



Linko

Governance & Control for SAP BTP®

SAP BTP® Technical Assessment

Prepared for	[Customer]
Global account	Lynxmind, LDA. (lynxmindlda)
Assessment date	2026-08-26 16:36 UTC
Assessment run	5ea7b6ff10c4
Health score	18 / 100 (target 100)
Report generated	2026-08-31 12:37 UTC

Contents

Key Highlights	3
Executive summary	6
Governance	8
BTP Platform History	8
Governance Analysis	
BTP Landscape	10
Prioritized Recommendations	
Usage & costs (FinOps)	11
FinOps Analysis	11
Cost by service	11
Cost by subaccount	11
Monthly cost trend	11
Prioritized Recommendations	12
Security	12
Trust configurations	13
Destinations	14
Prioritized Recommendations	
Users, roles & authorizations (IAM)	16
Users Overview	16
IAM Assessment	
Prioritized Recommendations	17
Service Inventory	19
Appendix - Services by subaccount	23

Key Highlights

18

Health score / 100

6

High & critical

4

Subaccounts

23

Users assessed

Health score: 18 / 100 (target 100, -82 vs target)

Findings: 6 high · 7 medium · 12 low

Since previous run: +0 new · 3 resolved · 13 handled · score 16→18

Data source: live BTP data (collected 2026-08-26 16:36 UTC) · coverage: destinations 4/4, trust 4/4, services 2/4 subaccounts

Findings by severity



■ high - 6
■ medium - 7
■ low - 12

Findings by subaccount

Lynx-Joule-for-Business		7
Lynx-Joule-Studio		6
Lynxmind AI		5
Lynx-AVR		4
global		3

How the health score is calculated

Each domain starts at **100**. Every active finding (state Open or In progress) deducts points by severity: **critical –15, high –8, medium –4, low –1**, info 0, giving a domain score of **max(0, 100 – its deductions)**. The overall health score is the **average of the domain scores** (so it stays consistent with them). Resolved and risk-accepted findings are excluded. A domain with no collected data shows no data and is left out of the average, so missing coverage never reads as healthy.

Domain scores

Governance		33/100
Usage & costs (FinOps)		0/100
Security		39/100
Users, roles & authorizations (IAM)		0/100

Confirmed good practices

- ✓ Random (non-guessable) subdomains in: Lynx-AVR, Lynxmind AI.
- ✓ Description maintained in: Lynxmind AI.
- ✓ Audit log active in: Lynx-AVR, Lynx-Joule-for-Business, Lynxmind AI, Lynx-Joule-Studio.
- ✓ No NEO subaccounts (no exposure to the 2028 end-of-life).
- ✓ All subaccounts hosted in European regions (data residency and GDPR by design).

Findings overview

Check	Severity	State	Subaccount
SEC-004 - Default Identity Provider active	high	open	Lynx-AVR
IAM-002 - Too many high-privilege users	high	open	Lynx-Joule-Studio
SEC-004 - Default Identity Provider active	high	in progress	Lynx-Joule-Studio
SEC-004 - Default Identity Provider active	high	in progress	Lynx-Joule-for-Business
IAM-002 - Too many high-privilege users	high	in progress	Lynxmind AI
SEC-001 - Destinations using BasicAuthentication	high	resolved	Lynxmind AI
SEC-004 - Default Identity Provider active	high	in progress	Lynxmind AI
FIN-002 - Single service dominates monthly consumption	medium	open	global
GOV-006 - Flat account structure (no directory organization)	medium	in progress	global
SEC-011 - Users with email domains outside the whitelist	medium	resolved	Lynx-AVR
GOV-002 - Subdomain exposes company name	medium	risk accepted	Lynx-Joule-Studio
IAM-001 - Ghost users (never logged in)	medium	risk accepted	Lynx-Joule-Studio
SEC-003 - Destinations without authentication	medium	open	Lynx-Joule-Studio
SEC-011 - Users with email domains outside the whitelist	medium	resolved	Lynx-Joule-Studio
GOV-002 - Subdomain exposes company name	medium	open	Lynx-Joule-for-Business
IAM-001 - Ghost users (never logged in)	medium	in progress	Lynx-Joule-for-Business
SEC-003 - Destinations without authentication	medium	open	Lynx-Joule-for-Business
SEC-011 - Users with email domains outside the whitelist	medium	resolved	Lynx-Joule-for-Business
IAM-001 - Ghost users (never logged in)	medium	open	Lynxmind AI
SEC-011 - Users with email domains outside the whitelist	medium	resolved	Lynxmind AI
GOV-010 - BTP pillar without an assigned platform owner	low	open	global
GOV-001 - Subaccount without description	low	open	Lynx-AVR
GOV-003 - Subaccount without labels	low	open	Lynx-AVR
SEC-009 - Role collections with no members	low	open	Lynx-AVR
GOV-001 - Subaccount without description	low	open	Lynx-Joule-Studio

Executive summary

The SAP BTP landscape is functional but shows several maturity gaps in governance, security, IAM, and cost management. The account structure is flat, with all four subaccounts placed directly under the global account while four existing directories remain unused. This limits clarity for delegation, policy application, and lifecycle governance as the landscape grows. Ownership metadata is also incomplete: no platform owners are defined for the main BTP pillars, several subaccounts lack descriptions, and none of the four subaccounts have labels.

The most significant risk area is security and identity configuration. The default SAP Identity Provider trust configuration, `sap.default`, remains active in all four assessed subaccounts and is classified as high severity in each case. In addition, two public subdomains include the company-identifying token `lynx`, making them more guessable, and several destinations are configured without authentication, including `n8n-mcp` in both Lynx-Joule-Studio and Lynx-Joule-for-Business. These items should be treated as immediate remediation priorities because they affect externally visible naming hygiene and access trust boundaries.

IAM findings indicate privilege concentration and account hygiene issues. Lynx-Joule-Studio and Lynxmind AI each have six administrators, exceeding the configured threshold of five, while three applications have users with no recorded login. Role collection cleanup is also needed, particularly in subaccounts with a high proportion of empty role collections. Together, these findings point to the need for tighter periodic access reviews, reduction of unnecessary administrator assignments, and removal or documentation of unused access artifacts.

FinOps exposure is concentrated rather than distributed: Cloud Foundry Runtime represents 759, or 99% of monthly consumption. This makes it the primary lever for cost validation, forecasting, and optimization. The recommended focus is therefore to first remediate identity provider and unauthenticated destination risks, then strengthen governance foundations through directories, ownership, descriptions, and labels, while implementing recurring IAM and Cloud Foundry Runtime consumption reviews to keep the environment controlled over time.

High priority actions

Severity	Check	Subaccount	Recommended action
high	IAM-002 - Too many high-privilege users	Lynxmind AI	Apply least privilege: reduce administrators and use custom viewer/operator roles.
high	IAM-002 - Too many high-privilege users	Lynx-Joule-Studio	Apply least privilege: reduce administrators and use custom viewer/operator roles.
high	SEC-004 - Default Identity Provider active	Lynx-AVR	Disable the Default IdP and use the corporate IdP (IAS) - prevents user creation outside corporate control.
high	SEC-004 - Default Identity Provider active	Lynx-Joule-for-Business	Disable the Default IdP and use the corporate IdP (IAS) - prevents user

Severity	Check	Subaccount	Recommended action
			creation outside corporate control.
high	SEC-004 - Default Identity Provider active	Lynxmind AI	Disable the Default IdP and use the corporate IdP (IAS) - prevents user creation outside corporate control.
high	SEC-004 - Default Identity Provider active	Lynx-Joule-Studio	Disable the Default IdP and use the corporate IdP (IAS) - prevents user creation outside corporate control.

Medium priority actions

Severity	Check	Subaccount	Recommended action
medium	FIN-002 - Single service dominates monthly consumption	global	Validate the service sizing; consider hibernation (Automation Pilot/Terraform) and dedicated budget alerts.
medium	GOV-002 - Subdomain exposes company name	Lynx-Joule-for-Business	Subdomains cannot be renamed: migrate the subaccount to a new one with a random subdomain (convention <code>env + nn + random8</code>).
medium	GOV-006 - Flat account structure (no directory organization)	global	Organize subaccounts into directories by line of business or landscape to group settings, delegate administration, and enable per-area FinOps.
medium	IAM-001 - Ghost users (never logged in)	Lynx-Joule-for-Business	Identify and remove shadow users/developers to reduce the attack surface.
medium	IAM-001 - Ghost users (never logged in)	Lynxmind AI	Identify and remove shadow users/developers to reduce the attack surface.
medium	SEC-003 - Destinations without authentication	Lynx-Joule-for-Business	Review whether the target is genuinely public; otherwise configure an appropriate authentication type.
medium	SEC-003 - Destinations without authentication	Lynx-Joule-Studio	Review whether the target is genuinely public; otherwise

Severity	Check	Subaccount	Recommended action
			configure an appropriate authentication type.

Governance - 33/100

BTP Platform Ownership

SAP BUSINESS TECHNOLOGY PLATFORM

App Development
Build and extend business apps with low-code and pro-code tools.
No owner assigned

Automation
Automate workflows and tasks with low-code tools and RPA.
No owner assigned

Integration
Connect apps, data and processes across cloud and on-premise.
No owner assigned

Data & Analytics
Manage, model and analyze data for planning and insight.
No owner assigned

AI
Embed pretrained and generative AI responsibly into business processes.
No owner assigned

Governance & Operations
Foundational, cross-cutting across every pillar

No owner assigned

BTP Platform History

Subaccounts grouped by creation year, oldest to newest.

4
TOTAL SUBACCOUNTS

1
PROD

2025
1 subaccount

Lynxmind AI
11/12/2025 **PROD**

2026
3 subaccounts

Lynx-Joule-for-Business
29/05/2026

Lynx-Joule-Studio
29/05/2026

Lynx-AVR
21/08/2026

Governance

The account hierarchy is currently not using the available directory model: all 4 subaccounts are placed directly under the global account, while 4 directories exist but contain no subaccounts. This indicates a flat structure despite an apparent intent to organize the landscape through directories, which can make delegation, policy application, and lifecycle governance less clear at scale.

Two subaccounts expose the company token in their public subdomain:
lynx-joule-studio-1cmlz4c3 for **Lynx-Joule-Studio** and lynx-joule-for-business-t0s4mkhs for **Lynx-**

Stage 6 costs (Policies - 01/08)

Energy costs

The Energy Budget shows a high concentration of monthly consumption in one service (Heat). Monthly Budgets accounts for 70% representing 60% of the monthly total. The fact that the cost apportionment affects almost entirely Heat as Heat Monthly Budgets is a change in the service would have the biggest potential impact on the overall monthly consumption profile.

The consumption per major service can be distributed across services. Heat is **single service consumes 60% of monthly consumption**. Heat is being apportioned proportionally. The other Heat Monthly Budgets for the service is monthly, electrical and storage through regular consumption costs.

Heat by service

Heat Monthly Budget	700000	700000
Other Heat Monthly Budgets	0	0
Total	700000	700000
Heat Monthly Budget		700000
Other Heat Monthly Budgets		0
Total		700000

Heat by sub-service

Heat	700000	700000
Other Heat	0	0
Total	700000	700000
Heat	Heat	700000
Other Heat	Other Heat	0

Production is not production, production is not production, production is not production.

Monthly cost report

Heat	700000	700000
Other Heat	0	0
Heat	700000	700000
Other Heat	0	0
Heat	700000	700000
Other Heat	0	0
Heat	700000	700000
Other Heat	0	0

NAME	TYPE	VAL	ADDRESS	STATUS
Device 00				Not connected
Device 01				Connected
Device 02				Connected
Device 03				Connected
Device 04				Connected
Device 05				Connected
Device 06				Connected
Device 07				Connected
Device 08				Connected
Device 09				Connected
Device 10				Connected

API endpoints

Endpoints:

Endpoint	Type	Method	Endpoint	Method	Endpoint
/api/v1	GET	GET	/api/v1	POST	/api/v1
/api/v1	GET	GET	/api/v1	POST	/api/v1
/api/v1	GET	GET	/api/v1	POST	/api/v1
/api/v1	GET	GET	/api/v1	POST	/api/v1
/api/v1	GET	GET	/api/v1	POST	/api/v1

Product information

1. Implement a directory-based account structure

When implementing the directory-based account structure, the directory-based account structure should be implemented using the directory-based account structure and the directory-based account structure.

2. Implement a directory-based account structure

When implementing the directory-based account structure, the directory-based account structure should be implemented using the directory-based account structure and the directory-based account structure.

3. Implement a directory-based account structure

When implementing the directory-based account structure, the directory-based account structure should be implemented using the directory-based account structure and the directory-based account structure.

4. Implement a directory-based account structure

When implementing the directory-based account structure, the directory-based account structure should be implemented using the directory-based account structure and the directory-based account structure.

5. Implement a directory-based account structure

When implementing the directory-based account structure, the directory-based account structure should be implemented using the directory-based account structure and the directory-based account structure.

Appendix: Services by subsector

Below services already mentioned in subsector chapters, this page lists the remaining. The table is a replacement for month journals, after the end of meeting. Below table must be added in page 100 in the current subchapter for the relevant page.

Service	Code	Fee	Subsector	Subsector
Service 1	Code 1	Fee 1	Subsector 1	Subsector 1
Service 2	Code 2	Fee 2	Subsector 2	Subsector 2
Service 3	Code 3	Fee 3	Subsector 3	Subsector 3
Service 4	Code 4	Fee 4	Subsector 4	Subsector 4
Service 5	Code 5	Fee 5	Subsector 5	Subsector 5
Service 6	Code 6	Fee 6	Subsector 6	Subsector 6
Service 7	Code 7	Fee 7	Subsector 7	Subsector 7
Service 8	Code 8	Fee 8	Subsector 8	Subsector 8
Service 9	Code 9	Fee 9	Subsector 9	Subsector 9
Service 10	Code 10	Fee 10	Subsector 10	Subsector 10
Service 11	Code 11	Fee 11	Subsector 11	Subsector 11
Service 12	Code 12	Fee 12	Subsector 12	Subsector 12
Service 13	Code 13	Fee 13	Subsector 13	Subsector 13
Service 14	Code 14	Fee 14	Subsector 14	Subsector 14
Service 15	Code 15	Fee 15	Subsector 15	Subsector 15
Service 16	Code 16	Fee 16	Subsector 16	Subsector 16
Service 17	Code 17	Fee 17	Subsector 17	Subsector 17
Service 18	Code 18	Fee 18	Subsector 18	Subsector 18
Service 19	Code 19	Fee 19	Subsector 19	Subsector 19
Service 20	Code 20	Fee 20	Subsector 20	Subsector 20
Service 21	Code 21	Fee 21	Subsector 21	Subsector 21
Service 22	Code 22	Fee 22	Subsector 22	Subsector 22
Service 23	Code 23	Fee 23	Subsector 23	Subsector 23
Service 24	Code 24	Fee 24	Subsector 24	Subsector 24
Service 25	Code 25	Fee 25	Subsector 25	Subsector 25
Service 26	Code 26	Fee 26	Subsector 26	Subsector 26
Service 27	Code 27	Fee 27	Subsector 27	Subsector 27
Service 28	Code 28	Fee 28	Subsector 28	Subsector 28
Service 29	Code 29	Fee 29	Subsector 29	Subsector 29
Service 30	Code 30	Fee 30	Subsector 30	Subsector 30

Item	Reference	Reference
100-100	100-100-100	100-100
100-100	100-100-100	100-100
100-100-100	100-100-100	100-100
100-100-100	100-100-100	100-100
100-100-100-100	100-100-100	100-100-100
100-100-100-100-100	100-100-100	100-100-100

Provision Recommendations

1. **Monthly** – Detailed review of Cloud Foundry Runtime consumption.
 Review Cloud Foundry Runtime consumption 100% or 90% of the monthly total. It should be the primary input to cost analysis and optimization.
2. **Monthly** – Review Cloud Foundry Runtime usage along with actual workload requirements.
 The finding about the use of services determines monthly consumption. It confirms that the level of runtime consumption in public should be reduced to a priority.
3. **Monthly** – Review monitoring for Cloud Foundry Runtime consumption trends.
 Review Cloud Foundry Runtime accounts for 90% of monthly consumption. Improving monitoring will help detect runtime changes in the cloud and public use.
4. **Use Cloud Foundry Runtime as the main input for finding forecasting and budgeting.**
 a. 10% of the monthly consumption is attributed to Cloud Foundry Runtime budget planning should focus primarily on this service.

Item	Value	Unit	Category	Value
Cloud Foundry Runtime	100%	100%	Cloud Foundry Runtime	100%
Cloud Foundry Runtime	100%	100%	Cloud Foundry Runtime	100%
Cloud Foundry Runtime	100%	100%	Cloud Foundry Runtime	100%
Cloud Foundry Runtime	100%	100%	Cloud Foundry Runtime	100%

Security – 100%

Security

The primary security concern is the reported high security finding that the public web security finding is not a priority. The main configuration, `SECURITY`, is not in a high security state. The finding is reported as high in the public web security finding. The finding is reported as high in the public web security finding. The finding is reported as high in the public web security finding.

The primary security concern is the reported high security finding that the public web security finding is not a priority. The main configuration, `SECURITY`, is not in a high security state. The finding is reported as high in the public web security finding. The finding is reported as high in the public web security finding.

The primary security concern is the reported high security finding that the public web security finding is not a priority. The main configuration, `SECURITY`, is not in a high security state. The finding is reported as high in the public web security finding. The finding is reported as high in the public web security finding.

Provision Recommendations

1. **Review or Update the public web security finding.**

