AWS SAP COMPETENCY CAMPAIGN 2

SAP Modernisation Masterclass

S/4HANA Readiness, Performance Optimisation and Cost Reduction on AWS

Campaign	SAP Competency Campaign 2
Prepared by	Cloudwrxs
Published	July 1, 2026
Region focus	KSA and MENA

Cloudwrxs perspective: SAP modernisation should be treated as an architecture, operating-model and business-readiness programme, not simply a hosting decision. The goal is a safer, more measurable SAP platform that is ready for S/4HANA, resilient operations, cost control and future data and AI use cases.

Contents

Published: July 1, 2026 **Campaign:** SAP Competency Campaign 2 **Prepared by:** Cloudwrxs

---

Executive Summary

SAP landscapes are often treated as static platforms: important, expensive, heavily customised, and too risky to change quickly. That mindset is understandable, but it creates a dangerous gap. Business teams expect SAP to support faster reporting, resilient operations, digital services, AI, analytics, and new regulatory demands. At the same time, many SAP estates still depend on fixed infrastructure, manual recovery processes, ageing backup designs, oversized non-production environments, and specialist knowledge held by a small number of people.

This whitepaper is written for KSA and MENA organisations that are evaluating SAP modernisation, S/4HANA readiness, or SAP workload optimisation on AWS. It does not assume that every SAP estate should move immediately or that migration alone solves the problem. Instead, it lays out a practical assessment model: understand the current landscape, quantify the gaps, design the future operating model, and prioritise actions that reduce business risk while building a credible path to transformation.

The central argument is simple: SAP modernisation is not a single migration event. It is an architecture, operations, security, cost and business-readiness programme. AWS provides the platform options - certified compute, resilient infrastructure patterns, automation, backup and DR services, observability, and flexible consumption models - but the value only appears when those services are mapped to the real SAP workload, the real business processes, and the real operating constraints of the organisation.

Cloudwrxs approaches SAP modernisation through four connected lenses:

1. **Readiness:** Is the current SAP estate ready for S/4HANA, growth, regulatory scrutiny, and digital integration?
2. **Risk:** Where are the operational, security, availability, and disaster recovery gaps that could interrupt the business?
3. **Economics:** Which parts of the SAP cost base are structural, and which are caused by overprovisioning, manual operations, inefficient scheduling, or unclear ownership?
4. **Execution:** What can be improved now, what should be migrated, what should wait, and what evidence does leadership need to approve the roadmap?

1. Why SAP Modernisation Matters Now

SAP sits at the centre of finance, manufacturing, supply chain, procurement, HR, compliance, reporting, and operational control. When SAP performs well, the business often notices only indirectly: finance closes faster, inventory records stay accurate, production planning runs on time, purchasing approvals move through the system, and executives trust the reports. When SAP performs poorly, the impact is immediate and visible. Batch windows stretch into business hours. Month-end close becomes a weekend event. Plant operations wait for confirmations. Reporting teams build workarounds. Users lose confidence.

Modernisation matters because the pressure on SAP is increasing from several directions:

- **S/4HANA readiness:** Organisations need to understand whether their current infrastructure, integrations, data volumes, custom code and operating model can support the next transformation stage.
- **Business continuity:** SAP downtime can stop finance, production, fulfilment, billing, procurement and reporting. Recovery plans that exist only as documents are not enough.
- **Security and compliance:** SAP contains highly sensitive business data. Identity, network design, encryption, logging and change control must be treated as core architecture concerns.
- **Cost scrutiny:** SAP hosting cost is often accepted as unavoidable. In reality, there is usually waste in non-production estates, storage growth, backup retention, oversized instances, manual processes and renewal assumptions.
- **Operational resilience:** Basis and infrastructure teams are being asked to support more change with fewer manual windows. Automation, monitoring and repeatable runbooks are now essential.

- **Innovation:** SAP data increasingly needs to connect with analytics, AI, automation, organisation portals, supplier platforms and real-time business intelligence.

The right question is not "Should SAP move to AWS?" The better question is "What architecture and operating model will make SAP safer, faster, more economical, and easier to evolve?"

2. What Good Looks Like for SAP on AWS

AWS and SAP have worked together to certify infrastructure options for SAP workloads, including SAP HANA. That certification matters because SAP performance and supportability are not generic compute questions. Memory ratios, CPU performance, storage throughput, network behaviour, operating system support, database architecture and failure handling all affect whether the system is fit for production.

A strong SAP-on-AWS design normally includes:

- **Certified instance selection:** Production HANA workloads should use SAP-certified EC2 options sized for memory, CPU, storage and growth. Non-production workloads can be sized differently and scheduled more aggressively.
- **Multi-AZ thinking:** Availability Zones allow resilient architecture patterns, but the design must explicitly cover application servers, ASCS/ERS, database replication, shared file systems, routing, monitoring and failover runbooks.
- **Clear RTO/RPO targets:** Recovery time objective and recovery point objective should be business-approved, tested, and mapped to the architecture. "We have backups" is not the same as "we can recover."
- **Backup and retention strategy:** SAP HANA backup, database backup, file-level backup, snapshots, retention, restore testing and archive policy should be designed together.
- **Identity and security controls:** SAP user governance, AWS IAM, privileged access, network segmentation, encryption, logging and vulnerability management must be joined up rather than treated as separate workstreams.
- **Operational telemetry:** CloudWatch, SAP monitoring tools, OS-level metrics, database metrics, application logs and business-process indicators should give teams early warning before users raise incidents.
- **Automation:** Start/stop schedules, system refreshes, backup checks, patch preparation, monitoring deployment, infrastructure templates and DR test routines should reduce the manual burden on SAP Basis and infrastructure teams.
- **Cost visibility:** Cost allocation tags, environment separation, utilisation reviews, pricing model selection and rightsizing should be built into the run model.

The AWS SAP Lens supplements the broader AWS Well-Architected Framework with SAP-specific design principles. Its value is that it forces the assessment to look beyond infrastructure into the operational and business context of SAP workloads.

3. The Common Gaps We See in SAP Landscapes

Gap 1: Production Is Protected, But Non-Production Is Forgotten

Many SAP estates protect production carefully but allow development, QA, sandbox and training environments to grow unchecked. These systems may run 24/7, hold copies of production data, consume high-cost storage, and remain oversized long after a project ends. They are rarely owned with the same discipline as production.

The fix is not simply to turn systems off. The right approach is to classify environments by business need, agree service hours, automate start/stop schedules, define refresh cycles, and track cost by environment. Basis teams should still have the flexibility to run systems when needed, but the default should not be permanent consumption.

Gap 2: Disaster Recovery Has Not Been Proved

SAP disaster recovery is often described in architecture diagrams but rarely tested end to end. A DR design should answer practical questions:

- Who declares the disaster?
- Which systems fail over first?
- How is SAP application connectivity redirected?
- What is the database replication state?
- How are interfaces paused or resumed?
- How are users told what to do?
- How is data consistency verified?
- How is failback handled?

For SAP HANA, high availability and disaster recovery designs must account for the database layer, application tier, file systems, operating systems, monitoring, backup and business validation. AWS provides services and patterns that support these designs, but the runbook and test discipline are just as important as the infrastructure.

Gap 3: HANA Sizing Is Treated as a One-Time Exercise

HANA sizing can quickly become outdated as data volumes grow, reports change, new modules are added, interfaces increase, or S/4HANA planning evolves. A one-time sizing estimate can leave teams either underprovisioned or paying for unused headroom.

Good sizing practice should include:

- current memory utilisation and peak patterns;
- CPU and storage throughput;
- database growth rate;
- batch and reporting windows;
- S/4HANA migration assumptions;
- compression and housekeeping opportunities;
- production vs non-production sizing policy;
- upgrade and testing headroom.

AWS gives teams more flexibility than fixed hardware procurement, but flexibility does not remove the need for measurement.

Example: HANA Sizing with Growth and Operational Headroom

HANA sizing should start from measured utilisation rather than simply copying the installed memory of the existing server.

Sizing Input	Example
Current observed peak HANA memory	1.20 TiB
Expected annual data/memory growth	10%
Planning period	3 years
Additional operational headroom	20%

Three-year projected memory requirement:

1.20 TiB × 1.10 × 1.10 × 1.10 = approximately 1.60 TiB

Adding 20% operational headroom:

1.60 TiB × 1.20 = approximately 1.92 TiB

The target EC2 configuration should therefore be selected from the current SAP-certified HANA instance list with sufficient memory above the calculated requirement. Memory should not be the only sizing factor. CPU utilisation,

SAPS, storage throughput, network throughput, batch peaks, reporting demand, data-load windows, backup duration and S/4HANA growth assumptions must also be reviewed.

The assessment should specifically validate:

- peak HANA memory during month-end and year-end processing;
- column-store and row-store consumption;
- database and large-table growth;
- expensive SQL and long-running statements;
- HANA data and log volume throughput;
- backup window and restore expectations;
- concurrent batch and interface activity;
- planned S/4HANA modules, company codes or data-retention changes;
- three-to-five-year growth assumptions;
- production versus non-production sizing policy.

Relevant SAP references should be validated for the organisation's exact HANA revision and scenario, including SAP HANA memory FAQ, HANA sizing/check tools, and cost-optimised non-production guidance.

Gap 4: SAP Security Is Split Across Too Many Owners

SAP security touches SAP roles, privileged access, network boundaries, data encryption, endpoint controls, AWS IAM, logging, monitoring, transport governance, and incident response. When ownership is split, gaps appear between teams.

A modern SAP security assessment should review:

- user and privilege model;
- emergency access and firefighter controls;
- access to SAP servers and databases;
- encryption at rest and in transit;
- segmentation between SAP tiers and connected systems;
- logging and alerting for privileged or unusual activity;
- vulnerability and patch process;
- backup access and restore control;
- regulatory evidence requirements.

The objective is not to create a heavier control environment. The objective is to make the control environment visible, testable and proportionate to the risk.

Gap 5: Basis Teams Carry Too Much Manual Work

SAP Basis teams often absorb operational complexity that should be automated: system copies, kernel patch preparation, backup verification, refresh requests, monitoring checks, storage growth, transport route checks, job failures and DR preparation. This keeps skilled people in reactive work and delays transformation.

Cloud-native SAP operations should free Basis teams to work on performance, readiness, process improvement, integration and business support. Automation should be introduced carefully, but the target state should be clear: fewer repetitive manual actions, clearer runbooks, earlier alerts, and better evidence.

4. S/4HANA Readiness Assessment Model

An S/4HANA readiness assessment should not be limited to application compatibility. The infrastructure and operating model matter because S/4HANA changes performance, data, integration and operational expectations.

Layer 1: Business and Process Readiness

Before technical design, confirm which business processes are in scope, which pain points must be solved, and which outcomes leadership expects. Questions include:

- Which SAP processes are most business-critical?
- Which month-end, production, procurement or reporting processes are slowest?
- Which outages or incidents created business impact in the last 12 months?
- Which transformation deadlines are immovable?
- Which stakeholders need evidence before approving spend?

Layer 2: Application and Custom Code

Assess custom code, interfaces, batch jobs, reports and historical modifications. Identify technical debt that could make the transformation risky. Basis and application teams should document the custom objects that are heavily used, rarely used, obsolete, or business-critical.

Layer 3: Data and HANA

Review data volume, growth rate, archiving policy, housekeeping, memory footprint, table growth, backup window, restore testing and reporting demand. This is where many organisations discover that the S/4HANA infrastructure discussion must be linked to data management.

Layer 4: Infrastructure and Resilience

Review compute, storage, network, DNS, load balancing, shared file systems, operating systems, HA, DR, monitoring and automation. The question is not simply whether the current environment works today. The question is whether it can support the next stage.

Layer 5: Security and Compliance

Map SAP security and AWS security controls to regulatory expectations, internal audit requirements and operational evidence. Ensure that logging, encryption, identity and incident response are not afterthoughts.

Layer 6: Operating Model

Define who owns SAP operations in the future state. Basis, infrastructure, cloud platform, security, finance and application teams all need clear responsibilities. This is especially important where managed services, AWS support, Cloudwrxs support and internal teams intersect.

5. Cost Optimisation for SAP Workloads

SAP cost optimisation should be treated carefully. The aim is not to reduce spend at the expense of resilience or performance. The aim is to eliminate waste, select the right pricing model, and make spend more transparent.

Common cost opportunities include:

- **Non-production scheduling:** Development, QA, training and sandbox environments can often be scheduled around working hours.
- **Rightsizing:** Instances should be sized from measured utilisation and growth assumptions, not copied from old hardware procurement.
- **Storage lifecycle:** Backup, logs, archive, snapshots and historical data should have defined retention and lifecycle policy.
- **Pricing model selection:** On-Demand, Reserved Instances, Savings Plans and other commitment models should be selected by workload pattern and risk tolerance.
- **Tagging and allocation:** SAP cost should be visible by environment, application, business unit and project.

- **Operational effort:** Manual work has a cost. Automation that reduces weekend work, repeated checks, slow refreshes and incident triage should be included in the business case.

The best SAP TCO models include infrastructure, licensing assumptions, migration effort, business downtime exposure, operational labour, security/compliance effort, backup/DR, growth and transformation opportunity cost.

6. High Availability and Disaster Recovery

For SAP, availability is not a generic percentage. It must be mapped to business process impact. A finance reporting system may tolerate a different recovery profile from a production manufacturing system. A corporate portal may have different requirements from core ECC or S/4HANA.

The assessment should define:

- critical systems and dependencies;
- acceptable outage by process;
- database replication and backup strategy;
- ASCS/ERS design;
- application server distribution;
- file system resilience;
- DNS, routing and access failover;
- interface dependencies;
- monitoring and alert ownership;
- DR test frequency;
- evidence required by audit or leadership.

AWS Availability Zones, SAP HANA replication, backup integration, Elastic Disaster Recovery patterns, CloudWatch alarms and automated recovery patterns can all form part of the design. The important point is that the design must be tested and understood by the people who will operate it.

Recommended SAP High Availability Patterns

The preferred HA design should be selected according to the SAP database, operating system, workload criticality and business-approved RTO/RPO rather than applying one standard pattern to every system.

For **SAP HANA on SUSE Linux Enterprise Server for SAP Applications**, a common production pattern is two HANA nodes distributed across separate AWS Availability Zones using **SAP HANA System Replication (HSR)** with **Pacemaker/Corosync** for automated takeover.

For **SAP HANA on Red Hat Enterprise Linux for SAP Solutions**, the equivalent design should use the supported RHEL Pacemaker framework and SAP HANA resource agents.

For in-Region HA, the HANA replication mode should be selected based on supported SAP HANA options, measured network latency and business RPO. For cross-Region DR, asynchronous replication is normally the more practical pattern because of geographic latency.

A typical production pattern is:

Availability Zone A * HANA primary. * ASCS. * SAP application server(s).

Availability Zone B * HANA secondary. * ERS. * SAP application server(s).

The HANA cluster, ASCS/ERS cluster and application tier should be treated as separate failure domains. A successful database takeover alone does not confirm that the complete SAP business service is available.

For other SAP-supported databases, use the database-native HA technology supported for the exact SAP/database/operating-system combination, for example:

- **Oracle:** Oracle Data Guard or another SAP-supported Oracle HA/DR configuration.

- **Microsoft SQL Server:** SQL Server Always On Availability Groups where supported by SAP, SQL Server edition and the Windows architecture.
- **IBM Db2:** Db2 HADR with the applicable SAP/IBM-supported cluster configuration.

The final design must be validated against the current SAP Product Availability Matrix, operating-system support matrix, database-vendor guidance and AWS SAP documentation.

ASCS/ERS Design Notes

SAP Central Services must not remain a single point of failure in an otherwise highly available landscape.

For ABAP systems, **ASCS** and **ERS** should normally be placed on separate EC2 instances in separate Availability Zones. A supported Pacemaker cluster can monitor and recover the Central Services resources when the active instance or underlying node becomes unavailable.

The design should cover:

- ASCS and ERS placement across separate Availability Zones;
- enqueue replication;
- SAP virtual hostname and name-resolution design;
- cluster fencing and node isolation;
- shared filesystem dependencies such as `/sapmnt` and transport directories;
- supported filesystem architecture;
- startup and shutdown order;
- application-server reconnection after ASCS failover;
- enqueue replication monitoring;
- controlled failover and failback testing;
- documented operational runbooks.

Application servers should be distributed across Availability Zones where practical. HA testing should validate SAP logon, enqueue processing, batch jobs, interfaces and database connectivity after failover, not only cluster resource movement.

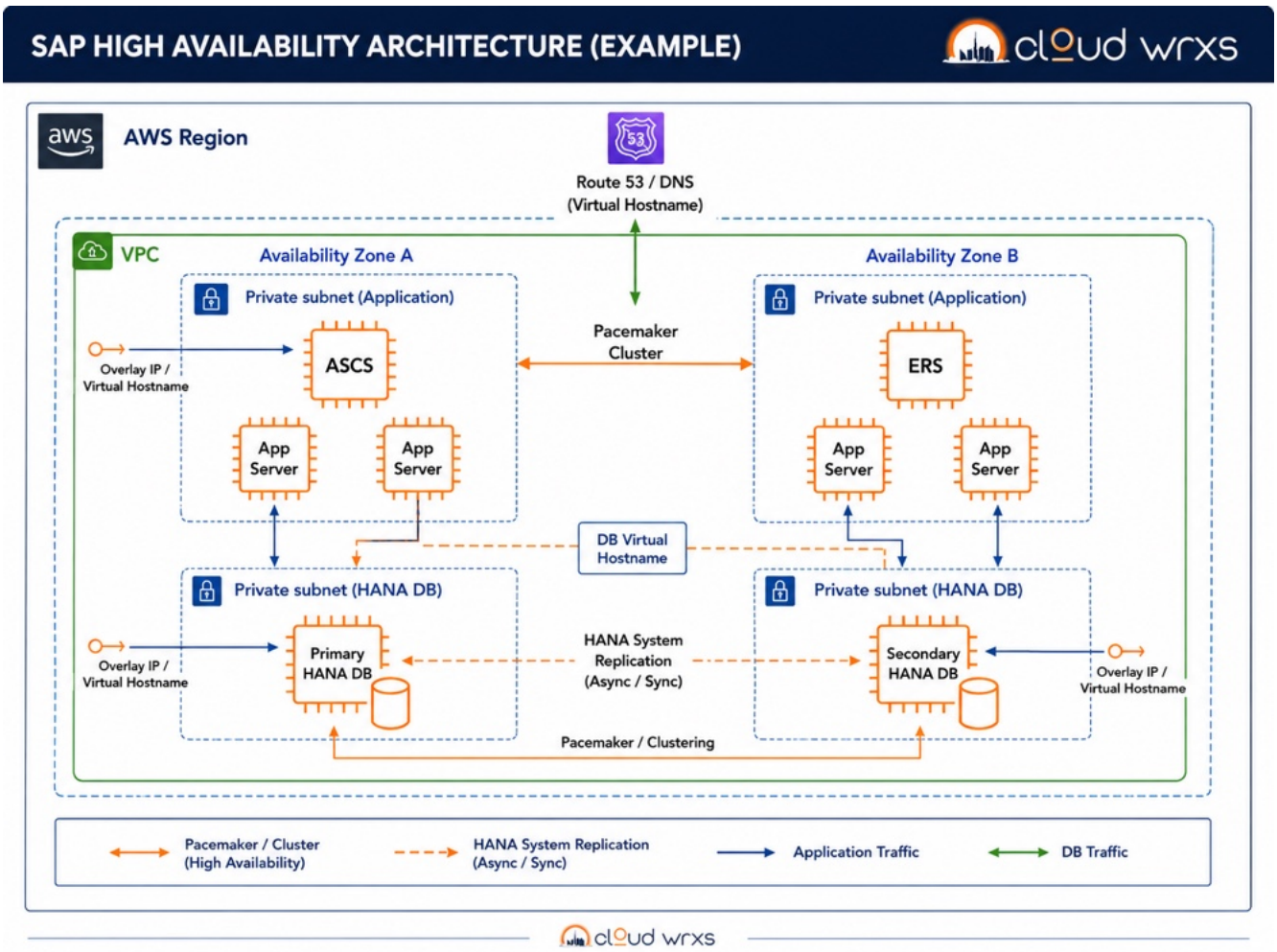

Figure – Cloudwrxs generic SAP HA pattern: ASCS/ERS and SAP application servers distributed across Availability Zones, with HANA primary/secondary replication and Pacemaker-based failover. This is an illustrative pattern and must be validated for the organisation's exact SAP, database and operating-system versions.

Backup and Restore Validation Checklist

A backup should not be considered proven merely because the scheduled backup job completed. Recovery capability must be validated regularly.

Scheduled Validation

- [ ] Confirm SYSTEMDB backup completed successfully.
- [ ] Confirm all tenant database backups completed successfully.
- [ ] Confirm HANA log backups are running without gaps.
- [ ] Review failed or cancelled backup jobs.
- [ ] Confirm the backup destination is accessible.
- [ ] Confirm expected backup objects exist in the repository.
- [ ] Check available backup/storage capacity.
- [ ] Check retention and lifecycle policy.
- [ ] Confirm encryption requirements are met.
- [ ] Review Backint or backup-agent errors.

Periodic Restore Validation

- [ ] Select an agreed recovery point.
- [ ] Provision or identify an isolated recovery environment.
- [ ] Confirm the required data/full backup is available.
- [ ] Confirm all required log backups are available.
- [ ] Validate backup integrity.

- [ ] Restore SYSTEMDB and tenant database(s) as applicable.
- [ ] Apply logs to the required recovery point.
- [ ] Start HANA and validate database consistency.
- [ ] Validate SAP application connectivity.
- [ ] Perform SAP logon and key transaction checks.
- [ ] Validate critical interfaces.
- [ ] Validate required background jobs.
- [ ] Record the actual restore duration.
- [ ] Record achieved RTO and RPO.
- [ ] Record issues and corrective actions.
- [ ] Obtain technical and business sign-off.

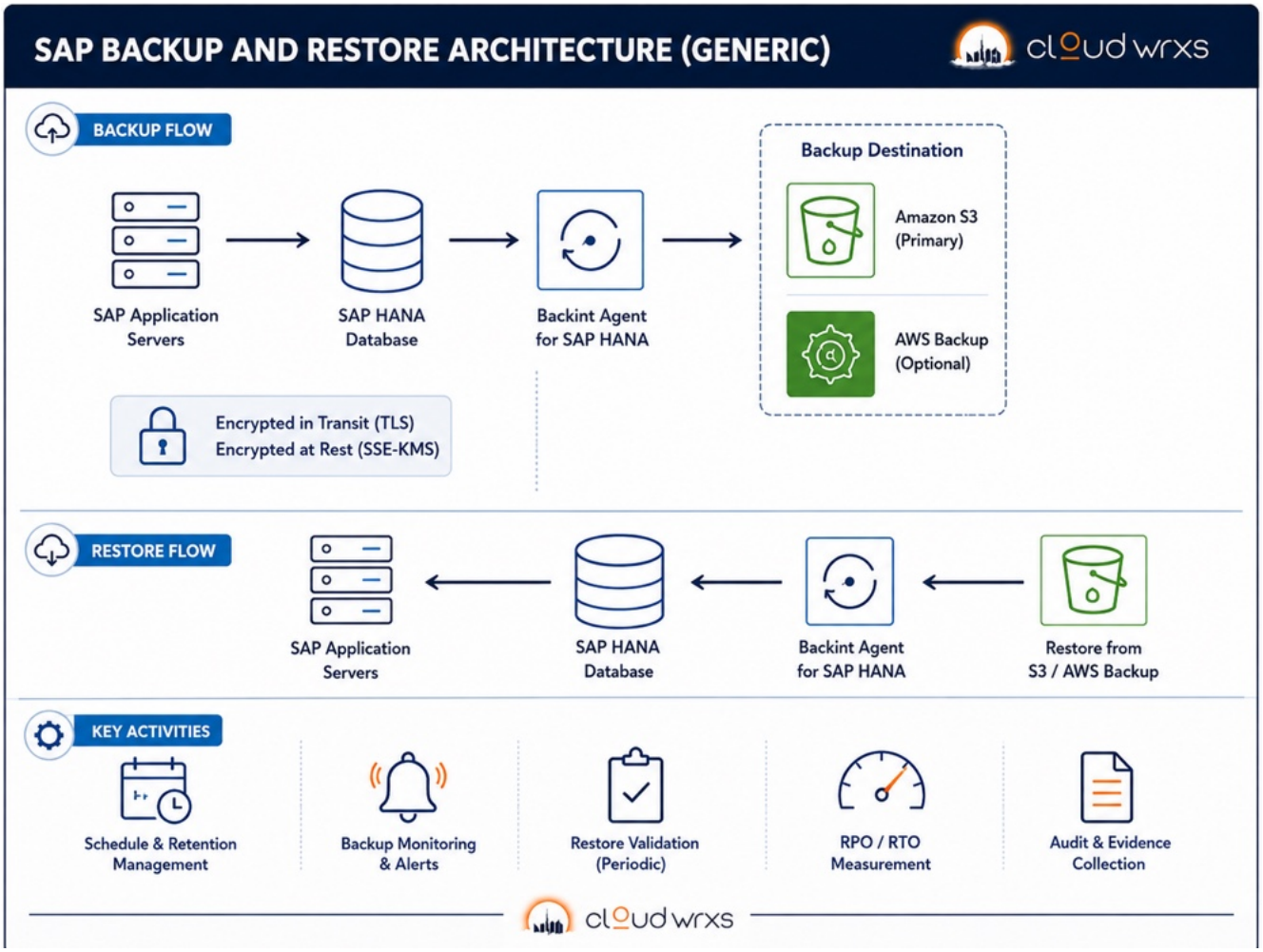

Figure – Cloudwrxs generic SAP backup and restore pattern using SAP HANA backup integration, Amazon S3/AWS Backup, encryption, monitoring, periodic restore testing and evidence collection.

7. Security and Compliance Considerations

SAP security should be assessed through both technical and governance lenses.

Technical Areas

- SAP user roles and segregation of duties;
- privileged account management;
- network segmentation and security groups;
- private connectivity and controlled ingress;
- encryption of storage, backups and data in transit;

- OS patching and vulnerability management;
- logging, monitoring and alerting;
- backup protection;
- incident response runbooks.

Governance Areas

- regulatory obligations including local data and financial-sector requirements where applicable;
- audit evidence;
- change approval and emergency access;
- third-party access;
- data retention and deletion;
- business continuity testing;
- access review cadence.

The desired result is a SAP environment where security is visible and testable. Leadership should not have to accept security on trust; the platform should generate evidence.

KSA Regulatory Evidence Examples

For organisations operating in the Kingdom of Saudi Arabia, SAP modernisation should include the capability to produce operational security evidence rather than relying only on architecture statements.

The exact control framework depends on the organisation and sector. Relevant frameworks may include the **National Cybersecurity Authority Essential Cybersecurity Controls (ECC)**, **Cloud Cybersecurity Controls (CCC)** and, where applicable to the organisation, the **Saudi Central Bank Cyber Security Framework**.

Examples of evidence that an SAP/AWS operating model can produce include:

Control Area	Example SAP / AWS Evidence
Identity and access	SAP user access review, privileged-user list, AWS IAM review, emergency/firefighter access records
Segregation of duties	SAP role review, SoD reports, administrator authorisation matrix
Change management	SAP transport approvals, transport import logs, emergency-change evidence
Logging	SAP Security Audit Log, AWS CloudTrail, CloudWatch logs, OS/database audit logs
Backup	HANA backup logs, backup-status reports, retention configuration
Recovery	Restore-test reports, screenshots/logs, actual recovery duration
Disaster recovery	DR runbook, failover-test report, achieved RTO/RPO and business sign-off
Monitoring	CloudWatch alarms, SAP monitoring alerts, incident tickets
Encryption	KMS configuration, EBS encryption, backup encryption and TLS configuration
Vulnerability management	OS patch records, vulnerability scans and remediation evidence
Privileged activity	SAP administrator activity and AWS administrative audit trail
Incident response	Incident record, root-cause analysis, corrective/preventive actions
Business continuity	DR test calendar, recovery procedure and evidence
Data retention	Backup/log retention policies and lifecycle/deletion evidence
Third-party access	Vendor access approval, expiry, MFA and activity records

The architecture should not be described as automatically compliant. The objective is to help the organisation implement applicable controls and produce repeatable evidence. Final control mapping should be validated with the organisation's cybersecurity, risk, compliance and legal teams.

8. Basis Team Operating Model

Basis teams are central to a successful SAP modernisation. They know where the fragile points are, which jobs fail, which integrations behave badly, which maintenance tasks consume time, and which users will notice performance changes first.

The modern Basis operating model should include:

- documented ownership between Basis, cloud platform, security and application teams;
- automation backlog for repetitive work;
- agreed patch and maintenance calendars;
- performance baselines and alert thresholds;
- backup and restore test evidence;
- DR runbook ownership;
- system refresh process;
- change and transport governance;
- knowledge transfer and skills development.

The role of Cloudwrxs is to help the Basis team move from infrastructure firefighting to controlled, measurable, cloud-enabled SAP operations.

CloudWatch and SAP Monitoring Implementation Example

AWS monitoring should complement rather than replace native SAP monitoring.

A practical monitoring architecture has three layers:

AWS Infrastructure Layer

Amazon CloudWatch and CloudWatch Agent can be used to monitor:

- EC2 CPU utilisation;
- operating-system memory and swap;
- filesystem utilisation and growth;
- EBS IOPS, throughput and latency;
- EC2 status checks;
- network throughput;
- AWS service health;
- backup-job status;
- selected operating-system logs.

SAP HANA / Database Layer

Database monitoring should include:

- HANA service availability;
- memory and CPU utilisation;
- expensive SQL and long-running statements;
- data/log volume utilisation;
- backup status and failures;
- HANA System Replication state;
- replication latency or backlog;
- primary/secondary role;
- critical database alerts.

SAP Application Layer

Basis monitoring should include:

- SAP instance availability;
- work-process utilisation;
- long-running work processes;
- SM21 system-log errors;
- ST22 short dumps;
- cancelled background jobs;
- jobs exceeding expected runtime;
- RFC and interface failures;
- IDoc failures;
- update errors;
- lock-table conditions;
- spool issues;
- certificate expiry;
- SAP filesystem growth.

A useful operating model is to use CloudWatch for infrastructure telemetry and centralised alerting while retaining SAP-native monitoring for application and database semantics. The objective is to correlate an AWS infrastructure symptom with its SAP business impact rather than investigate each layer independently.

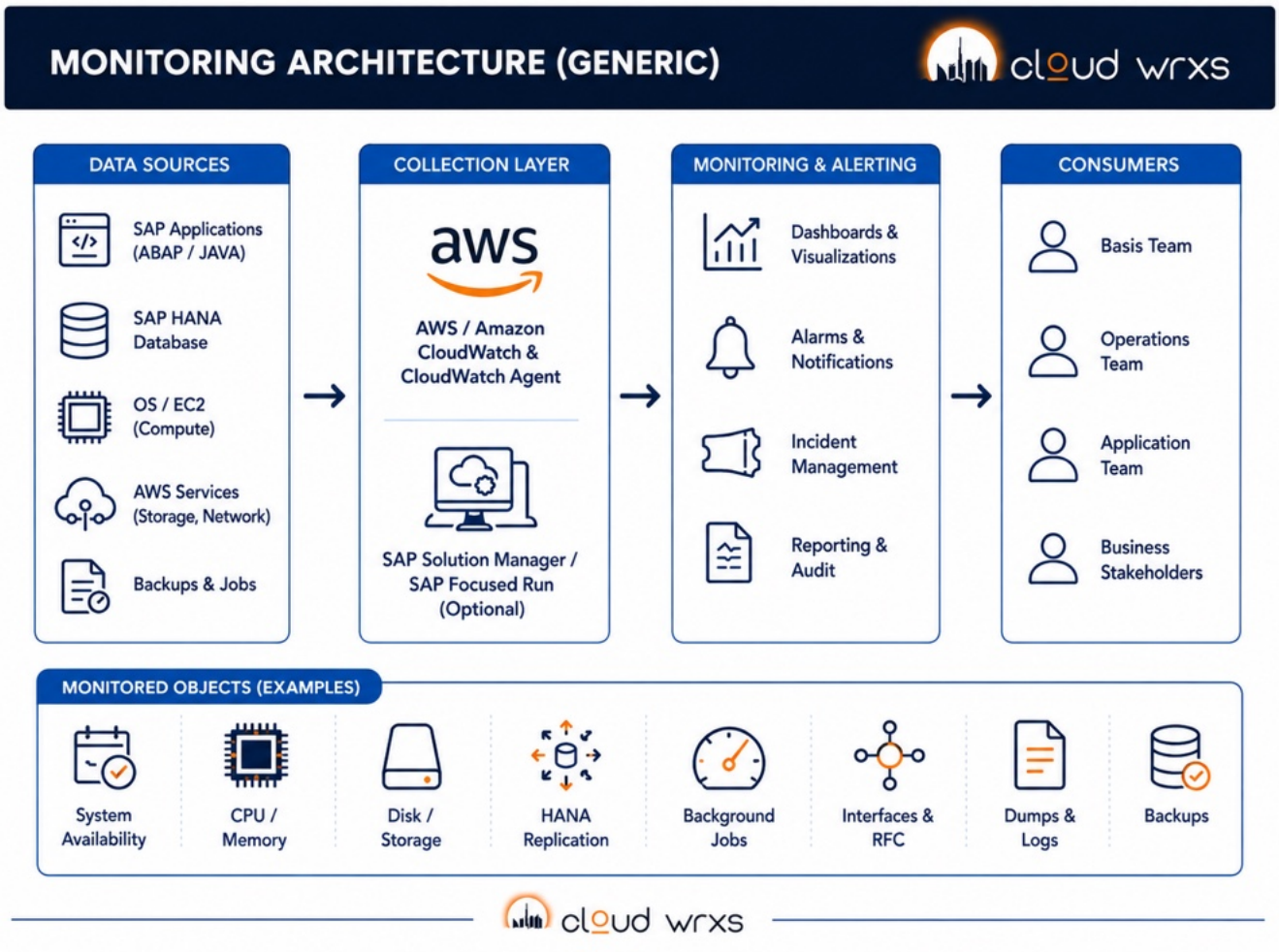

Figure – Cloudwrxs generic monitoring architecture showing SAP application, HANA, operating system, AWS services and backup telemetry flowing into CloudWatch/SAP monitoring, alerting, dashboards, incident management and audit reporting.

SAP Transport Governance Considerations

SAP transport management remains a core Basis responsibility after migration to AWS.

The operating model should define:

- approved DEV → QAS → PRD transport path;
- transport ownership and import authorisation;
- required approvals;
- transport sequence and dependencies;
- emergency transport procedure;
- production import windows;
- return-code handling;
- import-log retention;
- validation and escalation/rollback procedure.

Before a production import, the Basis team should confirm:

5. Required transports are released.
6. Dependencies are understood.
7. Import sequence is agreed.
8. The transport was validated in QAS.
9. Required downtime is approved.
10. Application owners are available for validation.
11. Backup/recovery requirements are understood.
12. Interfaces and dependent systems are considered.

After import, validate return codes, application functionality and business/application-owner acceptance. Transport evidence can also form part of the organisation's change-management and audit trail.

SAP System Refresh / System Copy Considerations

Cloud infrastructure can simplify provisioning, but an SAP system refresh remains an SAP-controlled process with important pre-copy and post-copy activities.

Pre-Refresh

- Capture source and target system details.
- Capture SAP profiles.
- Capture RFC destinations.
- Capture logical-system information.
- Capture printers and interfaces.
- Capture batch jobs and target-specific job configuration.
- Capture target-specific users/settings.
- Capture certificates and licences where applicable.
- Capture database connectivity.
- Suspend outbound interfaces as required.
- Confirm backup/recovery point.
- Obtain refresh approval.

Database Refresh

- Stop SAP services in the required sequence.
- Restore or copy the database.
- Validate database consistency.
- Validate database connectivity.
- Update required host/database-specific configuration.
- Start the SAP system in a controlled sequence.

Post-Refresh

Validate or correct:

- logical system names;
- BDLS requirements where applicable;
- RFC destinations;
- ALE/IDoc destinations;
- interfaces;
- background jobs;
- target-specific job variants;
- production-only users and user locks;
- printers and spool configuration;
- email/SAPconnect configuration;
- batch users;
- certificates;
- SAP profiles;
- database connections;
- HANA user-store entries where applicable;
- third-party integrations;
- transport routes;
- monitoring;
- backup configuration;
- security connections;
- external URLs and file-transfer destinations;
- cloud-specific hostname/IP dependencies.

The refresh should finish with a Basis technical validation, application/business validation and documented sign-off. Repeatable activities can be automated, but system-specific exclusions and business safeguards must remain visible.

9. Workshop Approach

Cloudwrxs recommends a workshop-led approach because it creates alignment before major decisions are made.

Phase 1: Discovery

Collect architecture diagrams, system inventory, interface list, user volumes, batch windows, outage history, backup design, DR objectives, cost baseline, security controls and current pain points.

Phase 2: Technical Assessment

Review the landscape against SAP-on-AWS and SAP Lens principles: operational excellence, security, reliability, performance efficiency, cost optimisation and sustainability. Focus on gaps that create business impact.

Phase 3: Commercial and Risk Assessment

Build a practical view of cost, risk, effort, benefits and decision points. Separate quick wins from migration decisions and longer transformation activities.

Phase 4: Roadmap

Produce a prioritised roadmap with immediate remediation, readiness activities, target architecture, dependency list, decision log and next-step workshop actions.

10. What You Should Do Next

If your SAP environment has any of the following symptoms, a SAP Modernisation Workshop is a sensible next step:

- batch jobs regularly run into business hours;
- DR has not been tested end to end in the last 12 months;
- non-production systems run permanently without clear ownership;
- SAP hosting contracts are approaching renewal;
- S/4HANA planning is underway but infrastructure readiness is unclear;
- Basis teams are spending too much time on repetitive operations;
- leadership wants a business case but the cost model is incomplete;
- security and compliance evidence is hard to produce quickly.

The workshop outcome should be a practical assessment: what is working, what is risky, what can be optimised now, what needs deeper design, and what should be prioritised for business approval.

Reference Sources

- AWS SAP Lens: https://docs.aws.amazon.com/wellarchitected/latest/sap-lens/sap-lens.html
- AWS SAP Lens design principles: https://docs.aws.amazon.com/wellarchitected/latest/sap-lens/well-architected-design-principles.html
- SAP on AWS high availability setup: https://docs.aws.amazon.com/sap/latest/sap-hana/sap-oip-sap-on-aws-high-availability-setup.html
- SAP HANA HA and DR on AWS: https://docs.aws.amazon.com/sap/latest/sap-hana/hana-ops-ha-dr.html
- SAP workload cost optimisation on AWS: https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-sap-cost-optimization/introduction.html
- AWS pricing models for SAP workloads: https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-sap-cost-optimization/pricing-models.html
- SAP HANA certified EC2 instances: https://docs.aws.amazon.com/sap/latest/general/sap-hana-aws-ec2.html

Additional SAP HANA Sizing References

- AWS SAP HANA sizing guidance.
- AWS SAP HANA certified and non-certified EC2 instance guidance.
- AWS SAP HANA EBS storage guidance.
- SAP HANA memory FAQ / relevant SAP KBA for the organisation's revision.
- SAP HANA sizing and hardware-configuration check guidance.
- SAP guidance for cost-optimised non-production HANA where applicable.

Additional High Availability References

- AWS SAP HANA High Availability and Disaster Recovery guidance.
- AWS SAP HANA System Replication guidance.
- AWS SAP NetWeaver ASCS/ERS HA guidance for SUSE Linux.
- AWS SAP NetWeaver ASCS/ERS HA guidance for Red Hat Enterprise Linux.

Additional Backup and Recovery References

- AWS Backint Agent for SAP HANA guidance.
- SAP HANA database backup and recovery FAQ.
- SAP guidance for determining required recovery files.
- SAP HANA backup integrity/recoverability check guidance.
- SAP HANA backup scheduling guidance.

Additional Monitoring References

- Amazon CloudWatch Application Insights guidance for SAP NetWeaver and SAP HANA.
- AWS SAP monitoring and operations guidance.

Saudi Arabia Cybersecurity / Regulatory References

- National Cybersecurity Authority – Essential Cybersecurity Controls (ECC).
- National Cybersecurity Authority – Cloud Cybersecurity Controls (CCC).
- National Cybersecurity Authority implementation guidance.
- Saudi Central Bank Cyber Security Framework, where applicable to the organisation's regulatory scope.

Reference note: SAP Notes and KBAs are revised over time. The latest version and applicability of each SAP Note/KBA should be checked through SAP for Me during detailed design or implementation.