Systems Patch Maintenance Procedure

Draft

Draft procedure is work in progress.

1. Purpose

This is a comprehensive Procedure document for SyWay SAP systems Patch Maintenance, covering both On-Premise and SaaS/Cloud (Public and Private) deployments. This procedure defines the standardized process for planning, assessing, applying, testing, validating and documenting SAP patches (Support Packages, Security Notes, Kernel patches, Hotfixes etc.) across the landscape. The goal is to minimize security risks, ensure system stability and compliance, reduce downtime, and maintain business continuity while adhering to the shared responsibility model in cloud environments.

1.1 Key Objectives

- Apply security patches regularly on monthly basis (especially SAP Security Notes released on Patch Day).
- Manage functional corrections, support packages, Hotfix Collections (HFC), Kernel updates and other Infrastructure patches.
- Coordinate maintenance across SAP Rise Private Cloud Edition (PCE), BTP, SaaS and components deployed in Azure/AWS CSPs, which are part of SyWay program.

2. Scope

The process mentioned in this document is applicable to following categories of Applications for both ROW and China specific instances.

Category	Application Series - 1	Application Series - 2
SAP Rise	SAP S/4HANA SAP Cloud Connector SAP Data Provisioning Agent SAP Web Dispatcher	SAC Agent OpenText Connector SAP TM Optimizer
Azure	SAP WWI Server NextLabs Policy Server OpenText xECM	Syniti Replicate (China) Syniti Connector (China)
AWS	Syniti Replicate (ROW) Syniti Connector (ROW)	
SAP BTP	Asset Performance Management Profitability and Performance Management Build Work Zone Task Center Cloud Identity Services (IPS+IAS) Identity Access Governance Datasphere SAP Analytics Cloud (SAC) Integration Suite Forms Service by Adobe	Business Network Freight Collaboration Risk and Assurance Management Business Network Global Track and Trace Sustainability Footprint Management Sustainability Control Tower Group Reporting Data Collection Advanced Financial Closing Document Reporting Compliance
SaaS	SuccessFactors Ariba ICertis Salesforce Syniti Knowledge Platform	BlackLine Kinaxis Maestro WalkMe OpenText Cloud (Core Capture & Archiving) Bloomberg Vertex EDICOM

3. Guiding Principles

- Prioritize security notes and aim to complete installation across the landscape within the same month
- Plan support pack upgrade for applicable systems once a year. Avoid patching before Major release.
- Always test in non-production environments first.
- Use SAP Cloud ALM for unified visibility across hybrid landscape.

- Maintain uniform patch levels across landscape where possible.
- Maintain detailed documentation of all changes for future reference (i.e., SOX and GDPR compliance).
- Define clear rollback plans in production (backups + transport rollback).
- Schedule regular Patch Day reviews with relevant stakeholders at regular intervals.
- For SaaS, subscribe to product community pages and cloud service status for schedule and plan.

4. Maintenance Procedure

4.1 SAP Rise

4.1.1 Support Package Stack (SPS)

Refer to Upgrade process outlined here. All environments in the landscape as per Upgrade plan. Refer to below best practices when planning SPS upgrade

- Side Effect Notes - Review side effects notes released with SPS, assess and take a decision on scope
- Component Version Notes - Review the notes released with component versions and known bugs released via notes
- Kernel Patches - Always include Kernel patch along with SPS upgrade
- Client Tools - Assess and include client tools such as DB clients or SAP GUI client etc.
- Add-on components - Assess and include add-on components

4.1.2 Kernel Updates

The frequency of Kernel updates is a balance between maintaining a stable system and staying protected against security threats. Kernel updates should be part of quarterly update cycle (every 3 months) and should be part of maintenance window on a quarterly basis.

Refer to below key points when planning Kernel update

- Monitor the "New" Kernel - Do not download the patch immediately after it is release. It is often a good practice to wait at least 2 weeks after a patch is released.
- Kernel version - Maintain same kernel version across the landscape
- Side Effect Notes or Known Bugs - Kernels are usually released with central note listing known bugs or pre-requisite OS patches. Check and take a decision on scope
- Database client - Kernel update is the best time to refresh DB clients.

4.1.3 ST-PI and ST-A/PI Plugins

The best practice is to maintain these plugins at the latest or second-latest Support Package to ensure the data collection modules match the latest cloud ALM features. Unlike Kernel or SPS upgrades, ST-PI and ST-A/PI are "low-risk" plugins, which does not require a system restart. These plugins can be included in quarterly update cycle along with Kernel updates.

4.1.4 Hot News

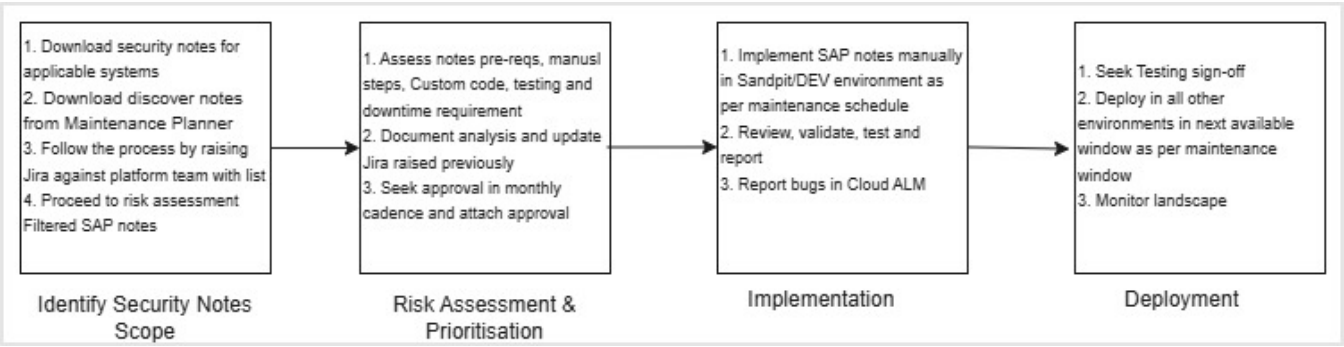
SAP releases a "Hot News" Security Note (specifically for vulnerabilities with a CVSS score of 9.0 or higher), these Hot News notes will bypass the quarterly/monthly cycles and should be applied immediately in next available maintenance windows. Hot News will usually affect components such as Internet Communication Manager (ICM) or the SAP Gateway

4.1.5 Application add-on Components & Others

In general, SAP application add-on components (such as Open Text, TM Optimizer etc.) and other components (DP Agent, Cloud Connectors, Web Dispatcher) are subjected to SAP Application Life Cycle Maintenance approach and SAP Security Patch Day every month. However, some of these components may have different patching rhythm. The best practice is to include these components into Quarterly Cycle Patch maintenance scope and perform latest or second-latest patch upgrade as of that quarter.

4.1.6 Security Notes

Below high level steps to be followed each month starting on SAP Patch Day (2nd Tuesday) which are sequenced as per SyWay approach.



4.2 Public Cloud (SaaS)

SAP or Vendor manages and follows the application maintenance through the landscape. Platform team to monitor and communicate with relevant stakeholders to fulfill Syensqo responsibilities.

4.3 Azure/AWS dependent components

Applications installed in Axure/AWS will follow IT patch maintenance life cycle process. More details will be updated in next revision.

5. Roles and Responsibilities

5.1 Shared Responsibility Model

Under RISE with SAP, security responsibilities are divided between SAP Enterprise Cloud Services (ECS) and the customer. That means SAP do not handles all patching automatically

SAP ECS — Infrastructure Layer	**Customer — Application Layer**
• OS-level security patching (hyperscaler VMs)	• Review & risk-assess all SAP Security Notes
• Database (HANA) patching & administration	• Request application patches via Service Request
• Network, compute & storage maintenance	• Provide downtime windows for scheduled patches
• HotNews/Emergency notes with no manual steps	• Test all implemented notes in DEV and QAS
• JAVA component patches (standard contract)	• Authorise transport to Production
• System reboots for infrastructure patches	• User administration, roles & authorisations
• 24×7 infrastructure monitoring	• Custom ABAP/code security & SoD management
• Key management for data at rest	• RFC access restriction & security configuration

5.2 RACI Matrix

Below is the RACI matrix to be followed for applying the Security Notes on a monthly basis

Activity	**SyWay Platform Team**	**Security**	**Functional Owner**	**SAP ECS**
Download/Review Security Notes	R, A		I	I
Perform Impact Assessment	R	R, A	C	C
Note Prioritization	A	R	C	I
Raise Jira	R	A	I	I
Implement note — application layer	R, A	C	I	I
Testing	R, A	R	R	I
Approve & deploy via Active Control	R, A	C	C	I
Post deployment Monitoring	R, A	C	I	I
Documentation & Governance	R	A	I	I

R = Responsible | A = Accountable | C = Consulted | I = Informed

6. Patch types, Frequency and Schedule

6.1 Monthly Candence Meetings

Monthly Cadence meetings are required to inform relevant stakeholders on patch maintenance/schedule. Below are the meeting details

Meeting Agenda	**Participants**	**Meeting date /time**

1. Review the Security Notes scope /assessment and seek approval 2. Review implementation schedule 3. Review Monitoring Status of previous month patch deployment 4. Update on upcoming releases /deployment	Technology Lead, Integration Lead, Cross Release Lead, Platform Lead, Security Lead, ECS CDM/TSM, ABAP Lead, Integration Lead	2nd Thursday of every month. Time - to be decided Duration - 55 mins

6.2 SAP Rise

Patch type	Frequency	Implementation Duration	Schedule	Maintenance Window	Remarks
Hotfixes	On Demand	Immediate	Next available window	Next available window	Assess, test and deploy immediately
Security Notes	Monthly basis	within month of Patch day	Jan, Feb, Mar, Apr, May, June, July, Aug, Sep, Oct, Nov, Dec	**China -** Non-Prod - 2nd Friday of each month, 23.00 - 3.00 AM CET Prod - 4th Sat of each month, 03:00 - 07:00 CET **ROW -** Sandbox, Dev and IT - 2nd Sat of each month, 03:00 - 07:00 CET QAS, Parallel run, Training - 3rd Sat of each month, 03:00 - 07:00 CET Prod - 4th Sat of each month, 03:00 - 07:00 CET	Apply based on assessment and priority.
Kernel	Quarterly	Within the same month of a quarter	Feb, May, Aug, Nov		Plan security notes, Kernel, ST plugins and applicable component upgrades in the same quarterly cycle
ST-PI and A/PI	Quarterly	Within the same month of a quarter	Feb, May, Aug, Nov		
Application add-on Components & Others	Quarterly	Within the same month of a quarter	Feb, May, Aug, Nov		
Support Pack Stack	Yearly	As per project plan	As per plan	As per plan	Follow guidelines specified in section 4 above.

6.3 Public Cloud (SaaS)

For SaaS applications managed by SAP or other vendors, SAP or vendor manages and applies bi-weekly and quarterly updates as per their application life cycle management process. Platform team to monitor, communicate and coordinate the SaaS application upgrades with relevant stakeholders as per the schedule published by SAP or other vendor.

6.4 Azure/AWS dependent components

The applications hosted in Azure/AWS will follow the Patch maintenance schedule of Syensqo IT. More details will be updated in next revision.

7. Testing

Below are the key points to consider to limit the testing scope by Technology or Functional resources

- Based on the impact assessment, either limit the scope of testing to impacted functional/technical scenarios or focus on critical scenarios in the system
- Test in Preview or test tenant for SaaS applications or Integrated Test environment for SAP Rise application
- Limit the scope of testing to 2-3 days (max)

8. Monitoring and Compliance

8.1 Monitoring

- **Cloud ALM** - There are several tools available within Cloud ALM. Configuration & Security Analysis to be leveraged for component version checks, Health Monitoring to be leveraged for post notes/patch implementation to check security notes implementation across the landscape.
- **Early Watch Alert -** EWA is a automated diagnostic service that monitors the health, performance and security of the SAP landscape

8.2 Compliance

Compliance for SAP Security Notes centers around Vulnerability Management and change control

Type	Definition	Recommendation
SLA Adherence	SAP standard best practice recommendation is to apply patches based on CVSS score or priority	Hot News - within 5 business days High Priority - within 30 days
Documentation & Audit trail	Every patch must be linked to associated change control process and details need to be updated as per maintenance procedure stated in this procedure document.	Jira request is required. Documentation is to be maintained in Jira. Jira Board for tracking initial notes, scope and deployment status for each month
Segregation of Duties (SoD)	The person downloaded/assessed notes should not be the one signing-off on functional testing	Functional owner sign-off required
Landscape consistency	Compliance requires that same patch is applied across all environments	Cloud ALM version