Arbeitsaufgaben in Abstimmung mit kundenspezifischen Geschäfts- und Leistungsprozessen

AP1-CHECK GESCHÄFTS- UND LEISTUNGSPROZESSE

IT-Arbeit ist kein „ich bastel mal", sondern läuft als strukturierter **Prozess** mit klaren Zuständen, definierten Rollen und lückenlosen Nachweisen. In der Praxis bedeutet dies: Jede Tätigkeit folgt einem nachvollziehbaren Ablauf, der dokumentiert, messbar und wiederholbar ist. Dies ist nicht nur Best Practice, sondern Prüfungsinhalt und beruflicher Standard zugleich.

Stellen Sie sich folgenden realistischen Fall vor: Nach einer geplanten Firewall-Umstellung melden sich plötzlich mehrere Benutzer mit unterschiedlichen Beschwerden: „Das Internet ist extrem langsam geworden", „Meine VPN-Verbindung bricht ständig ab", „Bestimmte Websites, die ich für meine Arbeit brauche, sind nicht mehr erreichbar". Genau solche Situationen zeigen, warum strukturierte Prozesse unverzichtbar sind – und wie schnell aus einer technischen Änderung ein komplexes Service-Management-Szenario wird.

Geschäftsprozess vs. Leistungsprozess – prüfungsfest verstehen

Die Unterscheidung zwischen Geschäfts- und Leistungsprozessen ist eine klassische Prüfungsfrage und essenziell für das Verständnis der IT-Rolle im Unternehmen. Hier die klare Abgrenzung:

Geschäftsprozess: Direkt wertschöpfend für das Unternehmen. Diese Prozesse generieren Umsatz oder tragen unmittelbar zur Kundenzufriedenheit bei. Beispiele sind „Auftrag bearbeiten", „Rechnung stellen", „Ware ausliefern" oder „Kundenanfrage beantworten". Sie sind das Kerngeschäft des Unternehmens.

Leistungsprozess (IT-Service): Unterstützend, liefert oder stützt die Leistungserbringung. Diese Prozesse ermöglichen erst die Geschäftsprozesse oder halten sie am Laufen. Beispiele: „Störung beheben", „Change umsetzen", „Benutzer anlegen", „System überwachen". IT-Services sind Enabler, keine direkten Wertschöpfer.

Merksatz für die Prüfung: Geschäft = „Geld verdienen/Leistung erbringen" · IT-Leistung = „Service am Laufen halten und ermöglichen"

Zuordnungsübung: Geschäfts- oder Leistungsprozess?

1

Incident bearbeiten

Leistungsprozess – Unterstützt die IT-Infrastruktur, stellt den Service wieder her. Kein direkter Umsatz, aber notwendig für Geschäftskontinuität.

2

Angebot schreiben

Geschäftsprozess – Direkt wertschöpfend, Teil des Vertriebsprozesses. Führt potenziell zu Aufträgen und Umsatz.

3

Benutzer anlegen

Leistungsprozess – IT-Service Request, ermöglicht Mitarbeitern die Arbeit. Standardisierter Support-Prozess.

4

Rechnung erstellen

Geschäftsprozess – Teil des Finanzprozesses, direkt umsatzrelevant. Kerngeschäft der Buchhaltung.

5

System patchen

Leistungsprozess – Wartung und Sicherheit der IT-Infrastruktur. Change-Management-Aktivität, die Geschäftsprozesse schützt.

Diese Unterscheidung ist nicht akademisch: In der Praxis bestimmt sie, wie Aufwände verrechnet werden, wie SLAs definiert sind und wie Prioritäten gesetzt werden. In der Prüfung wird oft nach der korrekten Einordnung und Begründung gefragt.

Kundenkommunikation – das Minimum, das in der Prüfung erwartet wird

Kommunikation ist nicht „nett zu haben", sondern Teil der Service-Qualität und wird in praktischen Prüfungsaufgaben regelmäßig abgefragt. Das Ziel: Erwartungen steuern und Nachweise schaffen.

Kommunikationsinhalte (Ticket/Telefon/E-Mail):

- **Problem präzise beschreiben + Impact benennen:** „Wer ist betroffen?" – ein User, eine Abteilung, der gesamte Standort?
- **Rückfragen strukturiert stellen:** Reproduzierbarkeit klären, Zeitpunkt, betroffene Systeme, Fehlermeldungen
- **Nächste Schritte konkret kommunizieren + Zeitfenster nennen:** „Wir prüfen die Firewall-Logs bis 13:00 Uhr"
- **Zwischenstatus geben, wenn es länger dauert:** Nicht schweigen! Alle 2-4 Stunden informieren
- **Abschluss mit Lösung + Prävention:** Was wurde getan? Wie wird es verhindert?

Prüfungsfalle: „Wir melden uns" ist keine Information und in der Prüfung zu unspezifisch. Besser: „Update um 14:00 Uhr, Workaround bis dahin: Nutzen Sie Browser XY statt Z"

Praxisbeispiel: Statusmail an den Kunden formulieren

> Betreff: Störung VPN-Verbindung – Status-Update und Workaround
>
> Sehr geehrte/r [Kunde],
>
> vielen Dank für Ihre Meldung bezüglich der instabilen VPN-Verbindung. Wir haben das Problem analysiert und identifiziert: Nach der gestrigen Firewall-Umstellung werden bestimmte VPN-Pakete verzögert verarbeitet, was zu Verbindungsabbrüchen führt.
>
> **Workaround bis zur finalen Lösung:** Bitte nutzen Sie alternativ den VPN-Server „vpn2.unternehmen.de" (Zugangsdaten unverändert). Dieser ist von der Störung nicht betroffen.
>
> **Nächste Schritte:** Unser Netzwerk-Team nimmt heute um 14:00 Uhr eine Korrektur der Firewall-Regelung vor. Der Test erfolgt um 15:30 Uhr. Sie erhalten spätestens um 16:00 Uhr eine Rückmeldung zur finalen Lösung.
>
> Bei Rückfragen stehen wir Ihnen jederzeit zur Verfügung – Ticket-Nr. INC-2024-1337.
>
> Mit freundlichen Grüßen,
> IT-Service Desk

Diese Struktur zeigt alle geforderten Elemente: Problem, Impact, Workaround, Zeitfenster, nächste Schritte und Kontaktmöglichkeit. In der Prüfung wird genau diese Vollständigkeit bewertet.

Fehlermanagement – Fehler ist nicht gleich Störung

Ein häufiger Irrtum: Incident geschlossen = Problem gelöst. Falsch! **Fehlermanagement** geht tiefer und sucht die **Root Cause** (Grundursache), um dauerhafte Beseitigung zu erreichen. Während Incident Management auf schnelle Wiederherstellung zielt, analysiert Fehlermanagement systematisch.

Typische Fehlerursachen:

- Software-Bug in einer Anwendung oder im Betriebssystem
- Falsche oder unvollständige Konfiguration (z.B. Firewall-Regel, DNS-Eintrag)
- Fehlendes oder unzureichendes Monitoring (Problem wird zu spät erkannt)
- Prozesslücke oder unklare Zuständigkeiten in Abläufen
- Fehlende Dokumentation oder veraltete Wissensdatenbank

Ergebnis des Fehlermanagements: Detaillierte Fehleranalyse + dauerhafter Fix + dokumentierte Präventionsmaßnahme. Oft wird ein Known Error angelegt, bis die finale Lösung verfügbar ist.

5-Why-Methode

5-mal „Warum?" fragen, bis zur eigentlichen Ursache vordringen

Ishikawa-Diagramm

Ursache-Wirkung visualisieren (Mensch, Maschine, Methode, Material)

Lessons Learned

Was lief gut/schlecht? Wie vermeiden wir Wiederholung?

Praxisbeispiel: Incident „User kann sich nicht anmelden" wird 3x geschlossen mit „Passwort zurückgesetzt". Fehlermanagement deckt auf: Account wird nachts automatisch deaktiviert (Skript-Fehler). Fix: Skript korrigieren + Monitoring ergänzen.

Störungsmanagement (Incident Management) – schnell wieder „Service läuft"

Ziel des Incident Management: Den normalen Betrieb so schnell wie möglich wiederherstellen – kontrolliert, nachvollziehbar und mit minimaler negativer Auswirkung auf das Business.

Typische Schritte im Detail:

1. **Ticket annehmen + klassifizieren:** Incident oder Request? Welche Kategorie? Erste Symptome erfassen
2. **Priorität festlegen:** Impact × Urgency bestimmen (siehe Matrix nächste Folie)
3. **Diagnose + Workaround:** Ursache eingrenzen, temporäre Lösung bereitstellen
4. **Lösung umsetzen:** Dauerhafte Behebung oder Eskalation an 2nd/3rd Level
5. **Test + Validierung:** Mit Kunde/User testen, Funktionalität bestätigen
6. **Kommunikation + Abschluss:** Kunde informieren, Ticket mit Lösung schließen

Firewall-Fall – typische Incidents nach Change:

- DNS-Auflösung blockiert → „Webseiten nicht erreichbar"
- IPS (Intrusion Prevention) blockt legitime App → „Teams/Banking funktioniert nicht"
- Routing/NAT fehlkonfiguriert → „VPN baut keine Verbindung auf"

Supportanfragen (Service Request) – kein Incident!

Ein **Service Request** ist kein Fehler, sondern eine Anfrage zur Bereitstellung oder Änderung eines standardisierten Service. Beispiele: „Neuer Benutzer anlegen", „VPN-Zugang freischalten", „Software installieren", „Firewall-Port 443 für Anwendung X freigeben".

Kritischer Unterschied:

- **Incident:** Etwas ist kaputt, funktioniert nicht wie erwartet. Ziel: Wiederherstellung des Normalzustands
- **Service Request:** Etwas soll bereitgestellt, geändert oder konfiguriert werden. Ziel: Erfüllung einer Anforderung

Diese Unterscheidung ist nicht Haarspalterei, sondern hat konkrete Auswirkungen: Service Requests haben andere SLAs (oft länger), andere Prioritätslogiken und andere Genehmigungsprozesse. Außerdem würde die Vermischung von Incidents und Requests die Statistiken verfälschen und echte Störungen unsichtbar machen.

Prüfungsfalle: Alles als „Störung" zu behandeln, führt zu falschen SLA-Messungen, verfälschten KPIs und ineffizienter Ressourcennutzung. In der Prüfung wird die korrekte Klassifikation explizit abgefragt.

Zuordnungsübung

Incident oder Service Request?

1) „Passwort vergessen"→ *Service Request (Standardprozess, kein Fehler)*

2) „Drucker druckt nicht"→ *Incident (Störung, etwas funktioniert nicht)*

3) „Neuen Laptop einrichten"→ *Service Request (Bereitstellung neuer Hardware)*

4) „VPN geht seit heute nicht mehr"→ *Incident (Störung, vorher funktionierte es)*

Bearbeitungsstatus & Priorisierung – strukturiert statt chaotisch

Wichtige Felder im Ticket (prüfungsrelevant): Kategorie (Incident/Request/Problem), Priorität (1-4), SLA-Ziel (Reaktions-/Lösungszeit), Betroffene Systeme/User, Beschreibung des Problems, Reproduktionsschritte, Workaround, finale Lösung, alle Zeitstempel (Erstellt, Begonnen, Gelöst, Geschlossen), Verantwortlicher Techniker/Team.

Prüfungsfalle: „Gelöst" ≠ „Geschlossen". Ein Ticket ist erst geschlossen, wenn der Kunde die Lösung bestätigt hat ODER eine definierte Frist (z.B. 3 Tage) ohne Rückmeldung verstrichen ist.

Impact × Urgency Matrix

Impact: Wie groß ist der Schaden? 1 User vs. Abteilung vs. ganzes Unternehmen
Urgency: Wie dringend? Deadline, Produktion steht, regulatorische Anforderung

1	2	3	4
Kritisch	**Hoch**	**Mittel**	**Niedrig**
Hoher Impact + hohe Urgency (z.B. Standort offline)	Hoher Impact oder hohe Urgency	Moderater Impact/Urgency	1 User, keine Dringlichkeit

Prüfungsnahe Fallübung – Firewall-Change-Szenario

Ausgangssituation: Nach einem geplanten Firewall-Change am Wochenende melden sich am Montagmorgen fünf verschiedene Tickets. Ihre Aufgabe: Klassifizieren Sie jedes Ticket als Incident oder Service Request, setzen Sie die Priorität (1-4) und geben Sie den initialen Status sowie die nächste Aktion an.

1	**Ticket A: „Standort offline – niemand kommt ins Netz"** Incident | **Priorität 1 (kritisch)** | Status: *In Bearbeitung* **Nächste Aktion:** Sofortige Analyse der Firewall-Routing-Regeln, Prüfung NAT/DHCP, ggf. Rollback der Change-Konfiguration. Alle verfügbaren Techniker einbinden, Management sofort informieren.
2	**Ticket B: „Bestimmte Website (externe Fachplattform) geblockt"** Incident | **Priorität 3 (mittel)** | Status: *In Bearbeitung* **Nächste Aktion:** Firewall-Logs prüfen (IPS/Content-Filter?), betroffene URL/IP identifizieren, Whitelist-Regel erstellen und testen. Workaround: Alternative Zugangsmöglichkeit prüfen.
3	**Ticket C: „VPN bricht alle paar Minuten ab"** Incident | **Priorität 2 (hoch)** | Status: *In Bearbeitung* **Nächste Aktion:** VPN-Gateway-Logs analysieren, Paket-Drops identifizieren (MTU? Timeouts?), Firewall-Regel für VPN-Port/Protokoll verifizieren. Workaround: Alternativen VPN-Server anbieten.
4	**Ticket D: „Neuer Benutzer benötigt VPN-Zugriff"** Service Request | **Priorität 3 (Standard-SLA)** | Status: *Warten auf Genehmigung* **Nächste Aktion:** Genehmigung durch Vorgesetzten einholen (falls noch nicht vorhanden), dann VPN-Account anlegen, Zugangsdaten versenden, Einrichtungsanleitung mitschicken.
5	**Ticket E: „Log-Export für Compliance-Audit benötigt"** Service Request | **Priorität 2 (Deadline beachten!)** | Status: *In Bearbeitung* **Nächste Aktion:** Zeitraum und Umfang klären, Firewall-Logs exportieren (Format: CSV/Syslog?), Datenschutz/Anonymisierung prüfen, verschlüsselt an Auditor übermitteln.

Diese Übung zeigt die Komplexität realer Service-Management-Situationen: Mehrere Tickets mit unterschiedlicher Dringlichkeit und Art erfordern strukturierte Priorisierung, klare Klassifikation und paralleles Arbeiten. Genau diese Fähigkeit wird in der Abschlussprüfung AP1 getestet.