwurf als abgenommen. Der Auftragnehmer hat nach Abnahme des Entwurfs den Bericht auf dieser Grundlage zu finalisieren und dem Auftraggeber spätestens zwei Wochen nach Abnahme zur Verfügung zu stellen.

4 Mitwirkungsobliegenheiten des Auftraggebers

Dem Auftraggeber obliegen folgende Mitwirkungsleistungen:

- Der Auftraggeber benennt zu Beginn des Projekts eine zentrale Ansprechperson sowie eine Stellvertretung für organisatorische, fachliche und administrative Abstimmungen. Diese koordinieren die Bereitstellung von Unterlagen, die Terminabstimmung für Interviews und Workshops sowie die Kommunikation mit den relevanten Stellen innerhalb des IQB.
- Der Auftraggeber stellt dem Auftragnehmer die für das IT-Audit erforderlichen Unterlagen und Informationen zur Verfügung, soweit diese vorhanden sind und rechtlich sowie organisatorisch bereitgestellt werden dürfen. Dazu gehören insbesondere Organisationsunterlagen, Kostenübersichten, Budget- und Beschaffungsunterlagen, Vertrags- und Lizenzinformationen, IT-Dokumentationen, Systemübersichten, Sicherheitskonzepte, Prozessbeschreibungen, Entwicklungsdokumentationen, Repository- und Release-Informationen sowie Unterlagen zu Betrieb, Wartung und Support der Webanwendungen.
- Der Auftraggeber ermöglicht dem Auftragnehmer den Zugang zu den für das Audit relevanten Ansprechpartner*innen. Dazu zählen insbesondere Personen aus IT-Betrieb, Softwareentwicklung, Verwaltung, Institutsleitung sowie gegebenenfalls fachliche Verantwortliche für die Webanwendungen. Der Auftraggeber wirkt darauf hin, dass Interviews, Workshops und Rückfragen innerhalb angemessener Fristen ermöglicht und beantwortet werden.
- Soweit für das Audit erforderlich, ermöglicht der Auftraggeber dem Auftragnehmer Einsicht in relevante Systeme, Anwendungen, Repositories, Dokumentationssysteme, Ticket- oder Projektmanagementsysteme, Monitoring- oder Betriebsinformationen sowie Kosten- und Vertragsunterlagen. Die Einsicht erfolgt grundsätzlich in Abstimmung mit dem Auftraggeber und, soweit erforderlich, lesend, zeitlich begrenzt und unter Beachtung der geltenden Datenschutz- und Sicherheitsanforderungen. Administrative Zugänge oder technische Prüfungen werden nur gewährt bzw. durchgeführt, wenn dies ausdrücklich abgestimmt und freigegeben wurde.
- Der Auftraggeber informiert den Auftragnehmer über die Schnittstellen und Abhängigkeiten zur HU, soweit diese für das Audit relevant sind. Hierzu gehört insbesondere die Bereitstellung vorhandener Vereinbarungen, Leistungsbeschreibungen, Ansprechpartnerinnen und Ansprechpartner, Zuständigkeitsabgrenzungen und Informationen zu von der HU bereitgestellten Infrastrukturdiensten. Eine Mitwirkung der HU selbst ist derzeit nicht vorgesehen.
- Der Auftraggeber stellt sicher, dass dem Auftragnehmer rechtzeitig mitgeteilt wird, welche Informationen, Systeme oder Unterlagen besonderen Vertraulichkeits-, Datenschutz- oder Sicherheitsanforderungen unterliegen. Der Auftraggeber informiert den Auftragnehmer außerdem über organisatorische Vorgaben, interne Sicherheitsrichtlinien, Zugangsregelungen und etwaige Einschränkungen bei der Nutzung oder Verarbeitung bereitgestellter Informationen.