Application Architecture SAP BTP

Status	Approved
Owner	KUMAR-ext, Anit
Stakeholders	
LeanIX Link	SAP BTP factsheet

Introduction

SyWay adopts SAP Business Technology Platform (BTP) as the foundation to integrate, extend, and operate the programme's SAP landscape. This document establishes a concise, region-agnostic application-architecture baseline that explains how the in-scope BTP services are organised into accounts and subaccounts, aligned to environments, and governed by platform-level guardrails for connectivity, security, operations, and lifecycle management. It is intended for Technical Architects and Operations.

Purpose

The purpose of this document is to provide a single, self-contained design baseline for SyWay's BTP application architecture. It defines the target tenancy and placement model, high-level connectivity patterns, the operational monitoring posture, and essential platform conventions such as naming and tagging. The document sets reusable guardrails to drive consistent design and operations, while intentionally excluding product-level configuration and detailed control frameworks handled elsewhere.

Scope & Objectives

This document applies to the following BTP services: **SAP Integration Suite, Forms Service by Adobe, SAP Build Work Zone, SAP Task Center, SAP Build Process Automation, SAP Build Code, SAP Business Application Studio (BAS), SAP Cloud Transport Management, ActiveControl – UI, Cloud Identity (IAS and IPS), SAP Secure Login Service for SAP GUI, Identity Access Governance (IAG), SAP Datasphere, SAP Profitability and Performance Management Cloud (PaPM Cloud), Sustainability Footprint Management (SFM), Sustainability Control Tower, Green Ledger, Asset Performance Management, Group Reporting Data Collection, Advanced Financial Closing, SAP Risk and Assurance Management, SAP Business Network Global Track & Trace (GTT) and Document Reporting Compliance (DRC).** Within scope are the account/subaccount model and environment alignment, high-level connectivity and communication-security patterns, the monitoring/observability approach, and platform naming/tagging conventions required for SyWay—kept region-agnostic by design.

The objectives are to establish a consistent placement and operating baseline for the listed services, standardise platform connectivity and monitoring so delivery and run activities are predictable, and define concise guardrails that reduce ambiguity without duplicating service-specific detail. Out of scope are product-level configuration parameters, detailed identity/authorisation policy design, transport workflow specifics, business process design, and compliance framework mapping.

Key Decisions and Requirements

Description	Rationale
Identity & provisioning via region-specific IAS, federated to Microsoft Entra ID; IPS (connectivity plan) co-hosted with IAG	Ensures consistent SSO and policy enforcement per region while keeping sensitive provisioning under IAG governance and within plan limits.
Encrypt in transit for all channels (HTTPS/TLS for web; SNC for SAP GUI/RFC)	Provides uniform confidentiality and integrity across user and system interfaces; removes weak protocol/cipher exposure.
Standardised connectivity via SAP Cloud Connector (1× for non-prod; 2× HA for prod; **Location IDs** per connector; **virtual hosts not publicly resolvable**; secure Destinations with OAuth2/mTLS and principal propagation)	Delivers controlled, auditable access to back-ends, improves resilience for production, and avoids embedded credentials while preserving user identity end-to-end.
Tenancy segmentation: three BTP global accounts with environment-specific subaccounts per domain	Maintains regional/environment isolation, aligns with service availability, and limits blast radius for changes.
Monitoring baseline: **SAP Cloud ALM** as primary pane; **Alert Notification** and **Audit Log Service** as supporting controls	Centralises health, exceptions, and alerts while retaining product consoles for deep diagnostics; improves operational response and evidencing.
Service placement conventions: co-host **Work Zone + Task Center + BPA + Build Code + BAS** per environment; co-locate **Datasphere + PaPM Cloud** in the analytics subaccount	Reduces cross-trust and latency, simplifies content federation and identity mappings, and streamlines connectivity and operations for analytics.
Document Reporting Compliance (DRC) routing: **DEV** may connect to multiple S/4HANA back-ends; **PRD** connects to **two** production S/4HANA systems (Europe and China)	Supports multi-region compliance scenarios in production while retaining flexible integration/testing patterns in development.

Application Architecture

Overview

SyWay's SAP BTP landscape is organised into global accounts with environment-aligned subaccounts (DEV, INT, UAT, PAR, TRG, PRD), establishing clear tenancy boundaries for the in-scope services referenced in the BTP account model and enabling predictable deployment and operations without duplicating product-level detail. The design remains region-agnostic and centres on consistent placement and isolation across environments, with all services running on the SAP BTP Cloud Foundry runtime. Platform health and alerting are monitored centrally through SAP Cloud ALM, while service-specific patterns and placements are detailed in the Application Architecture Components section.

BTP Global Account & Subaccount Model

Runtime: Cloud Foundry (CF) for all subaccounts

Naming: syw-<area>-<env>-<region> (e.g., syw-itg-uat-eu20)

Environment codes: dev, int, uat, par, trg, prd

Europe — Global Account: Syensqo Main

Account ID: 59549222-81b5-4701-afde-9a23643d0b00

Regions used: EU20 (Azure Europe – Netherlands), EU10 (AWS Europe – Frankfurt)

Directory /Domain	Services	Region	Development Subaccount	Integration Test Subaccount	UAT Subaccount	Parallel Testing Subaccount	Training Subaccount	Production Subaccount
/SyWay /Shared Svcs / Integration (itg)	Integration Suite(API Management), Forms Service by Adobe, SAP Process Integration Runtime	EU20	syw-itg-dev-eu20	—	syw-itg-uat-eu20	—	—	syw-itg-prd-eu20
/SyWay /Shared Svcs / User Interface (ui)	SAP Build Work Zone, SAP Task Center, SAP Build Process Automation , SAP Build Code, BAS	EU20	syw-ui-dev-eu20	syw-ui-int-eu20	syw-ui-uat-eu20	syw-ui-par-eu20	syw-ui-trg-eu20	syw-ui-prd-eu20
/SyWay /Shared Svcs / Deployment Mgmt (dep)	SAP Cloud Transport Management, ActiveControl -UI	EU20	syw-dep-dev-eu20	—	—	—	—	syw-dep-prd-eu20

/SyWay /Shared Svcs / Identity Mgmt (sec)	Cloud Identity (IAS and IPS), SAP Secure Login Service for SAP GUI	EU20	syw-sec-dev-eu20	—	syw-sec-uat-eu20	—	—	syw-sec-prd-eu20
/SyWay /Shared Svcs / IAG (iag)	Identity Access Governance (IAG)	EU10	syw-iag-dev-eu10	—	syw-iag-uat-eu10	—	—	syw-iag-prd-eu10
/SyWay /Analytics (ana)	Datasphere, PaPM Cloud	EU20	syw-ana-dev-eu20	—	syw-ana-uat-eu20	—	—	syw-ana-prd-eu20
/SyWay /Sustainability (sus)	Sustainability Footprint Management (SFM), Sustainability Control Tower, Green Ledger	EU20	syw-sus-dev-eu20	—	syw-sus-uat-eu20	—	—	syw-sus-prd-eu20
/SyWay/Asset Performance Mgmt (apm)	Asset Performance Management	EU20	syw-apm-dev-eu20	syw-apm-int-eu20	syw-apm-uat-eu20	—	—	syw-apm-prd-eu20
/SyWay /Finance (fin)	Group Reporting Data Collection, Advanced Financial Closing, SAP Risk and Assurance Management	EU10	syw-fin-dev-eu10	—	syw-fin-uat-eu10	—	—	syw-fin-prd-eu10
/SyWay /Logistics (gtt)	SAP Business Network Global Track and Trace(GTT), Audit Log Viewer, Personal Data Manager, Authorization Apps for Freight Collaboration,Carrier Apps for Freight Collaboration	EU10	syw-gtt-dev-eu10	—	—	—	—	syw-gtt-prd-eu10
/SyWay /Document Reporting Compliance (drc)	Document Reporting Compliance	EU10	syw-drc-dev-eu10	—	—	—	—	syw-drc-prd-eu10

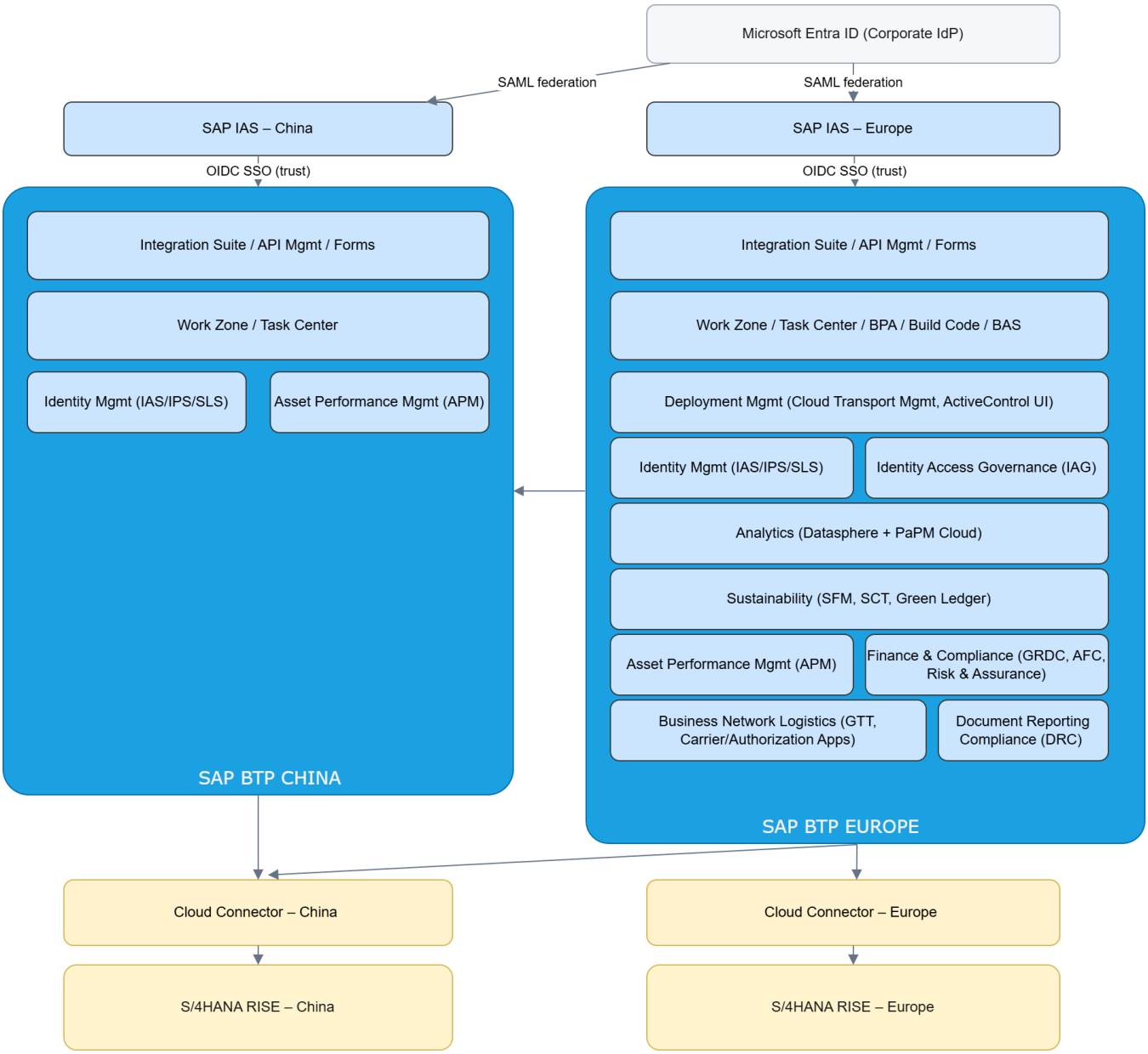
China — Global Account: Syensqo China

Account ID: (To be provisioned)

Region used: CN20 (Azure China North 3 – Hebei)

Directory/Domain	Services	Region	Integration Test Subaccount	UAT Subaccount	Parallel Testing Subaccount	Training Subaccount	Production Subaccount
/SyWay/Shared Svcs / Integration (itg)	Integration Suite, API Management, Forms Service by Adobe	CN20	—	syw-itg-uat-cn20	—	—	syw-itg-prd-cn20
/SyWay/Shared Svcs / User Interface (ui)	SAP Build Work Zone, SAP Task Center	CN20	syw-ui-int-cn20	syw-ui-uat-cn20	syw-ui-par-cn20	syw-ui-trg-cn20	syw-ui-prd-cn20
/SyWay/Shared Svcs / Identity Mgmt (sec)	Cloud Identity (IAS and IPS), SAP Secure Login Service for SAP GUI	CN20	—	syw-sec-uat-cn20	—	—	syw-sec-prd-cn20
/SyWay/Asset Performance Mgmt (apm)	Asset Performance Management	CN20	syw-apm-int-cn20	syw-apm-uat-cn20	—	—	syw-apm-prd-cn20

Application Architecture Components



Component	Purpose	Dependencies / Back-Ends
Integration Suite (incl. API Mgmt, Forms)	Enterprise integration, API exposure, message processing; Adobe Forms runtime	SAP S/4HANA RISE (EU/CN), SAP Cloud Connector (per region), IAS (regional)
User Interface (Work Zone, Task Center, Build Process Automation, Build Code, BAS)	Launchpad/workspace, task aggregation, citizen/dev automation and IDE	IAS (OIDC), downstream BTP services via Destinations, S/4HANA via Integration or direct (case-by-case)
Deployment Mgmt (Cloud Transport Management, ActiveControl UI)	Centralized content transport orchestration; change visibility	Trusted BTP subaccounts as transport nodes
Identity Mgmt (IAS,IPS and SLS)	Authentication and (where scoped) provisioning connectivity	Microsoft Entra ID (SAML to IAS); subaccounts (OIDC to IAS); IPS connectivity plan with IAG
Identity Access Governance (IAG)	SoD, access request, risk analysis for SAP apps	IPS (connectivity plan), target systems (S /4HANA, etc.)
Analytics (Datasphere + PaPM Cloud)	Data modeling/virtualization and profitability/performance modeling	S/4HANA (via Integration/Destinations/Cloud Connector), IAS

Sustainability (SFM, SCT, Green Ledger)	Sustainability footprint mgmt, control tower, ledger	S/4HANA, IAS, relevant SAP sustainability data sources
Asset Performance Management (APM)	Asset health & performance	S/4HANA and sensor/maintenance data as applicable
Finance & Compliance (GRDC, AFC, SAP Risk & Assurance Mgmt)	Group reporting data collection, advanced close, risk & assurance	S/4HANA, IAS
Business Network Logistics (GTT, Carrier /Authorization Apps, Personal Data Manager, Audit Log Viewer)	Track & trace and logistics extensions	S/4HANA, partner endpoints, IAS
Document Reporting Compliance (DRC)	E-invoicing/e-reporting compliance	**DEV:** multi-backend to non-prod S/4HANA • **PRD:** two region to EU/CN S/4HANA productions

Application Security

Authentication

SyWay standardises Single Sign-On on SAP BTP using **region-specific SAP Identity Authentication Service (IAS) tenants** federated to **Microsoft Entra ID**. Each BTP subaccount trusts its regional IAS tenant as the **default identity provider**; interactive sign-in between BTP subaccounts/services and IAS uses **OIDC**, while federation from IAS to Entra ID uses **SAML 2.0**. **Conditional Access** in Entra (including MFA and session controls) governs user access to BTP applications. Developer tooling (e.g., BAS/Build Code/CLI) follows the same **IAS Entra** flow—no separate SAP ID service identities. For service-to-service calls and Destinations, SyWay adopts standards supported by each target: **OAuth 2.0** (including client credentials), **OAuth2 SAML Bearer Assertion**, or **mutual TLS**; **Basic** authentication is permitted only where a service does not support modern methods, and such exceptions are documented. **Principal propagation** is used where supported by the back-end/service pair. **Identity provisioning** is out of scope for this section and is addressed in the programme's Identity Provisioning artefact. Detailed administrative posture and group/role design are governed by the programme's Security/IAM design artefacts.

Authorisation

Authorization on SAP BTP follows a group-based RBAC model: **IAS groups BTP role collections**, with **no direct user assignments** in subaccounts. Role collections are **scoped per subaccount and environment** to preserve separation across DEV/INT/UAT/PAR/TRG/PRD. Access to back-end systems via **Destinations** requires the appropriate **OAuth scopes/authorities** and alignment with corresponding **S/4HANA authorizations** (S/4 role design is out of scope here). **User access provisioning and role assignment** are executed using **SAP Identity Access Governance (IAG)** together with **SAP Identity Provisioning Service (IPS)**; the provisioning workflows, mappings, and controls are documented in the **Identity Access Provisioning Design** document. **Periodic access recertification** applies to BTP role collections, with cadence and evidence requirements defined in the IAM artefacts.

Communication Security

- **Transport security:** All endpoints expose **HTTPS/TLS 1.2**.
- **SAP GUI/RFC:** Access to SAP back-ends uses **SNC** via **SAP Secure Login Service (SLS)** to provide mutual authentication, encryption, and integrity.
- **Connectivity pattern:** Connectivity to RISE systems is **exclusively via SAP Cloud Connector** with minimal resource mappings and **Locatio n IDs** per connector.
- **Virtual hostnames:** Destinations use **non-resolvable virtual hosts**; these are referenced only within BTP and not exposed publicly.
- **Destination authentication:** Use **OAuth 2.0** variants (including client credentials) and **mutual TLS only where required by the target**; **Basic** authentication is permitted only when modern methods are not supported and must be documented at component level.
- **IP allow-listing:** Applied **case-by-case** where products support it.
- **Certificates & PKI:** Certificates (server, client/mTLS, SNC) are issued by the **Syensqo enterprise CA**, with **1-year validity** and centrally managed rotation; subaccount trust stores include only required issuers.
- **Regional specifics:** Additional constraints for sovereign/regulated landscapes (e.g., CN) will be documented when confirmed (**TBC**).

Data Security

- **Governance & classification:** Data security follows SyWay **programme standards** for classification, handling, and evidence. This AAD remains region-agnostic and defers identity/authorization specifics to the respective sections.
- **Regional placement & residency:** Data resides in the regions reflected by the **BTP Global Account & Subaccount Model**. Any cross-region data movement is implemented only through approved data-movement designs; **CN20** may require additional residency/egress constraints (**TBC** pending confirmation).
- **Encryption at rest:** SAP-managed BTP services use **platform-managed encryption at rest** by default. Where a service supports **customer -managed keys (CMK)**, SyWay may adopt **enterprise KMS-backed key control**; ownership and rotation follow programme key-management standards.

- **Egress control:** Outbound data flows are restricted to **allow-listed Destinations** and **explicit Cloud Connector mappings** (using non-resolvable virtual hosts). No implicit or ad-hoc egress paths are permitted from BTP services.
- **Scope boundaries:** Authentication/Authorization mechanics (e.g., scopes, role collections, principal propagation) are defined in the **Authentication** and **Authorization** sections; backup/restore and monitoring are covered in their respective sections.

Other Controls

- **Audit & evidencing:** Use **SAP BTP Audit Log Service** (with **Audit Log Viewer**) to capture and review subaccount-level security and administrative events.
- **Privacy operations:** Apply **Personal Data Manager (PDM)** where applicable to execute subject-data requests and corrective actions in supported services; record actions for operational auditability.
- **Operational notifications:** Route critical platform/service events through the **Alert Notification service for SAP BTP** to email, complementing dashboards and alerts in SAP Cloud ALM.
- **Configuration posture & drift:** Leverage **SAP Cloud ALM – Configuration & Security Analysis** to capture baseline configurations for BTP services and detect/record configuration changes for review.
- **Network access governance:** Maintain **allow-listed Destinations** and Cloud Connector mappings as the approved egress paths; apply **IP allow-listing** on exposed endpoints **case-by-case** where products support it.
- **Certificate lifecycle:** Manage server, mTLS, and SNC certificates via the **Syensqo enterprise PKI** with a **1-year validity**; curate subaccount trust stores to the minimum required issuers and track rotations centrally.

System Landscape

BTP Application	Region	DEV	INT	UAT	PAR	TRG	PROD
Build Work Zone	EU	**DEV**	INT	QAS	PAR	TRG	PRD
	CN	-	INT	QAS	PAR	TRG	PRD
Asset Performance Management	EU	DEV	INT	QAS	-	INT	PRD
	CN	-	INT	QAS	-	INT	PRD
Profitability and Performance Mgmt.	EU	**DEV**		QAS			PRD
Business Network Freight Collaboration	EU	Non-PRD					PRD
Business Network Global Track and Trace	EU	**Non-PRD**					PRD
Group Reporting Data Collection	EU	DEV	INT	QAS	PAR	INT	PRD
Document Reporting Compliance	EU	**Non-PRD**					PRD
Advanced Financial Closing	EU	Non-PRD					PRD
DataSphere	EU	**DEV**		Test			PRD
Integration Suite	EU	**DEV**	Test				PRD
	CN	-	Test				PRD
Cloud Identity (IAS, IPS), Secure Login Service (SLS)	EU	**DEV**	Test				PRD
	CN	-	Test				PRD
Identity Access Governance	EU	**DEV**	Test				PRD
Risk and Assurance Management	EU	**DEV**	Test				PRD
ActiveControl	EU	**SAP Transport Management**					
SAP Build Code	EU	**SAP Build Code**					

Operation Architecture

Transport Management

Please refer **DD-TEC-170 Transport Management for Release 4**

Application Monitoring

Service / Domain	SAP Cloud ALM – Monitor Types	In-Product Consoles (as needed)	Logs / Traces	Alerting
Integration Suite (Cloud Integration, API Management), Forms Service by Adobe, SAP Process Integration Runtime	**Integration & Exception Monitoring**, **Health Monitoring**	Message Monitoring (Cloud Integration), API Mgmt Analytics /Policy Trace, Forms runtime dashboards	SAP Cloud Logging / Application Logging for custom adapters or extensions	Cloud ALM Alerting; optional Alert Notification for cTMS /API events
Build Work Zone, Task Center	**Real User Monitoring**, **Health Monitoring**	Work Zone admin analytics; Task Center booster monitors	(If extended apps) forward to Cloud Logging	Cloud ALM Alerting
Build Process Automation (BPA)	**Job & Automation Monitoring**, **Health Monitoring**	BPA Monitor (runs, queues)	Cloud Logging (optional)	Cloud ALM Alerting
Build Code, BAS	**Health Monitoring**	Pipeline/CI logs; BAS workspace logs	Cloud Logging for pipeline outputs	Alert Notification webhooks (optional) + Cloud ALM (where integrated)
Cloud Transport Management (cTMS), ActiveControl – UI	**Health Monitoring** (cTMS)	cTMS import/export logs; ActiveControl dashboards	—	Alert Notification subscriptions for cTMS events; Cloud ALM Alerting
Cloud Identity (IAS, IPS), Secure Login Service (SLS)	**Health Monitoring**	IAS/IPS admin consoles; SLS logs	Audit Log Service (BTP) for security events	Cloud ALM Alerting
Identity Access Governance (IAG)	**Health Monitoring**	IAG dashboards (access requests, SoD)	—	Cloud ALM Alerting
Datasphere, PaPM Cloud	**Health Monitoring**	Datasphere space/job monitors; PaPM calculation monitors	—	Cloud ALM Alerting
Sustainability: SFM, Sustainability Control Tower, Green Ledger	**Health Monitoring**	Product runtime/tenant monitors	—	Cloud ALM Alerting
Asset Performance Management (APM)	**Health Monitoring**	APM analytics/diagnostics	—	Cloud ALM Alerting
Finance: GRDC, AFC, Risk & Assurance Management	**Health Monitoring**	Product consoles (submission /status, closing calendars, risk dashboards)	—	Cloud ALM Alerting
Business Network Logistics: GTT; Freight Collaboration (Authorization/Carrier Apps); Personal Data Manager; Audit Log Viewer	**Health Monitoring**	GTT/BN cockpits; PDM and Audit Log Viewer UIs	Audit Log Service (for audit events)	Cloud ALM Alerting
Document Reporting Compliance (DRC)	**Health Monitoring**	DRC submission/queue dashboards	—	Cloud ALM Alerting

System Monitoring

Service / Domain	SAP Cloud ALM – Health Monitoring (platform /service health)	BTP Platform Signals	Security / Compliance Signals	Notes
Integration Suite / API Mgmt / Forms / PIR	Tenant/service availability, adapter/runtime KPIs	BTP **Monitoring service** (app/service metrics); **Alert Notification** for service events	**Audit Log Service** (subaccount events)	Use cTMS alerts for transport-related impacts
Work Zone / Task Center	Availability and UX KPIs via CALM Health + RUM	Monitoring service for app instances	Audit Log Service	Task Center depends on same subaccount trust as Work Zone
Build Process Automation	Job/queue health, runtime status	Monitoring service (runtime), Alert Notification	Audit Log Service	Map job failures to CALM alerts
Build Code / BAS	Service health; workspace availability	Monitoring service; pipeline/webhook signals	Audit Log Service	Forward pipeline failures via Alert Notification
Cloud Transport Management, ActiveControl – UI	cTMS tenant health	Alert Notification for import/export events	Audit Log Service	ActiveControl monitored in vendor UI; optionally feed CALM via webhooks
IAS / IPS / SLS	Identity service health	—	IAS/IPS audit in product; BTP Audit Log for platform	Focus on auth failures, connector jobs
IAG	Service health	—	IAG audit in product	SoD/job status as secondary signals

Datasphere / PaPM Cloud	Tenant/space health, job statuses	Monitoring service where applicable	—	Watch connection health to S/4 /Destinations
SFM / SCT / Green Ledger	Service health	—	—	Green Ledger largely S/4—track via S/4 + CALM if applicable
APM	Service health	—	—	—
GRDC / AFC / Risk & Assurance	Service health	—	Product audit (where available)	Align with closing windows/SLAs
GTT / Freight Collaboration / PDM / Audit Log Viewer	Service health	—	**Audit Log Service** central to PDM/ALV	Ensure retention/forwarding to SIEM if required
DRC	Tenant health; submission pipeline status	Alert Notification for failures	Product audit (where available)	—

Sizing

- **Scope of sizing.** In-scope SAP BTP services are **SAP-managed SaaS**; SyWay does not perform server or infrastructure sizing. Responsibility is limited to selecting **service plans/entitlements** and defining **tenant counts per environment** in line with the account model.
- **Cloud Foundry workloads.** There are **no custom Cloud Foundry applications**; CF org/space quotas are **out of scope**.
- **Component-specific** sizing documented in Application Architecture design**.**
- **Integration Suite / API Management / PIR:** sizing is captured in the Application Architecture design.
- **Datasphere / PaPM Cloud:** sizing is captured in the Application Architecture design.
- **Build Process Automation (BPA): TBC** for peak job concurrency and queue depth (to be baselined during UAT).
- **Other services** (Work Zone, Task Center, Build Code, BAS, IAS/IPS/SLS, IAG, Finance, Sustainability, GTT, DRC): no additional sizing beyond plan/entitlement and tenant count.
- **Capacity adjustments.** When required, capacity changes are executed via **plan/entitlement adjustments** with SAP; review cadence is managed operationally outside this document.

High Availability and Disaster Recovery

All in-scope SAP BTP services are **SAP-operated SaaS**; platform high availability and disaster recovery are provided under SAP's published targets. For SAP BTP, the documented disaster-recovery objectives are **RPO 5 minutes** and **RTO 2 hours** (same-metro DR), with service execution and failover managed by SAP. Where products rely on **SAP HANA Cloud**, database recovery specifically supports a **maximum RPO of 15 minutes** via continuous log backups, with overall service recovery still governed by the platform targets. SyWay's responsibility is limited to monitoring and incident execution per runbooks; no server-level HA/DR activities are in scope for this document.

Backup/Restore

- **Platform-managed:** For SAP-managed BTP services, backups are handled by SAP; restore is service-specific and generally not customer-operated. Guidance is outlined in the BTP admin help ("Data Backups Managed by SAP").
- **SAP HANA Cloud (used by services like Datasphere/PaPM):** Continuous log backups enable **point-in-time recovery** within a configurable retention window (default 14 days; extendable up to 215 days). Restores are performed by creating a new database instance at the chosen time.
- **SAP Datasphere:** Backup/restore follows the **SAP HANA Cloud resiliency layer**; recovery is handled by SAP for disasters within SAP's control.
- **Audit evidence:** BTP **Audit Log Service** stores subaccount audit data for 90 days by default; export/forward logs if longer retention is needed.

Maintenance Plan

- **Cadence.** SAP operates **biweekly updates** (standard), **immediate updates** for critical fixes, and **major upgrades** (up to four per year).
- **What's New & release calendars.** Teams subscribe to **What's New for SAP BTP** and consult the **Consolidated Release Schedules for SAP BTP** and Intelligent Enterprise Suite: Harmonized release calendar for SAP Cloud products to track feature deliveries and maintenance windows.
- **Regional communications.** For **China (CN20)**, availability and maintenance announcements are published at **status.cn40.platform.sapcloud.cn** (subscription supported).
- **Major upgrades.** SAP provides **4 weeks' advance notice** of major upgrades; SyWay reviews impact and coordinates any required readiness actions as documented in System upgrade plan.

Exceptions

See also

File	Modified
File drawio-backup-BTP Components-rev-5 draw.io diagram backup	Feb 11, 2026 by BROWAEYS-ext, David
File BTP Components draw.io diagram	Feb 03, 2026 by KUMAR-ext, Anit
File ~BTP Components.tmp draw.io Draft	Feb 03, 2026 by KUMAR-ext, Anit
PDF File Approval from Frank.pdf Frank's Approval	Nov 12, 2025 by CHIEW-ext, Yock Sang
PDF File Stakeholder endorsement 2025-10-29.pdf Endorsement email from Francois Ruffinoni	Oct 29, 2025 by WENNINGER-ext, Sascha
File SyWay-BTP-Architecture-final.drawio	Oct 02, 2025 by KUMAR-ext, Anit

Download All

Change log

Version	Published	Changed By	Comment
CURRENT (v. 74)	**Feb 03, 2026 06:42**	**KUMAR-ext, Anit**	Remove CUI instance - CR0279
v. 73	Feb 03, 2026 06:35	**KUMAR-ext, Anit**	Removed CUI instance - CR0279
v. 72	Dec 05, 2025 10:44	**WENNINGER-ext, Sascha**	added ToC
v. 71	Oct 15, 2025 17:00	**WENNINGER-ext, Sascha**	
v. 70	Oct 04, 2025 06:19	**KUMAR-ext, Anit**	
v. 69	Oct 04, 2025 06:04	**KUMAR-ext, Anit**	
v. 68	Oct 04, 2025 05:50	**KUMAR-ext, Anit**	
v. 67	Oct 04, 2025 05:42	**KUMAR-ext, Anit**	
v. 66	Oct 02, 2025 08:36	**KUMAR-ext, Anit**	
v. 65	Oct 02, 2025 08:26	**KUMAR-ext, Anit**	

Go to Page History

Workflow history

This view shows the 5 most recent entries. The complete workflow log is available from the 'Document Activity' menu item.

Apr 07, 2026	Actor	Type	Activity	Version
Approved	WENNINGER-ext, Sascha	State	changed state to Approved at 10:20 am	v74
Edited following Approval	WENNINGER-ext, Sascha	State	gave *Minor change* approval at 10:20 am *updated as per revised CUI approach (CR0279)*	
Feb 03, 2026				
	KUMAR-ext, Anit	Edit	updated the page at 6:35 am	

	KUMAR-ext, Anit	State	changed state to Edited following Approval at 5:35 am	v73
Dec 05, 2025				
Approved	WENNINGER-ext, Sascha	Edit	updated the page at 10:44 am *added ToC*	
		State	changed state to Approved at 9:44 am	v72