AsDiCore Validitas

User Manual 1.0

Operational Validity & Exception Management

Version	1.0
Produkt	AsDiCore Validitas
Zielgruppe	Owner, Security, Compliance, Architektur, PMO, Entscheider, Administratoren
Status	Erstfassung für Validitas 1.0
Herausgeber	AsDiTech

Inhaltsverzeichnis

1. Überblick

AsDiCore Validitas unterstützt Organisationen dabei, operative Gültigkeit nachvollziehbar zu führen. Im Mittelpunkt stehen Zustände, die im Betrieb häufig über Excel, Jira, Confluence, PDF-Ablagen oder E-Mail-Verläufe verteilt sind.

Validitas führt unter anderem:

- Zertifikate und andere gültigkeitskritische Objekte
- Ausnahmen und Sonderregelungen
- Risikoakzeptanzen
- Kommunikationsfreigaben
- Reviews und Wiedervorlagen
- Evidence und Nachweise
- Owner und Verantwortlichkeiten
- Freigaben, Entscheidungen und Audit-Trail
- Berichte und Exporte

Das Ziel ist nicht nur Dokumentation, sondern ein prüfbarer Zustand: Was gilt? Wer trägt es? Bis wann gilt es? Welches Risiko wurde akzeptiert? Welche Evidence liegt vor? Wer hat entschieden?

2. Grundbegriffe

2.1 Validity Item / Vorgang

Ein Vorgang ist das zentrale Arbeitsobjekt in Validitas. Ein Vorgang beschreibt einen operativen Zustand, der geführt, geprüft oder nachgewiesen werden muss.

- ein Zertifikat
- eine Ausnahme
- eine Risikoakzeptanz
- eine Kommunikationsfreigabe
- ein technischer Sonderzustand
- ein Compliance-relevanter Nachweiszustand

Ein Vorgang enthält typischerweise Name, Beschreibung, Typ, Status, Gültigkeits- oder Ablaufdatum, Reviewdatum, Owner, Risiko- oder Compliance-Bezug, Evidence und Audit-Historie.

2.2 Owner

Ein Owner ist die Person oder Rolle, die für einen Vorgang fachlich oder technisch verantwortlich ist. Ownership bedeutet nicht nur „Name steht im Feld“, sondern Verantwortung für Aktualität, Nachweisbarkeit und Gültigkeit.

2.3 Evidence

Evidence sind Nachweise, die einen Vorgang stützen. Dazu können Dokumente, Exporte, Screenshots, Prüfprotokolle, Freigaben, Zertifikatsinformationen oder andere Belege gehören.

2.4 Review

Ein Review ist eine geplante oder notwendige Prüfung eines Vorgangs. Reviews stellen sicher, dass ein Zustand nicht nur einmal erfasst wurde, sondern regelmäßig bestätigt, angepasst oder beendet wird.

2.5 Risikoakzeptanz

Eine Risikoakzeptanz beschreibt einen Zustand, bei dem ein bekanntes Risiko bewusst akzeptiert wurde. Validitas führt dabei Laufzeit, Entscheidung, Owner, Evidence und Audit-Historie.

2.6 Ausnahme / Exception

Eine Ausnahme beschreibt einen Zustand, der von einer Regel, Policy, Architekturvorgabe, Sicherheitsanforderung oder betrieblichen Norm abweicht. Ausnahmen müssen begründet, befristet, entschieden und nachvollziehbar geführt werden.

2.7 Segregation of Duties / SoD

Segregation of Duties bedeutet Funktionstrennung: Arbeitsfähig ja. Selbstfreigabe nein.

3. Anmeldung

Die Anwendung wird über die bereitgestellte URL geöffnet, zum Beispiel https://validitas.asditech.de.

1. Öffnen Sie die Validitas-URL im Browser.
2. Geben Sie Benutzername oder E-Mail-Adresse ein.
3. Geben Sie Ihr Passwort ein.
4. Klicken Sie auf Anmelden.

Melden Sie sich nach der Arbeit über das Benutzer-/Profilmenü ab, insbesondere auf gemeinsam genutzten Geräten.

4. Dashboard

Das Dashboard gibt einen Überblick über die wichtigsten operativen Zustände.

- bald ablaufende Vorgänge
- überfällige Reviews
- offene Freigaben
- blockierte oder warnende Gate-Zustände
- fehlende Evidence
- hohe Restrisiken
- Reminder- und Benachrichtigungsstatus
- aktuelle Aktivitäten

Verwenden Sie das Dashboard als Einstiegspunkt: Prüfen Sie auffällige Kennzahlen, öffnen Sie Vorgänge mit Handlungsbedarf und bearbeiten oder eskalieren Sie offene Punkte.

5. Vorgänge / Validity Items

Die Vorgangsliste zeigt die geführten Validity Items. Je nach Rolle können Sie Vorgänge ansehen, filtern, erstellen, bearbeiten oder exportieren.

Typische Spalten sind Name, Typ, Status, Owner, Ablaufdatum, Reviewdatum, Risiko, Evidence-Status und Aktionen.

Nutzen Sie Suche, Filter, Sortierung und Paging, um relevante Vorgänge zu finden.

In der Detailansicht sehen Sie Stammdaten, Verantwortlichkeiten, Fristen, Risiko- und Compliance-Informationen, Evidence, Reviews, Entscheidungen und Audit-Historie.

6. Vorgang anlegen

5. Öffnen Sie die Vorgangsübersicht.
6. Klicken Sie auf Neu, Anlegen oder die entsprechende Aktion.

7. Erfassen Sie die erforderlichen Angaben.
8. Speichern Sie den Vorgang.

Typische Pflichtfelder sind Name, Typ, Beschreibung, Owner, Ablauf- oder Gültigkeitsdatum, Reviewdatum und Kritikalität oder Risikoangabe.

Eine gute Beschreibung beantwortet: Worum geht es? Warum existiert der Vorgang? Welche Systeme, Prozesse oder Organisationseinheiten sind betroffen? Welche Risiken oder Abhängigkeiten bestehen?

7. Vorgang bearbeiten

Öffnen Sie den Vorgang und wählen Sie die Bearbeiten-Funktion. Je nach Rolle und Status stehen unterschiedliche Felder zur Verfügung.

Nach Änderungen speichern Sie den Vorgang. Validitas protokolliert relevante Änderungen im Audit-Trail.

Änderungen an Owner, Ablaufdatum, Reviewdatum, Risikoangaben, Status, Evidence sowie Freigabe- oder Entscheidungsinformationen sind besonders relevant.

8. Evidence / Nachweise

9. Öffnen Sie den Vorgang.
10. Wechseln Sie in den Bereich Evidence oder Nachweise.
11. Wählen Sie Datei hochladen oder die entsprechende Aktion.
12. Wählen Sie die Datei aus.
13. Ergänzen Sie Beschreibung oder Kontext, falls vorgesehen.
14. Speichern oder bestätigen Sie den Upload.

Prüfen Sie bei Evidence, ob der Nachweis fachlich passend, aktuell, lesbar, vollständig und dem richtigen Vorgang zugeordnet ist.

Ein Evidence Gap liegt vor, wenn ein Vorgang nicht ausreichend nachgewiesen ist.

9. Reviews

Reviews stellen sicher, dass ein Vorgang regelmäßig geprüft wird.

- Ist der Vorgang noch gültig?
- Ist der Owner noch korrekt?
- Sind Fristen noch angemessen?
- Ist Evidence vorhanden und aktuell?
- Hat sich das Risiko verändert?
- Muss eine Freigabe erneuert, widerrufen oder verlängert werden?

Überfällige Reviews sind ein Hinweis darauf, dass ein Zustand nicht mehr aktiv geführt wird.

10. Risiko und Risikoakzeptanzen

Risikoangaben helfen, die Kritikalität eines Vorgangs einzuschätzen.

Eine Risikoakzeptanz sollte nur verwendet werden, wenn ein Risiko bewusst getragen werden soll.

Typische Angaben sind Beschreibung des Risikos, Begründung der Akzeptanz, Laufzeit, Risk Owner, betroffene Systeme oder Prozesse, Evidence und Entscheidung.

Risikoakzeptanzen sollten nicht automatisch dauerhaft bestehen. Sie können verlängert, beendet oder widerrufen werden.

11. Ausnahmen und Freigaben

Eine Ausnahme beschreibt eine bewusste Abweichung von einer Vorgabe, Policy oder Regel.

Typische Angaben sind Beschreibung, Grund, betroffene Systeme, Laufzeit, Owner, Risiko, Evidence und benötigte Freigabe.

Je nach Vorgang und Berechtigung kann eine Ausnahme eingereicht, geprüft, genehmigt, abgelehnt, verlängert oder widerrufen werden.

Eine Person, die eine Ausnahme beantragt, sollte diese nicht final selbst freigeben.

12. Kommunikationsfreigaben

Kommunikationsfreigaben können verwendet werden, wenn bestimmte technische oder organisatorische Kommunikation ausdrücklich legitimiert werden muss.

- temporäre Firewall- oder WAF-Freigaben
- Ingress- oder Routing-Ausnahmen
- Sonderkommunikation zwischen Systemen
- fachlich begründete technische Freischaltungen

Auch hier gelten klare Begründung, Owner, Laufzeit, Evidence, Risiko, Freigabe und Review.

13. Berichte und Exporte

Validitas stellt Berichte bereit, um prüfbare Zustände sichtbar zu machen.

- Compliance Gap Report
- Evidence Gap Report
- Risk Acceptance Report
- Review Overdue Report
- Approval / Exception Register

Je nach Bericht können Exporte als CSV oder PDF verfügbar sein. Nutzen Sie Exporte für Audit-Vorbereitung, Management-Reporting, Review-Termine, Compliance-Nachweise und Risiko- oder Ausnahmeübersichten.

14. Audit-Trail

Der Audit-Trail dokumentiert relevante Änderungen und Entscheidungen.

Typische Audit-Informationen sind Zeitpunkt, Benutzer, Aktion, betroffener Vorgang, alter und neuer Zustand sowie Entscheidungs- oder Änderungskontext.

Der Audit-Trail dient der Nachvollziehbarkeit und darf nicht als normale Bearbeitungsfläche verstanden werden.

15. Rollen und Berechtigungen

Validitas arbeitet mit Rollen und Berechtigungen. Je nach Rolle können Funktionen sichtbar, eingeschränkt oder gesperrt sein.

15.1 Reader / Auditor

Kann Vorgänge, Reports und Audit-Informationen einsehen, aber keine operativen Änderungen vornehmen.

15.2 Contributor
Kann Vorgänge vorbereiten, Informationen ergänzen oder Evidence hochladen.

15.3 Owner
Ist für bestimmte Vorgänge verantwortlich und kann diese pflegen, Reviews durchführen oder notwendige Informationen ergänzen.

15.4 Security / Compliance
Kann Risiken, Nachweise, Compliance-Bezüge oder Freigaben prüfen und bewerten.

15.5 Decision Maker / Approver
Kann Entscheidungen treffen, Freigaben erteilen oder ablehnen, sofern keine SoD-Regel verletzt wird.

15.6 TenantAdmin
Verwaltet Benutzer, Rollen und Organisationseinstellungen innerhalb des eigenen Tenants.

15.7 SystemAdmin
Verwaltet systemweite Funktionen, Tenants und administrative Grundkonfigurationen.

16. Tenant und Organisation
Validitas ist mandantenfähig. Ein Tenant repräsentiert typischerweise eine Organisation, Organisationseinheit, Umgebung oder Kundeneinheit.

Tenantbezogene Einstellungen können Name, Anzeigeinformationen, Benutzer und Rollen, SMTP-/Benachrichtigungseinstellungen, Logo oder Branding und organisatorische Einstellungen enthalten.

Normale Benutzer sehen nur die Daten, für die sie innerhalb ihres Tenants berechtigt sind.

17. Benachrichtigungen
Validitas kann Benachrichtigungen erzeugen, zum Beispiel für bald ablaufende Vorgänge, überfällige Reviews, offene Freigaben, fehlende Evidence sowie kritische Risiko- oder Ausnahmezustände.

Benachrichtigungen ersetzen nicht die fachliche Verantwortung. Sie unterstützen dabei, Zustände rechtzeitig zu prüfen.

18. Gute Arbeitsweise mit Validitas

18.1 Vorgänge nicht nur anlegen, sondern führen
Ein Vorgang ist erst dann wertvoll, wenn er aktiv gepflegt wird: Owner aktuell halten, Reviewdaten ernst nehmen, Evidence ergänzen, Risikoänderungen erfassen und Entscheidungen nachvollziehbar treffen.

18.2 Keine Dauer-Ausnahmen ohne Review
Ausnahmen sollten befristet sein. Wenn eine Ausnahme dauerhaft benötigt wird, sollte geprüft werden, ob die zugrunde liegende Regel, Architektur oder Betriebsrealität angepasst werden muss.

18.3 Evidence nicht irgendwo ablegen
Nachweise gehören an den Vorgang. Sonst entsteht wieder genau die Verteilung, die Validitas vermeiden soll.

18.4 Verantwortung sichtbar halten

Ein gültiger Zustand ohne klaren Owner ist organisatorisch schwach. Validitas soll sichtbar machen, wer einen Zustand heute trägt.

19. Häufige Situationen

19.1 Ein Zertifikat läuft bald ab

15. Dashboard prüfen.
16. Vorgang öffnen.
17. Owner und Ablaufdatum prüfen.
18. Evidence und Reviewstatus prüfen.
19. Erneuerung oder Entscheidung dokumentieren.
20. Reviewdatum aktualisieren.

19.2 Eine Ausnahme soll verlängert werden

21. Ausnahme öffnen.
22. Begründung prüfen.
23. Risiko und Evidence prüfen.
24. Neue Laufzeit begründen.
25. Freigabe einholen.

19.3 Evidence fehlt

26. Vorgang öffnen.
27. Evidence-Bereich prüfen.
28. Passenden Nachweis hochladen.
29. Beschreibung ergänzen.

19.4 Risikoakzeptanz läuft ab

30. Risikoakzeptanz öffnen.
31. Risiko erneut bewerten.
32. Maßnahmen und Evidence prüfen.
33. Entscheiden: beenden, verlängern oder widerrufen.

20. Fehler und Hinweise

20.1 Funktion nicht sichtbar

Wenn eine Funktion nicht sichtbar ist, kann dies an Berechtigungen, Rolle, Tenant-Kontext oder Status des Vorgangs liegen.

20.2 Speichern nicht möglich

- Pflichtfelder vollständig?
- Datumsfelder korrekt?
- Berechtigung vorhanden?
- Statuswechsel zulässig?
- SoD-Regel verletzt?

20.3 Upload nicht möglich

- Dateigröße prüfen
- Dateityp prüfen

- Netzwerkverbindung prüfen
- Berechtigung prüfen

20.4 Report öffnet nicht

- Filtereinstellungen prüfen
- Berechtigung prüfen
- Browser-Popup- oder Download-Einstellungen prüfen
- Prüfen, ob Daten für den Bericht vorhanden sind

21. Datenschutz und Sicherheit im Umgang mit Validitas

Nutzen Sie Validitas nicht zur Ablage unnötiger personenbezogener Daten. Evidence sollte nur Informationen enthalten, die für den Vorgang erforderlich sind.

Vermeiden Sie insbesondere Passwörter, API-Schlüssel, private Schlüssel, unnötige personenbezogene Informationen und vertrauliche Informationen ohne fachliche Notwendigkeit.

Falls Nachweise sensible Informationen enthalten, achten Sie auf Berechtigung, Zweckbindung und organisatorische Vorgaben.

22. Zusammenfassung

AsDiCore Validitas hilft dabei, operative Gültigkeit aktiv zu führen.

- Vorgänge sichtbar machen
- Owner zuordnen
- Fristen und Reviews führen
- Evidence am Zustand halten
- Risiken und Ausnahmen nachvollziehbar entscheiden
- Reports und Audit für Prüfung und Steuerung nutzen

Dokumentation zeigt, dass etwas beschrieben wurde. Validitas zeigt, ob es noch gilt.