9.3 Genehmigungen und Freigabeverfahren

> **Kurz erklärt**
>
> Nicht jeder Service Request darf sofort ausgeführt werden.
>
> Viele Leistungen verursachen Kosten, verändern Berechtigungen oder beeinflussen Sicherheit und Compliance.
>
> Deshalb benötigen bestimmte Requests vor der Bearbeitung eine oder mehrere Genehmigungen.
>
> Ziel ist es, Risiken zu reduzieren, Verantwortlichkeiten eindeutig festzulegen und gleichzeitig unnötige Wartezeiten zu vermeiden.

Warum Genehmigungen notwendig sind

Genehmigungen stellen sicher, dass eine angeforderte Leistung berechtigt, sinnvoll und zulässig ist.

Sie helfen dabei:

- unberechtigte Zugriffe zu verhindern,
- Kosten zu kontrollieren,
- Sicherheitsrichtlinien einzuhalten,
- gesetzliche Vorgaben umzusetzen,
- Verantwortlichkeiten nachzuweisen,
- Änderungen nachvollziehbar zu dokumentieren.

Eine Genehmigung bedeutet dabei nicht automatisch eine lange Bearbeitungszeit.

Gut definierte Standardprozesse können Genehmigungen weitgehend automatisieren.

Was ist eine Genehmigung?

Eine Genehmigung ist die formelle Zustimmung einer berechtigten Person oder Stelle zur Durchführung eines Service Requests.

Die Genehmigung bestätigt beispielsweise:

- der Benutzer darf die Leistung erhalten,
- Budget steht zur Verfügung,

- Sicherheitsanforderungen sind erfüllt,
- Unternehmensrichtlinien werden eingehalten,
- Risiken sind akzeptiert.

Erst danach beginnt – sofern erforderlich – die eigentliche Bearbeitung.

Nicht jeder Request benötigt eine Genehmigung

Viele Standardleistungen können ohne zusätzliche Freigabe bereitgestellt werden.

Beispiele:

- Passwort zurücksetzen
- Entsperren eines Benutzerkontos
- Abrufen eines Knowledge-Artikels
- Installation bereits freigegebener Standardsoftware
- Download eines Druckertreibers

Hier würde eine zusätzliche Genehmigung lediglich den Prozess unnötig verzögern.

Wann Genehmigungen sinnvoll sind

Eine Genehmigung ist häufig erforderlich bei:

- neuer Software
- kostenpflichtigen Lizenzen
- zusätzlicher Hardware
- erweiterten Berechtigungen
- Administratorrechten
- VPN-Zugängen
- Cloud-Ressourcen
- neuen Benutzerkonten
- Zugriff auf sensible Daten
- Änderungen an sicherheitskritischen Systemen

Je höher Risiko oder Kosten, desto wichtiger wird eine Freigabe.

Typische Genehmigungsstellen

Je nach Organisation können unterschiedliche Stellen beteiligt sein.

Beispiele:

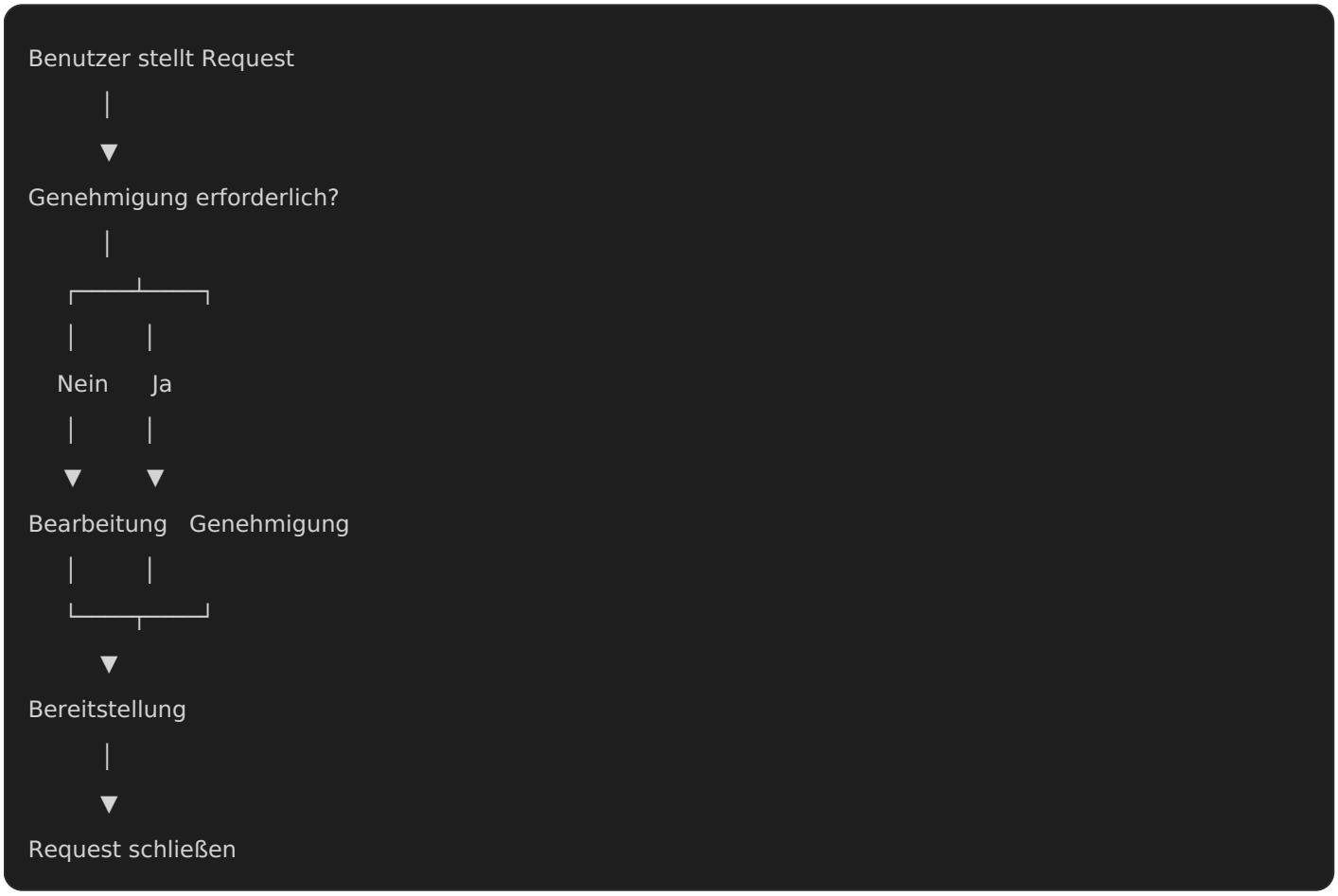
Anfrage	Genehmigung

Notebook	Vorgesetzter
Softwarelizenz	Lizenzmanagement
Administratorrechte	Informationssicherheit
SAP-Berechtigung	Fachbereich
Cloud-Ressourcen	Kostenstellenverantwortlicher
VPN-Zugang	Vorgesetzter oder IT-Sicherheit
Mobiltelefon	Einkauf oder Kostenstelle

Die zuständige Stelle sollte im Request Model eindeutig definiert sein.

Einfacher Genehmigungsprozess

Ein typischer Ablauf:



Nicht jeder Request durchläuft denselben Ablauf.

Mehrstufige Genehmigungen

Komplexere Requests können mehrere Freigaben benötigen.

Beispiel:

Ein Administratorzugang wird beantragt.

Mögliche Reihenfolge:

1. Vorgesetzter
2. Informationssicherheit
3. Systemverantwortlicher

Erst nach allen Genehmigungen beginnt die technische Umsetzung.

Parallele Genehmigungen

Nicht alle Freigaben müssen nacheinander erfolgen.

Sind Genehmigungen unabhängig voneinander, können sie parallel eingeholt werden.

Vorteile:

- kürzere Bearbeitungszeit,
- weniger Wartezeiten,
- bessere Planbarkeit.

Dies wird von vielen ITSM-Systemen unterstützt.

Genehmigungsregeln

Ein Request Model sollte eindeutig festlegen:

- Wer genehmigt?
- Wann wird genehmigt?
- Welche Kriterien gelten?
- Wann entfällt eine Genehmigung?
- Was passiert bei einer Ablehnung?
- Gibt es Vertretungsregelungen?
- Welche Fristen gelten?

Klare Regeln vermeiden Rückfragen und Verzögerungen.

Genehmigung ist keine technische Prüfung

Die Genehmigung beantwortet in erster Linie organisatorische Fragen.

Beispiele:

- Ist die Software notwendig?
- Ist Budget vorhanden?
- Darf der Benutzer den Zugriff erhalten?
- Ist die Anfrage nachvollziehbar?

Die technische Umsetzung erfolgt anschließend durch die zuständigen IT-Teams.

Ablehnung eines Requests

Nicht jeder Request wird genehmigt.

Mögliche Gründe:

- fehlendes Budget,
- unzureichende Begründung,
- Sicherheitsrisiko,
- fehlende Berechtigung,
- Lizenz nicht verfügbar,
- Richtlinie verbietet die Leistung,
- falscher Antrag.

Eine Ablehnung sollte dokumentiert und nachvollziehbar begründet werden.

Vertretungsregelungen

Genehmigungen dürfen nicht von einzelnen Personen abhängig sein.

Deshalb sollten Vertretungen definiert werden.

Beispiele:

- Abwesenheit wegen Urlaub,
- Krankheit,
- Dienstreise,
- organisatorische Änderungen.

Fehlende Vertretungen führen häufig zu langen Bearbeitungszeiten.

Fristen für Genehmigungen

Viele Organisationen definieren Zielzeiten.

Beispiele:

Genehmigung	Zielzeit

Vorgesetzter	1 Arbeitstag
Lizenzmanagement	4 Stunden
Informationssicherheit	2 Arbeitstage
Einkauf	3 Arbeitstage

Werden Fristen überschritten, kann eine Erinnerung oder Eskalation erfolgen.

Automatische Genehmigungen

Einige Requests können automatisch genehmigt werden.

Beispiele:

- Standardsoftware innerhalb einer Abteilung
- zweiter Monitor nach Unternehmensrichtlinie
- Passwort zurücksetzen
- Druckertreiber installieren

Voraussetzung ist, dass alle Regeln bereits definiert wurden.

Bedingte Genehmigungen

Manche Genehmigungen hängen von Bedingungen ab.

Beispiele:

- Hardwarewert über 1.000 Euro
- Administratorrechte länger als 24 Stunden
- Zugriff auf personenbezogene Daten
- Software außerhalb des Standardportfolios

Sind die Bedingungen nicht erfüllt, entfällt die zusätzliche Freigabe.

Genehmigungen dokumentieren

Jede Genehmigung sollte nachvollziehbar gespeichert werden.

Typische Informationen:

- Genehmiger
- Datum
- Entscheidung
- Bemerkung

- Version des Requests
- eventuelle Auflagen

Dadurch bleibt später nachvollziehbar, warum eine Leistung bereitgestellt wurde.

Genehmigungen und Compliance

Viele gesetzliche oder interne Vorgaben verlangen dokumentierte Genehmigungen.

Beispiele:

- ISO/IEC 27001
- Datenschutz
- Informationssicherheitsrichtlinien
- interne Compliance-Vorgaben
- Lizenzmanagement
- Finanzvorgaben

Eine fehlende Dokumentation kann später zu Problemen bei Audits führen.

Genehmigungen und Least Privilege

Das Prinzip der minimalen Berechtigung spielt eine wichtige Rolle.

Benutzer sollen nur die Rechte erhalten,

die sie tatsächlich benötigen.

Deshalb benötigen insbesondere folgende Requests häufig zusätzliche Genehmigungen:

- Administratorrechte
- Datenbankzugriffe
- Domänenadministration
- Firewall-Änderungen
- Cloud-Administrationsrechte
- Zugriff auf personenbezogene Daten

Temporäre Berechtigungen

Nicht jede Berechtigung muss dauerhaft vergeben werden.

Beispiele:

- Administratorrechte für einen Tag
- Projektzugriff für vier Wochen

- Testumgebung bis Projektende
- externer Zugriff bis Wartungsende

Nach Ablauf sollte die Berechtigung automatisch entzogen werden.

Genehmigungen regelmäßig überprüfen

Genehmigungsprozesse sollten regelmäßig bewertet werden.

Fragen dabei:

- Gibt es unnötige Freigaben?
- Entstehen lange Wartezeiten?
- Werden Genehmigungen häufig abgelehnt?
- Können Schritte automatisiert werden?
- Stimmen Verantwortlichkeiten noch?
- Haben sich Richtlinien geändert?

Ein effizienter Prozess schützt die Organisation, ohne die Benutzer unnötig auszubremsen.

Praxisbeispiel

Ein Entwickler benötigt Administratorrechte auf seinem Notebook.

Der Ablauf:

1. Entwickler stellt Request.
2. Vorgesetzter bestätigt die Notwendigkeit.
3. Informationssicherheit prüft das Risiko.
4. IT vergibt die Berechtigung.
5. Die Rechte gelten nur für zwei Wochen.
6. Nach Ablauf werden sie automatisch entfernt.

So bleiben Sicherheit und Nachvollziehbarkeit gewährleistet.

Typische Fehler

Fehler 1

Jeder Request benötigt dieselben Genehmigungen.

Fehler 2

Genehmigungen sind nicht dokumentiert.

Fehler 3

Vertretungen fehlen.

Fehler 4

Genehmigungen verzögern Standardleistungen unnötig.

Fehler 5

Ablehnungen werden nicht begründet.

Fehler 6

Administratorrechte werden dauerhaft vergeben.

Fehler 7

Genehmigungsregeln sind unklar.

Fehler 8

Abgelaufene Berechtigungen werden nicht entfernt.

Fehler 9

Genehmigungen erfolgen außerhalb des ITSM-Systems und sind später nicht nachvollziehbar.

Fehler 10

Genehmigungsprozesse werden nie überprüft oder verbessert.

Checkliste Genehmigungen

- [ ] Genehmigung erforderlich?
- [ ] Genehmiger eindeutig definiert
- [ ] Antrag vollständig
- [ ] Voraussetzungen erfüllt
- [ ] Fristen berücksichtigt

- [ ] Vertretung vorhanden
- [ ] Entscheidung dokumentiert
- [ ] Benutzer informiert
- [ ] Bereitstellung durchgeführt
- [ ] Request abgeschlossen

Checkliste Berechtigungs-Requests

- [ ] Benutzer eindeutig identifiziert
- [ ] Berechtigung notwendig
- [ ] Least-Privilege-Prinzip eingehalten
- [ ] Genehmigung dokumentiert
- [ ] Ablaufdatum definiert (falls erforderlich)
- [ ] Protokollierung aktiviert
- [ ] regelmäßige Überprüfung geplant
- [ ] Entzug nach Ablauf vorgesehen

Bedeutung für Fachinformatiker für Systemintegration

Fachinformatiker setzen viele genehmigte Service Requests technisch um.

Typische Aufgaben:

- Benutzerkonten erstellen,
- Gruppenberechtigungen vergeben,
- Administratorrechte einrichten,
- Software bereitstellen,
- Hardware ausgeben,
- Dokumentationen pflegen,
- Genehmigungen prüfen,
- zeitlich begrenzte Berechtigungen verwalten.

Dabei müssen technische Umsetzung und dokumentierte Genehmigung immer zusammenpassen.

Zusammenfassung

> Benutzer stellt Request

↓

Genehmigung erforderlich?

↓

Genehmiger prüfen Anfrage

↓

Freigabe oder Ablehnung

↓

Bereitstellung der Leistung

↓

Dokumentation

↓

Benutzer informieren

↓

Request abschließen

Merksätze

> Nicht jeder Service Request benötigt eine Genehmigung.

> Genehmigungen schützen Sicherheit, Budget und Compliance.

> Standardleistungen sollten möglichst automatisiert freigegeben werden.

> Administratorrechte sollten zeitlich begrenzt vergeben werden.

>

> Genehmigungen müssen nachvollziehbar dokumentiert sein.

Verwandte Seiten

- 9.1 Ziele und Grundlagen des Service Request Management
- 9.2 Request Model und Standard Requests
- 9.4 Erfüllung, Automatisierung und Self-Service
- 9.5 Zusammenspiel mit Incident, Change, Knowledge und Service Level Management
- Information Security Management
- Service Level Management
- Knowledge Management

Quellen und Versionsstand

Offizielle Grundlagen

- PeopleCert – ITIL Practice Guide: Service Request Management
- PeopleCert – ITIL Practice Guide: Information Security Management
- ITIL Foundation – Version 5

Einordnung

Die dargestellten Genehmigungsprozesse, Beispiele und Rollen sind herstellerneutrale Praxisempfehlungen. ITIL schreibt keine festen Genehmigungsstufen oder Freigabeworkflows vor. Organisationen definieren diese anhand ihrer Sicherheitsrichtlinien, Compliance-Anforderungen und Geschäftsprozesse.

Behandelter Framework-Stand: ITIL Version 5
Zusätzlich berücksichtigt: aktuelle ITIL-4-Practice-Guidance
Fachlicher Stand: August 2026
