|  |
| --- |
| International SOS AWS Management |
| Interlock |
| Process |
| Document number: 1 |
| Release date: |
| Status: Draft |
| Version: 3.0 |

Document status

|  |  |
| --- | --- |
| Title: | Document for International SOS |
| Status: | Initial |
| Owner: | Ashlesha Mahadik |
| Author(s): | Jagruti Joshi |
| Approver(s): | Ashlesha Mahadik, Nitin Thakur, Ranjit Iyer |
| Document number: | 1 |
| Document type: |  |
| Version: | 1.0 |
| Release date: | 20th Oct 2023 |

Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Changes made | Author(s) |
| 0.1 | 11 July 23 | *Original version* | Jagruti Joshi |
| 0.2 | 24 Aug 23 | *Updated change management & Patch process* | Jagruti Joshi |
| 0.3 | 27 Sept 23 | *Updated Incident process, Problem management and overall scope*  Patch management process | Jagruti Joshi |
| 1.0 | 20 Oct 23 | *Updated RACI* for change and patch management | Ashlesha Mahadik |
| 2.0 | 02 Feb 24 | Added MIM process & Project work process | Sanjay Varma |
| 3.0 | 10 Nov 24 | *Updated escalation matrix* | Hiren Tank |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[**1** Introduction 5](#_Toc201335128)

[1.1 **Summary** 5](#_Toc201335129)

[1.2 **Scope** 5](#_Toc201335130)

[1.3 **Out of scope** 6](#_Toc201335131)

[1.4 **Modification guidelines** 6](#_Toc201335132)

[1.5 **Deviation request** 6](#_Toc201335133)

[1.6 **References** 6](#_Toc201335134)

[**2** Service management 7](#_Toc201335135)

[2.1 **Service support** 7](#_Toc201335136)

[2.2 **Service management team roles** 7](#_Toc201335137)

[2.3 **Escalation Matrix** 7](#_Toc201335138)

[Escalation Matrix of International Integrator 7](#_Toc201335139)

[Escalation Matrix of Integrated Operations Team (CSD) 8](#_Toc201335140)

[2.4 **Delivery and Operations Model** 8](#_Toc201335141)

[2.5 **Tools** 8](#_Toc201335142)

[2.6 **Support:** 8](#_Toc201335143)

[2.7 **Inventory:** 9](#_Toc201335144)

[**3** Reactive incident management 10](#_Toc201335145)

[3.1 **Reactive incident management** 10](#_Toc201335146)

[3.2 **Customer expectations** 10](#_Toc201335147)

[3.3 **Points of contact** 10](#_Toc201335148)

[3.4 **Roles** 10](#_Toc201335149)

[3.5 **SLO Measurements** 11](#_Toc201335150)

[3.6 **Case entrance criteria** 12](#_Toc201335151)

[3.7 **Process flow** 12](#_Toc201335152)

[3.8 **US - Interim Service Engagement Model (until e-bonding)​** 13](#_Toc201335153)

[3.9 **When users are fully following the Interim Process**​ 14](#_Toc201335154)

[3.10 **Procedure** 15](#_Toc201335155)

[3.11 **RACI matrix** 15](#_Toc201335156)

[3.12 **Escalation matrix** 15](#_Toc201335157)

[**4** Vendor Management 17](#_Toc201335158)

[**5** Problem management 18](#_Toc201335159)

[5.1 **Description** 18](#_Toc201335160)

[5.2 **Customer expectations** 18](#_Toc201335161)

[5.3 **Points of contact** 18](#_Toc201335162)

[5.4 **Roles** 18](#_Toc201335163)

[5.5 **Entry criteria** 18](#_Toc201335164)

[5.6 **Inputs** 18](#_Toc201335165)

[5.7 **Tools** 18](#_Toc201335166)

[5.8 **Measurements** 18](#_Toc201335167)

[5.9 **Procedure** 19](#_Toc201335168)

[5.10 RACI matrix 19](#_Toc201335169)

[**6** Change Management 20](#_Toc201335170)

[6.1 Description 20](#_Toc201335171)

[6.2 Customer expectations 20](#_Toc201335172)

[6.3 Tools: 20](#_Toc201335173)

[6.4 Escalation Matrix: 21](#_Toc201335174)

[6.5 Entry criteria: 21](#_Toc201335175)

[6.6 Types of changes 22](#_Toc201335176)

[6.7 Process flow 23](#_Toc201335177)

[6.8 Procedure: 23](#_Toc201335178)

[6.9 RACI matrix 24](#_Toc201335179)

[6.10 Maker & Checker process (4 Eye process) 24](#_Toc201335180)

[**7** Patch & Release management 25](#_Toc201335181)

[7.1 Description 25](#_Toc201335182)

[7.2 Customer expectations 25](#_Toc201335183)

[7.3 Points of contact 25](#_Toc201335184)

[7.4 Roles 25](#_Toc201335185)

[7.5 Entry criteria 26](#_Toc201335186)

[7.6 Inputs 26](#_Toc201335187)

[7.7 Tools 30](#_Toc201335188)

[7.8 Process Flow 31](#_Toc201335189)

[7.9 Patch Management RACI matrix 31](#_Toc201335190)

[**8** Configuration Management -TBC 32](#_Toc201335191)

[**9** Major Incident Management Process 33](#_Toc201335192)

[**10** Project Work Process 34](#_Toc201335193)

[11 Service Level Reporting 34](#_Toc201335194)

[A.1 Acronyms 35](#_Toc201335195)

[A.2 Terms 35](#_Toc201335196)

[A.3 Additional documents 36](#_Toc201335197)

Introduction

* 1. **Summary**

This document describes the baseline process to be followed by International Integrator for referring and supporting Customer incidents between support groups involving the **products and services** supported by International Integrator

**Whenever possible** this interlock processes should be used for interaction within International Integrator teams in the support of our International SOS but due to the customized nature of the offerings International Integrator may be involved in to support, we need to be **flexible** and **accommodating** for using alternate customized interlock processes, if justifiable reasons can be provided.

This document is the Baseline model for the interlock, where the COG will be required to provide the detailed specifics associated with the overall support and interlock.

* 1. **Scope**

This interlock is applicable for providing support to International SOS AWS Management.

|  |  |
| --- | --- |
| Operations, Monitoring, and State Management | MSP provides availability management (event and Incident response), service level management, configuration management, Service Request management, service de-provisioning, Service Request approval workflows, and triage of AWS Services Incidents to AWS. |
| OS Support | Managed OS Support to provide a reproducible, tested, and consistent AWS environment that provides a uniform software system for Microsoft Windows and supported Linux platforms. |
| OS Builds | MSP expected to build all OS builds in AWS hosted instances with standard allowed Software's |
| Patch Management | MSP should provide OS Patching and Management Of Patching Changes for all Managed EC2 Instances, based on OS image standards within AWS |
| Security Management | MSP should manage AWS Resource Groups and IAM, ACL, Directory services in AWS environment.  Check point management server and Firewalls |
| Antivirus, Anti-Malware | MSP Should ensure protection against Viruses and Malicious attacks in AWS environment |
| Backup Service | MSP Should provide an Image Level Backup service of EBS Backed EC2 Instances and Volumes using a native AWS Backup Solution. A complete Backup service management is expected from MSP |
| Billing Management | MSP will perform all billing functions for both the Services and the Customer’s AWS environment usage |
| Automation & IAC | MSP is responsible for maintaining Automated environment and Use IAC tools to deploy AWS infrastructures |
| Service Management | MSP is fully responsible for Complete end to end Service management by integrating with our Service Management tool. |
| Incident Management | MSP is responsible for End-to-End incident Management |
| Load Balancer Management | MSP will update Customer’s Load Balancer(s) configurations in response to workload changes. |
| VPC Management | MSP will Manage and Maintain VPC within AWS environment and support for connectivity to On-premises & other Networks |
| EQX Cloud Exchange Back bone Mgmt. | MSP will Manage and Support Equinix Cloud Exchange for all Express Route Connectivity. |
| On-Boarding & Design Service | MSP will be responsible for On boarding and Supporting / Designing any new services, environment in AWS infrastructure Including Landing Zone. |
| AWS Trusted Advisor Reporting | MSP will be responsible for complete AWS Reporting either via trusted Advisor or Third-party tools like Cloudchecker |
| SLA | Refer to the SLA Tab |

* 1. **Out of scope**
* Third Party Applications & NTP Servers related incidents are not supported by Orange business.
* For Physical LAN, WAN, Security Devices Management, it is out of scope of this proposal.
* Charges for Complex changes shall be on actual effort estimation basis.
* It's assumed that the listed devices are remotely accessible and manageable. Customer needs to provide access to the in-scope devices.
* It's assumed all the LLD's are updated and will be handed over for operational activities. LLD & Site Architecture details will be provided and signed off by International SOS.
* Software Service Support Contracts are in place and will be handed over to Orange for L4 support from OEM.

* 1. **Modification guidelines**

This document is owned and maintained by Operation manager. Any requests for changes to this document must be provided to Operation manager. Operation manager will update the document, as appropriate. Changes in the document needs to be approved by stakeholders. Until the document is updated, approved, and posted into the [Orange Process Repository](https://orange0.sharepoint.com/sites/OrangeProcessRepository/Shared%20Documents/Forms/AllItems.aspx?viewid=ba51b922%2De20b%2D4a56%2D99af%2D46b1ff34c3cf) (OPR), the existing process must be followed, unless a deviation request has been granted.

* 1. **Deviation request**

It is expected that employees implementing this process will apply their best judgment in every situation to determine the best course of action for the International SOS (International SOS) and the company. This may occasionally require deviation from the approved process.

All deviations must be documented and approved by an Operation manager.

* 1. **References**

The following documents are referenced by this document or contain information necessary for the use of this document:

|  |  |
| --- | --- |
| Document number | Title |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Service management

* 1. **Service support**
* Incident management
* Problem management
* Change management.
* Patch / release management
* Configuration management
* OEM/TPV vendor co-ordination
* Service reporting
  1. **Service management team roles**

|  |  |  |
| --- | --- | --- |
| Role | Name | Email id |
| Customer service Desk | Integrated Customer service desk | [Csdshared.ind@orange.com](mailto:Csdshared.ind@orange.com) |
| L2, L3 team | International Integrator Operations Team | [obs.hyperscalersindia@orange.com](mailto:obs.hyperscalersindia@orange.com) |
| Operation manager | Hiren Tank | [Hiren.tank@orange.com](mailto:Hiren.tank@orange.com) |
| Technical Operations Lead | Pranav Telang | [pranav.telang@orange.com](mailto:Rashmi.sharma@organe.com) |
| Technical Account Director | Ranjit Iyer | [Ranjit.iyer@orange.com](mailto:Ranjit.iyer@orange.com) |

* 1. **Escalation Matrix**

Escalation Matrix of International Integrator

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Escalation Level | Name | Title | Mobile Phone | E-mail address |
| 1 | L2 Operations Team | Cloud Operations Team | - | [obs.hyperscalersindia@orange.com](mailto:obs.hyperscalersindia@orange.com) |
| 2 | Girish Dahibawkar | Shift Lead | 9819938561 | Girish.dahibawkar |
|  |
| 3 | Sahil Sood | SME | 9999458437 | izInternational SOS.cloudsme@orange.com |
| Manish Kumar | 8800099287 |
| 4 | Pranav Telang | Technical Operations Lead | 9052092172 | [pranav.telang@orange.com](mailto:pranav.telang@orange.com) |
| 5 | Hiren Tank | Senior Operations Manager | 9833927771 | [hiren.tank@orange.com](mailto:hiren.tank@orange.com) |
| 6 | Nitin Thakur | Head of Cloud Services Delivery | 9833879809 | [nitin.thakur@orange.com](mailto:nitin.thakur@orange.com) |
| 7 | Bhaskar Banerjee | Head of Service Delivery Management | 8454847441 | [bhaskar.banerjee@orange.com](mailto:bhaskar.banerjee@orange.com) |

Escalation Matrix of Integrated Operations Team (CSD)

|  |  |  |  |
| --- | --- | --- | --- |
| Level | Integrated Operations Team | | |
| Contact Name | Contact info | E-Mail |
| 1 | On Duty Engineer Integrated Ops | From UK to reach the Service Desk +44 (0)207 347 0177 | [csdshared.ind@orange.com](mailto:csdshared.ind@orange.com) |
| PIN: 341009# |
| 2 | Amanpreet Singh Chandpuri | Tel: +91 9643707575 | [amanpreet.chandpuri@orange.com](mailto:amanpreet.chandpuri@orange.com) |
| (Incident Manager-Integrated Ops) |
| 3 | Sanesh Sharma | Tel: +91 99 996 37 788 | [sanesh.sharma@orange.com](mailto:sanesh.sharma@orange.com) |
| (TEM- Integrated Ops) |
| 4 | Davinder BHUTANI | Tel: +91 97 114 99 071 | [davinder.bhutani@orange.com](mailto:davinder.bhutani@orange.com) |
| (Manager Integration Ops) |
| 5 | Kuldeep Aswal | Tel: +91 98 731 73 776 | [kuldeep.aswal@orange.com](mailto:kuldeep.aswal@orange.com) |
| (Head of Integrated Ops) |

* 1. **Delivery and Operations Model**



* 1. **Tools**
* Ocean Tool will be used to work on incident and Machx / SWAN will be used for change tickets.
* Monitoring Tool – cloudwatch will be used to monitor alerts.

|  |  |
| --- | --- |
| Tool Name | Ownership |
| Cloudchecker | Ranjit Iyer and Abhishek Singh |
| Cloudwatch | Ashlesha Mahadik and Rashmi Sharma |
|  |  |

* 1. **Support:**
* English Language Support
* 24 x 7 Remote Support
* Contract Duration: 36 Months
  1. **Inventory:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AWS EU – 16 AWS Accounts | |  | **AWS US – 23 AWS Accounts** | |
| §   **Services** | §   **instance (total)** |  | §   **Services** | §   **instance (total)** |
| §   EC2 (managed OS) | §   120 |  | §   EC2 (managed OS) | §   363 |
| §   CloudFront | §   0 |  | §   CloudFront | §   2 |
| §   RDS (managd-mySQL) | §   23 |  | §   RDS (managd-mySQL) | §   36 |
| §   SNS Topics | §   68 |  | §   SNS Topics | §   689 |
| §   SNS Subscriptions | §   47 |  | §   SNS Subscriptions | §   546 |
| §   Glacier | §   6 |  | §   Glacier | §   8 |
| §   DynamoDB Tables | §   77 |  | §   DynamoDB Tables | §   326 |
| §   SQS | §   14 |  | §   SQS | §   121 |
| §   VPC | §   21 |  | §   VPC | §   211 |
| §   CloudFormation | §   1105 |  | §   CloudFormation | §   4122 |
| §   Route 53 | §   3 |  | §   Route 53 | §   1 |
| §   CloudTrail | §   15 |  | §   CloudTrail | §   17 |
| §   SES | §   1 |  | §   SES | §   40 |
| §   Kinesis | §   8 |  | §   Kinesis | §   11 |
| §   S3 | §   223 |  | §   S3 | §   632 |
| §   Direct Connect | §   1 |  | §   Direct Connect | §   1 |
| §   Certificate Manager | §   31 |  | §   Certificate Manager | §   102 |
| §   Lamda | §   190 |  | §   Lamda | §   2103 |
| §   AWS Config | §   13 |  | §   AWS Config | §   24 |
| §   ELB/AELB | §   53 |  | §   ELB/AELB | §   159 |
| §   Transit Gateway | §   1 |  | §   Transit Gateway | §   1 |
| §   Redshift | §   4 |  | §   Redshift | §   4 |
| §   KMS | §   158 |  | §   KMS | §   348 |
| §   IAM | §   24 |  | §   IAM | §   94 |

Reactive incident management

* 1. **Reactive incident management**

The objective of incident management is to restore normal service operation as per agreed SLO and minimize adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

* 1. **Customer expectations**
* Restore services at the earliest.
* Periodic updates on incident resolution.
  1. **Points of contact**

Customer can raise an incident using Orange ticketing tool or alternatively contact Customer Service Desk CSD on email or phone for logging an incident.

Queue details for Service Desk: EDS queue name – ATQDEL

Point of contacts:

[sanesh.sharma@orange.com](mailto:sanesh.sharma@orange.com)

[pragyat.kulshreshtha@orange.com](mailto:pragyat.kulshreshtha@orange.com)

Intl Integrator Oceane Queues:

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Team** | **EDS Code** | **EDS Group** |
| 1 | AWS /Server Administration (AWS OPS) | ATQC85 | CSO MUM GSI Serv-Mgmt. |
| 2 | Security Administration (SOC) | ATQC87 | CSO MUM GSI SOC-Desk |

* 1. **Roles**

The following roles participate to the execution of this process:

* Customer Service Desk CSD will log incidents reported by International SOS.

1. Integrated desk L1 team will respond to incidents and assign to Orange L2 Operations team.
2. Orange L2 Operations team will provide the resolution of the incidents.
3. CSD would be SPOC for the Customer
4. CSD will route the Incident/ ticket logged by International SOS IT Service Desk to International Integrator Team via Oceane to International Integrator Queue (ATQC85) for the resolution process.

* Orange Business will interwork with:

1. OEM for escalations or Third-Party Vendor (if International SOS engaged)
2. Assumption that vendor maintenance coverage in place.
3. Orange Account team needs to ensure that Orange CSD Oceane ITSM Tool access is extended to International Integrator.

* IntlSOS Business line users can send incident to CSD via email or phone post which CSD will create an Oceane ticket and assign it to the L2 queue.
* If Business line users creates ticket in ServiceNow, it generates a ticket in Ocean tool via ebonding which CSD will intercept and assign to Orange L2.
* L2 Operations Team gets tickets directly in Ocean vie monitoring tool. After receiving ticket directly, L2 will initiate email conversation including issue & true sight ticket details to Customer and CSD. L2 request CSD to open a ticket for the same. Then once CSD opens new ticket & assigns to L2 for resolution, true sight ticket will be closed by L2 Operations Team
  1. **SLO Measurements**

The following table gives the Service Level Objectives

Response Time: It is measured from the time when an Incident is logged to the time when support technician in charge of Incident diagnostic is assigned to the Incident.

Resolution Time: It is the time taken to resolve an Incident on the service from the time the Incident occurred to the time the Incident is resolved.

* MTTR doesn’t include time to arrange for Field Engineer on site and delivery of the spare on site.
* In case of SLO Violation, There is no Penalty (Service Credit) Applicable to Orange International Integrator
* The above Resolve times relate to 1st and 2nd line support only. Where it is identified that 3rd line support is required, then the Core System SLA Measurement shall change to Management decision.

**Incident SLA:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Priority | Description | Examples | Customer Acknowledgements | Customer Resolution |
| Priority 1 | Emergency  Incident | AWS Services down, single point of failure, site security breach, etc. | Initial acknowledgement within 15 minutes and at status change thereafter (e.g., completion) | Resolution within 4 hours  (unless triaged to another MSP provided service or third party). |
| Priority 2 | Business critical Incident | Site degradation not related to single point of failure, suspected security vulnerability, etc. | Initial acknowledgment within 30 minutes and at status change thereafter (e.g., completion) | Resolution within 12 hours  (unless triaged to another MSP provided service or third party) |
| Priority 3 | Important Incident requiring action within 24 hours | Preventive work, such as restarting servers, user security changes, and Access Control List changes | Initial acknowledgement within four hours and at status change thereafter (e.g., completion) | Resolution within 24 hours  (unless triaged to another MSP provided service or third party) |
| Priority 4 | Non-service affecting incident or service requests | Request for Information, reports, documentation, | Initial acknowledgement within eight hours and at status change thereafter (e.g., completion) | Resolution time determined on a case-by case basis. |

* 1. **Case entrance criteria**

When reporting an incident, either on the telephone or via email Customer Service Desk CSD shall gather below information from Customer as listed below.

* Impacted site name:
* Issue description (in detail):
* Issue starts date & time (in CET):
* Impacted VLAN(s):
* Source MAC address (for network):
* Destination MAC address (for network):
* Was it working earlier?
* Characteristic of issue (constant / intermittent / specific time of the day):
* Are you aware of any recent change on this site (that might have caused this issue)?
* Other technical details that can help in quicker troubleshooting: (for network):

Source IP

Destination IP

Ping

Traceroute (source to destination)

Reverse traceroutes (destination to source)

* 1. **Process flow**
* Business line users whenever, if there is an incident that needs to be reported, business line uses, or business unit users can directly send via e-mail or phone call.
* Users send incident report in attached format to L1 service desk in the service management template. So, it's a form that ITSS / users or business line can fill up and send it to L1 service desk so they can do it by e-mail or by phone call & L1 service desk will then create an ocean / SWAN ticket and if it is for security, they will assign it to security. If it is for cloud, they will assign it to Cloud team.

Incident request form:



* 1. **US - Interim Service Engagement Model (until e-bonding)​**

The following flow chart illustrates this process

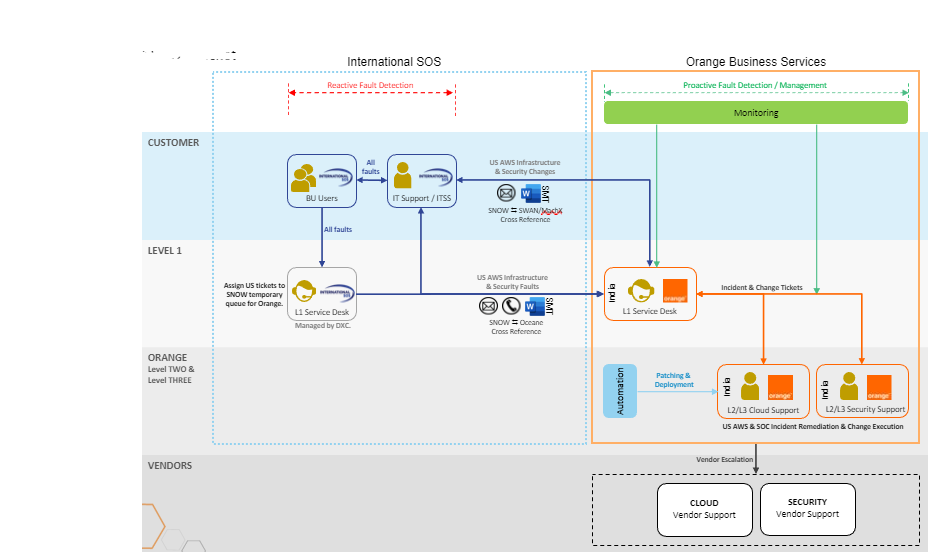


* 1. **When users are fully following the Interim Process**​



**US - Interim Service Engagement Model (until e-bonding)**

When users submit SNOW ticket:



* 1. **Procedure**

This process contains the following tasks:

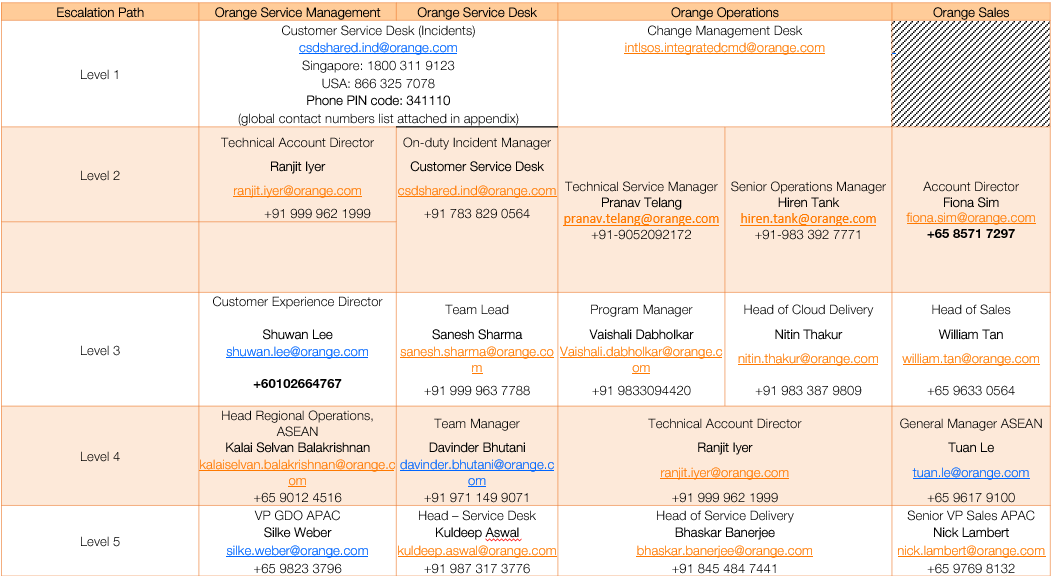
|  |  |  |
| --- | --- | --- |
| Sr No | Activity | Actors |
| 1 | Raise incidents in SNOW tool or contact Customer Service Desk CSD for incident creation | Customer team |
| 2 | Create incident in Oceane tool | Customer Service Desk CSD |
| 3 | Classify incident in Oceane tool | Customer Service Desk CSD |
| 4 | Respond and assign incident to Orange L2 Operations team | Customer Service Desk CSD |
| 5 | Perform troubleshooting | Orange L2 Operations |
| 6 | Consult OEM if required | Orange L2 Operations / Service Desk (depending upon the vendor) |
| 7 | Follow up with Customer to gather more information from Customer | Customer Service Desk CSD |
| 8 | Implement solution | Orange L2 Operations |
| 9 | Update Oceane tool ticket and assign to Customer Service Desk CSD | Orange L2 Operations |
| 10 | Obtain resolution confirmation | Customer Service Desk CSD |
| 11 | Confirm incident resolution | Customer team |
| 12 | If issue is not resolved reassign incident to Orange L2 Operations | Customer Service Desk CSD |
| 13 | Close incident in Oceane tool | Customer Service Desk CSD |

* 1. **RACI matrix**

Refer to the RACI Matrix for Incidents.



* 1. **Escalation matrix**



Logistics & Contacts for International SOS Customer to log incident

For AWS Landing Zone Changes, below are the contact details of teams rendering support as per the interim engagement model.

Please submit changes via email to the service desk with account id and landing zone details in the Service Management template.

|  |  |
| --- | --- |
| Customer Name: | International SOS |
| Customer Code: | 681885 |
| Orange business Team Name: | L1 Service Desk |
| Location of Designated Team: | Gurgaon – India Major Service Centre |
| Oceane Queue ID (EDS): | ATQDEL (for Orange internal use only) |
| Email: | [csdshared.ind@orange.com](mailto:csdshared.ind@orange.com) |

Vendor Management

Vendor Management:

* International Integrator detects AWS portal Faults after the Root Cause Analysis and engage with Third Party Vendor for further analysis of fault if required.
* Orange business will provide co-ordination support for Next level of support with OEM.
* The responsibility of procuring and managing the OEM maintenance contract is with Orange Account team or International SOS.

Problem management

* 1. **Description**

Orange Business Problem Management process seeks to reduce the number of tickets causing service failures by detecting the root cause of recurrent failures and implementing the proper changes to eliminate, minimize the possibility of further failures or minimizing the impact of tickets.

* 1. **Customer expectations**
* Investigation and diagnosis of major incidents and recurring incidents
* Prevention of recurrence of incidents
  1. **Points of contact**

Customer can request Operation manager for creation of problem ticket.

* 1. **Roles**

The following roles participate to the execution of this process:

* Technical Lead – Technical Lead will inform Customer Service Desk CSD to log problems reported by Customer team.
* L2, L3 team – Orange L2 Operations team will prepare the RCA and implement the corrective and preventive actions.
  1. **Entry criteria**

Problem ticket will be created for below mentioned criteria.

* Major Incidents
* Critical issues closed with workaround.
* Recurring issues identified in trend analysis.
* Potential issues identified by Orange L2 Operations team.
* Failed changes with business impact
  1. **Inputs**

The following inputs may be required for this process:

* Major incident report
* Recurring incident identified in trend analysis.
  1. **Tools**

The following tools will be used during this process:

* Ticketing tool
  1. **Measurements**

Root cause analysis (RCA) will be sent to Customer as per below timelines.

P1 – 1 week. P2 – 2 weeks P3 – 3 weeks

* 1. **Procedure**

|  |  |  |
| --- | --- | --- |
| Sr No | Activity | Actors |
| 1 | Trend analysis of incidents and problem management process trigger by major incident | Problem manager |
| 2 | Creation of problem ticket in ticketing tool and assign it to International Integrator queue for investigation and root cause analysis. | Problem manager |
| 3 | Orange L2 Operations team can request creation of problem ticket to Problem Manager which will be assigned to Orange L2 Operations queue by Problem Manager. | Orange L2 Operations |
| 4 | Low priority problem ticket will be created by Problem Manager. Orange L2 Operations team can change the priority of the problem ticket based on the business impact. | Problem manager & Orange L2 Operations |
| 5 | Co-ordinate with Orange L2 Operations team to investigate the problem and prepare solution plan for the in-scope problem tickets and register the action plan | Problem manager |
| 6 | Provide detailed RCA in 5 business days. | Orange L2 Operations |
| 7 | The Orange L2 Operations team is responsible for providing the root cause to the Problem Manager for the in-scope problem tickets via email or attaching in problem ticket in ticketing tool. | Orange L2 Operations |
| 8 | Orange L2 Operations team will connect with Customer for any assistance from vendor during problem investigation and diagnosis. | Orange L2 Operations |
| 9 | Problem Manager can have periodic RCA call with Orange L2 Operations team for discussion and progress on RCA. | Orange L2 Operations Problem manager |
| 10 | Present the Root Cause Analysis report to Customer IT team. | Problem manager |
| 11 | Track open Corrective and Preventive Actions identified during Root Cause Analysis. | Problem manager |
| 12 | Target date of Corrective Actions and Preventive Actions shall be discussed and agreed during RCA call with Customer. | Orange L2 Operations Problem manager, Customer |
| 13 | Create change ticket in ticketing tool through Change Management Process for implementation of Corrective and Preventive actions approved by Customer. | Problem Manager |
| 14 | Implement the change ticket (corrective and preventive actions). | Orange L2 Operations |
| 15 | Post implementation of Corrective Actions and Preventive Actions problem ticket will be kept under observation for at least 2 weeks to maximum 1 month. | Problem manager |
| 16 | Problem Manager would collect improvement action result and present to Customer for final approval or problem closure | Problem manager |
| 17 | Problem Manager will have a weekly call with Orange L2 Operations team to discuss open RCA and status of improvement actions. | Problem manager, Orange L2 Operations |

* 1. RACI matrix

Refer to the RACI Matrix:



Change Management

* 1. Description

A change is the addition, modification, or removal of anything that can have an impact on

IT services.

Change management process is responsible for controlling the lifecycle of all changes.

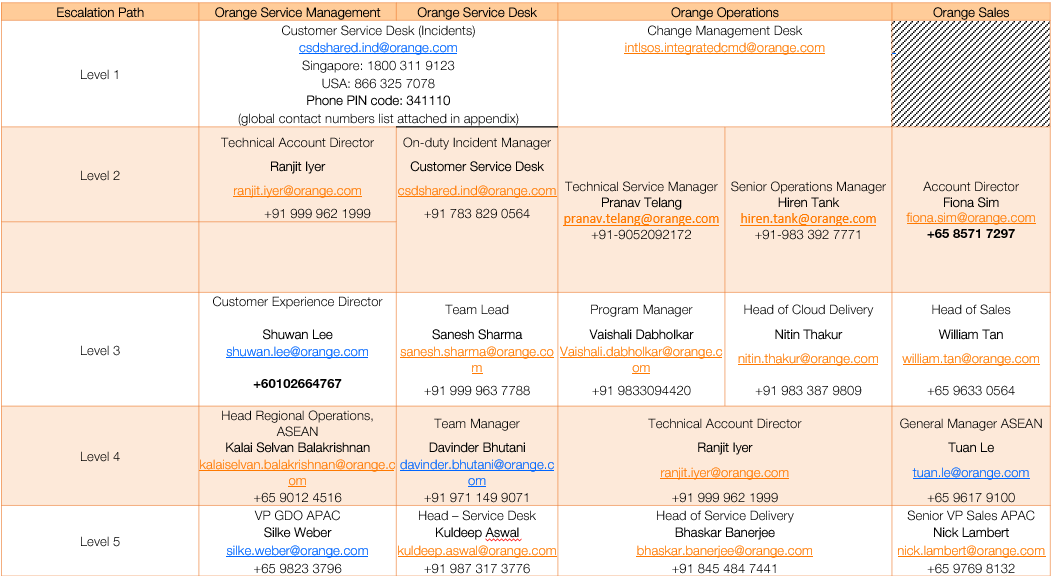
and enabling beneficial changes to be made with minimum disruption to IT services.

* Change Management will follow to those changes which are defined in the service catalogue as Simple Change (Standard Change) or those which are triggered as part of solution to fix the Incident/Problem
* Change Catalogue will be always get referred to identify whether it is standard or complex change.
* Normal changes will go through a CAB process.
* Any non-standard or complex change request for change submitted to Orange will be reviewed for both technical and commercial impact by Technical account manager.
* Managed Services include minor Moves, Adds & Changes (MACD), which are defined by an activity or tasks that require less than 4 hours of engineering work per request**. Any work over 4 hours will need to be explicitly approved by Orange Customer change advisory and may lead to additional charge**. This must be reviewed by Technical account manager and Orange operational management.
  1. Customer expectations
* Minimum risk and impact on business caused by a change.
* Standard procedure for managing changes.
  1. Tools:
* Machx tool used for change management for SOC Operations.
* SWAN tool will be used for change management for AWS Operations.

Orange L2/L3 Change Queues:

|  |  |  |  |
| --- | --- | --- | --- |
| # | Team | Tool | Change Management Tool |
| 1 | AWS Cloud Operations | SWAN | ATQC85 - CSO MUM GSI Ser-Mgmt |
| 2 | Security Administration (SOC) | Machx | SOC-GSI |

* 1. Escalation Matrix:



* 1. Entry criteria:

The entry points for a request for change are as follows:

* iCare (Service Now) after e-bonding
* The Orange Service Desk
* Technical Account Manage
* The list of persons authorized to submit requests for change is updated by International SOS and addressed to the Customer Service Center or to the Technical Account Manager.
* If the request for change is originated by Orange, the Customer's explicit agreement is sought before implementation can begin. An exception will be made to this procedure where the change was required in response to an Incident of Priority level 1, as defined in the Service Level Agreement. In that event, Orange notifies the Customer as promptly as possible following implementation of the change.

Interim model for Change Management Operations for AWS

Attached form is used currently to fill and send to customer to log a change request as interim change management process.



The following roles participate to the execution of this interim process:

* Customer/Business Lines – Customer will log changes via email to Orange CMD team. If the change is requested from Business Lines, they will require approval from ITSS Team to log the change. Change requests should not be accepted from Business line users directly, they should come from ITSS Cloud Ops team.

ITSS Cloud Services <DL.GLB.ITSSCloudServices@internationalsos.com>

* Orange CMD team – Orange CMD will log changes once approval received from ITSS team with implementation details from the CR form attached.

Orange CMD can further create a change ticket based on whether it is for SOC or AWS OPS.

* Orange L2/L3 Team – Orange L2/L3 team will review the change.

If it is a standard change, Orange L2/L3 team will implement the change.

If it is a non-standard or complex change Orange L2/L3 Team to review the change with ITSS Cloud Ops Team.

Once the changes are approved by ITSS Cloud Ops Team, L2/L3 Team to implement and close the change.

* Technical Account Manager- If the change has commercial impact and if it takes more than 4 hours to implement, Technical Account Manager will further review the changes with ITSS Cloud Ops team.
* Change Manager – Accountable for overall change management process, represent changes in CAB meetings and maintain change catalogue. Post implementation review the changes and document lessons learnt.
  1. Types of changes

The following types of changes will be used in this process:

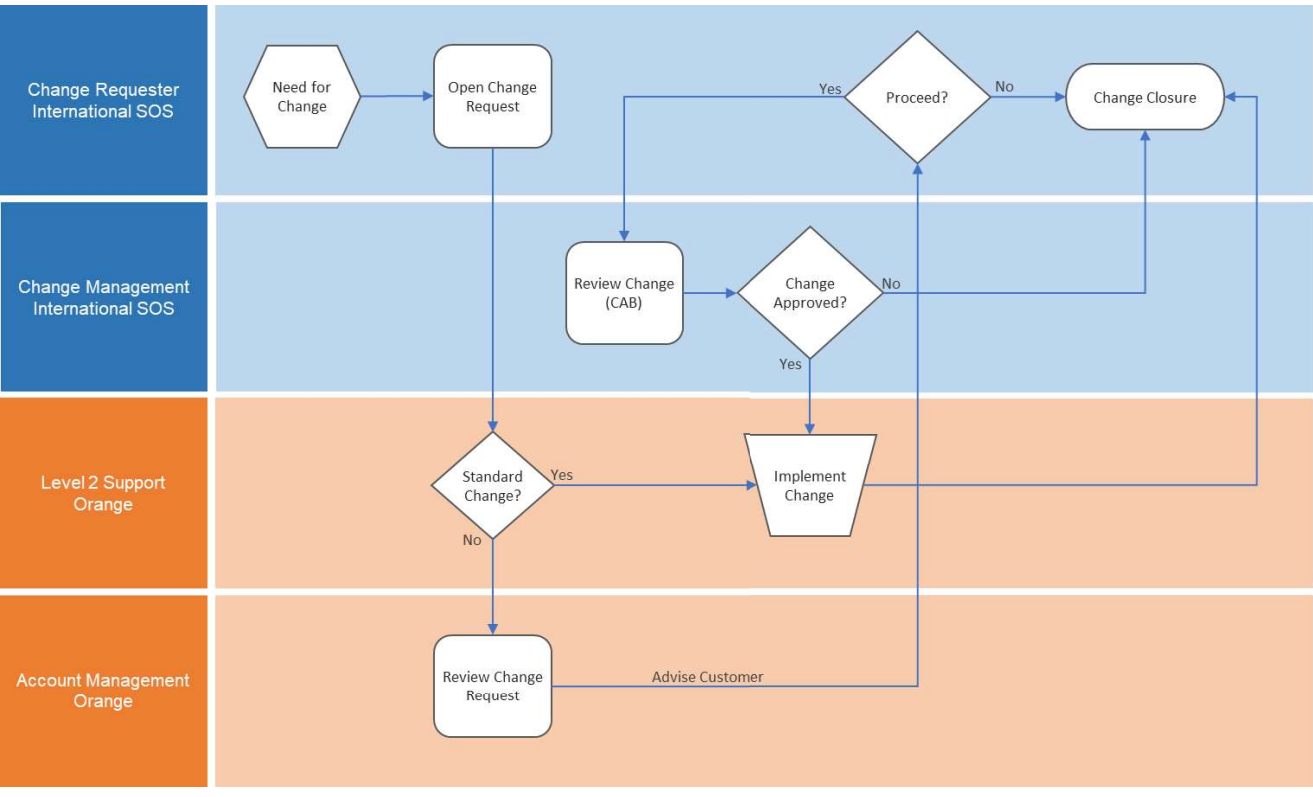
* Standard Change: A standard change is a pre-authorized change that is low risk, relatively common and follows a specified procedure or work instruction.  
  A standard change is one that is frequently implemented, has repeatable implementation steps, and has a proven history of success. As Standard changes are pre-approved, they follow a streamlined process in which group level or peer approval and CAB authorization steps are not required.
* Orange provides a list of standard changes below. This is a dynamic list, and additions/removals may be made to the list as per business requirements in the run phase.
* Change Catalogue will be referred to identify whether it is Standard change or non-standard change.
* Standard change should be raised 4 days in advance.
* Emergency change can be raised only if a change is required to fix a severity 1 or severity 2 incident.
* Normal change will follow CAB process.

Change catalog:



* 1. Process flow

The following flow chart illustrates this process:



* 1. Procedure:

|  |  |  |
| --- | --- | --- |
| Sr No | Activity | Actors |
| 1a | Change requested by Customer by email sent to Orange CMD Team | ITSS |
| 1b | Change requested by Customer will be raised in ticketing tool by Orange CMD | Orange CMD |
| 2 | Review the change requested by Customer for change categorization (standard/non-standard) changes | Orange L2 Operations |
| 3 | If it is a Standard Change, it will be implemented Orange L2 Operations. | Orange L2 Operations |
| 4a | If it is a non-standard change, Orange L2 Operations to review the change with the ITSS Cloud Ops Team & Technical account manager | Orange L2 Operations |
| 4b | If the change has a commercial impact or if it takes more than 4 hours to complete, Technical Account Manager to review the change with ITSS Cloud Ops Team. | Technical Account Manager |
| 5 | ITSS to review and approve the changes | ITSS |
| 6 | Post approval from ITSS, Orange L2 Operations to implement the change | Orange L2 Operations |
| 7 | Orange L2 Operations to update the change and close the change request in the tool post implementation. | Orange L2 Operations |

* 1. RACI matrix

Refer to the RACI Matrix uploaded on below path:



* 1. Maker & Checker process (4 Eye process)

• Cloud operations support team will follow maker & checker process

• Cloud operations team member will perform change activity while peer in shift will review/validate activity performed

Patch & Release management

* 1. Description

Patch management is the process of distributing and applying updates to system. These patches are necessary to fix bugs in the system.

Patch management is the process of planning and deploying software and security updates, or patches, to Operating System. Patches are updates that are designed to fix security vulnerabilities, and software bugs, and improve the performance of Operating System.

Orange ensures that maintenance windows are planned in collaboration with International SOS. Orange Cloud

to be deployed to the systems. International SOS will then approve the deployment of patch update.

The customer’s development/application/database support teams will participate in the patch deployment activity by conducting necessary validation tests of customer managed services.

In the event of a failure during patch deployment, International SOS will be notified, and Orange cloud operations will perform the necessary investigation to address the issue.

In an event of having high priority security patch released by the OEM, the Cloud Operations Lead will work with the customer to schedule a window to have these priority patches deployed.

Orange is going to use AWS Systems Manager Patch Manager service to do patching for all the EC2 instances (Windows & Linux) as per patching calendar provided by International SOS.

* 1. Customer expectations
* Increased security and reduced risk.
* Better system uptime
* Compliance to standards
* System robustness
  1. Points of contact

Customer can get the all the information related to patching activities by contacting Patch Manager.

Name: Satish Agrahari

Email Id: [Satish.agrahari@orange.com](mailto:Satish.agrahari@orange.com)

Contact number: +91 9322404020

* 1. Roles

The following roles participate to the execution of this process:

* **Orange L2 Operations** – International Integrator resolver group will implement the patch on the system after consultation with change manager.
* **Vendor** – Vendor will provide the newly released patch details to International Integrator resolver group.
* **Patch manager** –
* Raise standard change request for patch implementation.
* Schedule all patching related meetings and coordinate with application teams.
* Organize meeting with SMEs/Ops team to review and update runbook.
* Sent Maintenance notification for patching activities for all the environments.
* **ITSS** – To govern the overall patch management process.
* **Business line / Application Team**: To test the applications after the patching is implemented.
  1. Entry criteria

Orange L2 Operations group will act upon patches released by vendor applicable to Customer environment.

Release Management:

* Release upgrade would be classified as below:
  + Minor release upgrade: Patch or release on the same service platform, not enabling any additional feature set to the existing platform.
  + Major release upgrade: Version or release upgrade enabling new feature set on the current service platform.
* International Integrator Patch and Release Management will include any minor patch (require resolving Incident/Problem) released by the OEM which is installed on the running system with International SOS team’s concurrence for the inventory in scope.
* Security related patch/updates recommended by OEM will be executed monthly.
* Major release upgrade will be on T&M basis.
  1. Inputs

The following inputs may be required for this process.

* New patch released by vendor.

1. **Pre-Execution Works/Due Diligence/Planning**

Microsoft releases patches on every second Tuesday of the month. After that this patch will be raised as change and discussed with customer on CAB meeting.

Monthly, a patch pre-scan will be performed by the International Integrator CloudOps team to identify the in-scope servers that will need patching. Additional patching requirements can be identified via the below mentioned triggers.

**Patching Triggers**: Deployment of a patch can be triggered by different reasons.

* To fix a security issue.
* To resolve a software error (stability of releases)
* To close a feature gap or enable a new feature.
* Monthly patch release by OEM

**Release of MS Patching**: Every second Tuesday of every month MS patches are released by Microsoft.

**Release of UNIX Patching**: There is no specific date for the Linux patch release. As per best practice, Linux patching will be carried out on monthly basis. Linux Patching will get aligned at start of each quarter with that months MS patching Cycle.

**Patching Assessment**: The servers identified during the monthly pre-scan along with the missing patch details will be provided to the customer.

**Patch Level Report**: The servers identified during the monthly pre-scan along with the missing patch details will be part of Patch Level Report. The Patch Level Report will have information of all patches available for the in-scope servers that are available to patch. In addition, it will also provide information on the patching versions that are available.

**Patching Runbooks Review:** Patching runbooks to be reviewed and tasks to be aligned with all the resources for the patching activities.

1. **Pre-Implementation Plan**

**Patch Schedule**: Patch schedule is agreed for the entire calendar year at the start of each year. Change requests will be raised for each group of Servers as per agreed dates. Servers which are in power down condition will miss the current patching cycle and will be covered in the next monthly cycle of patching.

Patching will be conducted by following annual patch calendar which is discussed and agreed with Customer.

Below is the Annual Patching calendar which is already agreed with Customer and Business Lines for 2023.



For time-to-time Customer may requests change freeze and patching will be halted for a particular duration.

Patching Templates: [GLB.ITSS.CloudServices - Patching Templates - All Documents (sharepoint.com)](https://internationalsosms.sharepoint.com/sites/GLBITSSCloudServices/Shared%20Documents/Forms/AllItems.aspx?csf=1&web=1&e=MTZ9ZC&cid=e3684f15%2Df13d%2D4a16%2Dbfd5%2D0fc26b41cd62&FolderCTID=0x0120004BA5AF59AFAE114982A364515D8C2437&id=%2Fsites%2FGLBITSSCloudServices%2FShared%20Documents%2FGeneral%2FPatching%2FPatching%20Templates&viewid=14a24c73%2D5079%2D426b%2D8f8e%2De76d995bde9a)



**Patching Communication**: As per the patching calendar

1. Dev environment- Email communication to be sent to ITSS & Business Lines for the upcoming Dev patching activity on Wednesday.
2. Stage environment- Email communication to be sent to ITSS & Business Lines for the upcoming Stage patching activity on Monday.
3. Production environment- Email communication to be sent to ITSS/IT Service Desk for the production patching activity on Monday.

|  |  |  |  |
| --- | --- | --- | --- |
| **Environment** | **Day** | **Communication list** | **Notes** |
| **Dev** | **Second Wednesday of the month** | **ITSS & Business owners** |  |
| **Stage** | **Third Monday of the month** | **ITSS & Business owners** |  |
| **Production** | **Fourth Monday of the month** | **ITSS & IT Service Desk** |  |

**Communication details:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Env** | **Communication** | **Who** | **To** | **Attachment  links** | **Reports** |
| DEV/QA | T-5 | Patch Manager | Contact Matrix | Contact Matrix | [GLB.ITSS.CloudServices - Patching Templates - All Documents (sharepoint.com)](https://internationalsosms.sharepoint.com/sites/GLBITSSCloudServices/Shared%20Documents/Forms/AllItems.aspx?csf=1&web=1&e=MTZ9ZC&cid=e3684f15%2Df13d%2D4a16%2Dbfd5%2D0fc26b41cd62&FolderCTID=0x0120004BA5AF59AFAE114982A364515D8C2437&id=%2Fsites%2FGLBITSSCloudServices%2FShared%20Documents%2FGeneral%2FPatching%2FPatching%20Templates&viewid=14a24c73%2D5079%2D426b%2D8f8e%2De76d995bde9a) |
| DEV/QA | T-3 | Patch Manager | Contact Matrix |
| DEV/QA | T-1 | Patch Manager | Contact Matrix |
| DEV/QA | Patching Start | Patch Manager | Contact Matrix |
| DEV/QA | Interim Update | Patch Manager | Contact Matrix |
| DEV/QA | Patching Completion | Patch Manager | Contact Matrix |
| STAGE | T-5 | Patch Manager | Contact Matrix |
| STAGE | T-3 | Patch Manager | Contact Matrix |
| STAGE | T-1 | Patch Manager | Contact Matrix |
| STAGE | Patching Start | Patch Manager | Contact Matrix |
| STAGE | Interim Update | Patch Manager | Contact Matrix |
| STAGE | Patching Completion | Patch Manager | Contact Matrix |
| PROD | T-5 | Patch Manager | ITSD |
| PROD | T-3 | Patch Manager | ITSD |
| PROD | T-1 | Patch Manager | ITSD |
| PROD | Patching Start | Patch Manager | ITSD |
| PROD | Interim Update | Patch Manager | ITSD |
| PROD | Patching Completion | Patch Manager | ITSD |

**Patching bridges**- Patching bridges invites to be sent to the business lines and application teams in alignment with the patching calendar in the beginning of the year, for the patching activity for Stage and Production.

Sharepoint Link-[GLB.ITSS.CloudServices - Patching - All Documents (sharepoint.com)](https://internationalsosms.sharepoint.com/sites/GLBITSSCloudServices/Shared%20Documents/Forms/AllItems.aspx?csf=1&web=1&e=MTZ9ZC&cid=e3684f15%2Df13d%2D4a16%2Dbfd5%2D0fc26b41cd62&FolderCTID=0x0120004BA5AF59AFAE114982A364515D8C2437&id=%2Fsites%2FGLBITSSCloudServices%2FShared%20Documents%2FGeneral%2FPatching&viewid=14a24c73%2D5079%2D426b%2D8f8e%2De76d995bde9a)

**Raising a Change**: All patching changes will be raised as standard changes and informed to the change manager. For each account, a change ticket will be raised 5 to 10 days prior to the schedule window. All patching runbooks and change details will be provided to the International SOS change manager.

1. **Implementation Plan**

**Patch Deployment**: A high-level overview of the OS Patching Deployment Process is portrayed in the diagram below.

Review Patch Level Report

Patch Release

Approve Change for Dev Patch

Raise change for Dev Patc

Pre-scan Dev environment

Deploy Patches in Dev

Deploy Patches in Stage env

Approve Change for Stage env.Patch

Raise change for Stage

App Testing & Customer Review

Raise Change for Prod Patch.

App Testing & Customer Review

Deploy Patches Prod env

Approve Change for Prod

App Testing & Customer Review

Update Runbooks

Client Review

Prepare Compliance Dashboard

High Level OS Patch Deployment Process

As per best practice, patching is always carried out starting from less critical environment starting with Dev environment and moving to the most critical environment (Stage and Prod) to minimize the impact of any patching related outages. Patching will be implemented in the maintenance window in alignment with the the patching calendar.

**Communication will be sent out to customer before the start of the patching activities**.

**Patching bridge will be opened during the patching window for stage and production environment**.

* Patch Manager:  Share screen and present the runbooks and update online status, record issues, inputs, and updates for reference (issues reported by application team etc)

After completion of patching activity, Summary of the patching activity will be shared with the ITSS and Business lines (Updated patching runbooks and installed missing patch list with compliance report will be shared through meeting invite on share-point) [GLB.ITSS.CloudServices - Patching - All Documents (sharepoint.com)](https://internationalsosms.sharepoint.com/sites/GLBITSSCloudServices/Shared%20Documents/Forms/AllItems.aspx?csf=1&web=1&e=MTZ9ZC&cid=e3684f15%2Df13d%2D4a16%2Dbfd5%2D0fc26b41cd62&FolderCTID=0x0120004BA5AF59AFAE114982A364515D8C2437&id=%2Fsites%2FGLBITSSCloudServices%2FShared%20Documents%2FGeneral%2FPatching&viewid=14a24c73%2D5079%2D426b%2D8f8e%2De76d995bde9a)

* Type major points, decisions in Teams channel chat to keep audit trail.

**Emergency/Out of Cycle Patching**: In cases where a critical security vulnerability is notified and requiring deployment of an emergency patch or as the result of a major incident requires a patch, the Emergency / Out of cycle patching process is triggered by a Severity 1 or Severity 2 incident being logged by either Client or Orange Cloud team. An emergency patch request will be completed based upon customers approval and will follow the Emergency Change Management process by submitting a change request.

In addition to a client request, the notification of an emergency change may come from a third-party vendor, or from the Technical Account Manager (TAM).

The Patch Manager is responsible for calling an emergency session for an out of cycle meeting. The authority to proceed can only be given during the meeting. During this meeting an out of service maintenance window will need to be agreed with customer.

1. **Post Patching:**

A post patching scan is done to confirm that a patch has been performed successfully and will show the current level of patches installed on the server as well as health of the Server.

Patching summary to be send in the patching bridge invite after completion of the activity by Patch manager.

Patching summary should contain the following information.

1. Contributors in the patching exercise (Orange, ITSS, Business Lines, DBA team, QA teams)
2. Accounts patched with timings.
3. SharePoint link to the updated runbooks with actual timings
4. SharePoint link to the compliance reports.
5. SharePoint link to the known issues/encountered issues.

In the compliance report (Item 4 above) the following pieces of information must be included:

* Installed Patch list.
* Compliance Dashboard.
* Exception report for excluded patches.

The Sharepoint path for Patching:

[GLB.ITSS.CloudServices - Patching - All Documents (sharepoint.com)](https://internationalsosms.sharepoint.com/sites/GLBITSSCloudServices/Shared%20Documents/Forms/AllItems.aspx?csf=1&web=1&e=MTZ9ZC&cid=e3684f15%2Df13d%2D4a16%2Dbfd5%2D0fc26b41cd62&FolderCTID=0x0120004BA5AF59AFAE114982A364515D8C2437&id=%2Fsites%2FGLBITSSCloudServices%2FShared%20Documents%2FGeneral%2FPatching&viewid=14a24c73%2D5079%2D426b%2D8f8e%2De76d995bde9a)

**Logging a Patching Issue**: In the event of an issue being identified with any patch, Orange will contact the Vendor as appropriate for further analysis. A knowledge base article will be created in tool for the issues encountered after the vendor provides a resolution and mapped to the Client or the Company Name.

If a particular patch needs to be excluded or uninstalled from the server to remediate an encountered issue during patching activity, Orange will notify ITSS team to get an exception approved.

**Patching Exclusion Process**: If any server needs to be excluded from the current patching cycle, Business lines to secure exception approved from ITSS. If in the next month, the same server needs to be excluded, ITSS/Business Lines needs to secure approval from International SOS INFOSEC team.

* 1. Tools

AWS Patching Manager is the Cloud Native tool used for patching the Windows and the Linux Estate in AWS environment.

Orange team apply patches through a run command in AWS system manager using AWS-RunPatchBaseline

**PATCH BASELINE:**

|  |  |
| --- | --- |
| **OS Name** | **Patch Baseline Name** |
| Windows / Linux | AWS-RunPatchBaseline |

* 1. Process Flow



* 1. Patch Management RACI matrix

Refer to the RACI Matrix:



Configuration Management -TBC

8.1 Introduction

Service Asset & Configuration Management process provides the details of the process and the stakeholders involved that shall use this process.

The primary target audience:

* Assistant Manager
* Operations Manager, Configuration Manager
* Support Analysts (L1, L2 & L3)
* Configuration items are stored in Customer Provided SharePoint or AWS portal.
* Customer has to define the backup storage path, mechanism & ensure availability of those backup to Orange business as on when requires.

RACI Matrix TBC

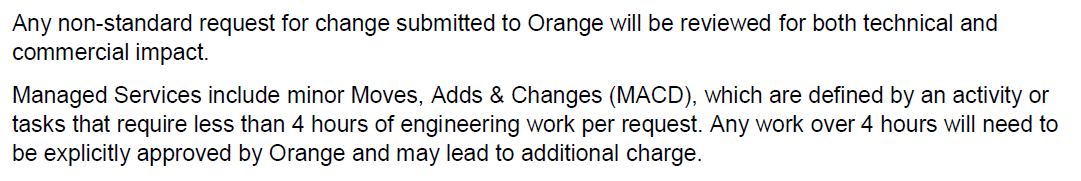
Refer to the RACI Matrix uploaded on below path:

[International SOS Process Documents](https://orange0.sharepoint.com/:f:/r/sites/IntlSOSAWSUSLZDelivery/Documents%20partages/General/International%20SOS%20Process%20Documents?csf=1&web=1&e=fXJbpt)

1. Major Incident Management Process

* ITSS team/Business Lines report the issue on Email/Teams chat. (If InternationalSOS are reporting issue on teams chat then OBS Cloud L2 engineer should acknowledge the chat and immediately join the call.
* L2 team engage CSD team via email and request tom raise reference ticket and share the bridge details if required.
* L2 team to inform internal stakeholders (Shift Lead, Technical Lead, Operations Manager) about the ongoing P1.
* CSD team raises P1 Incident ticket for Cloud L2 team.
* CSD team will initiate the bridge with ITSS, Business Line and L2 team.
* L2 team will perform investigation, diagnosis and identify resolution to restore the service.
* After confirmation received from ITSS and Application team CSD team will close the bridge.
* Once issue will get resolved Cloud L2 engineer will send technical investigation summary email to CSD and ITSS.
* Cloud Ops L2 team will update the ticket with their findings and move ticket in CSD queue for closure.
* Responsible team will prepare the RCA.

1. Project Work Process

* SMEs & Technical operations lead to identify/analyze request from Intl.SOS for any non-standard change request which require additional efforts (Project work).
* Refer below snap from SOW to categorize non-standard request.
* 
* SMEs/Technical operations lead to highlight new request (project work) with Technical Account Manager (TAM), Operations Manager & Nitin Thakur.
* TAM to discuss new project work with Intl.SOS for confirmation/agreement on commercial change request.
* Upon confirmation of commercial change from Intl.SOS & TAM; SME will prepare level of efforts (LOE) for the project work and share with Operations manager.
* Operations manager to initiate process to generate SRF.
* Once SRF is approved; SMEs/L2 operations team would proceed with implementation of project work.
* Inform stakeholders after completion of project work.

11 Service Level Reporting

* Orange Business will provide reporting (Details of incidents opened and status) on Incidents/changes-based Oceane tool.
* Manual Capacity and Performance parameters related reports would be shared by Orange Business (Optional Scope)
* Reports will be shared to the International SOS by e-mail through Orange TAM
* Orange Business Operations Team will help Orange TAM for providing the reports to the International SOS.
* Report Generation is possible within first 10 days of the month.

1. Glossary
   1. Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| OPR | Orange Process Repository |
| SLO | Service Level Objective |
| RACI | Responsible, Accountable, Consultant, Informed |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

* 1. Terms

|  |  |
| --- | --- |
| Term | Definition |
| Deviation | An approved variance from an approved process document |
|  |  |
|  |  |
|  |  |

* 1. Additional documents

|  |  |
| --- | --- |
| Document name | Attachment |
| Change and service request catalog |  |
| RCA template |  |
| RACI Matrix for NOC team |  |
| SOW |  |
| RACI Matrix |  |
|  |  |
| Any Email |  |
| Document approval sign off email |  |
| Device inventory |  |
| Patch calendar | [GLB.ITSS.CloudServices - Patching - All Documents (sharepoint.com)](https://internationalsosms.sharepoint.com/sites/GLBITSSCloudServices/Shared%20Documents/Forms/AllItems.aspx?csf=1&web=1&e=MTZ9ZC&cid=e3684f15%2Df13d%2D4a16%2Dbfd5%2D0fc26b41cd62&FolderCTID=0x0120004BA5AF59AFAE114982A364515D8C2437&id=%2Fsites%2FGLBITSSCloudServices%2FShared%20Documents%2FGeneral%2FPatching&viewid=14a24c73%2D5079%2D426b%2D8f8e%2De76d995bde9a) |
| Patch Runbooks | [GLB.ITSS.CloudServices - Patching - All Documents (sharepoint.com)](https://internationalsosms.sharepoint.com/sites/GLBITSSCloudServices/Shared%20Documents/Forms/AllItems.aspx?csf=1&web=1&e=MTZ9ZC&cid=e3684f15%2Df13d%2D4a16%2Dbfd5%2D0fc26b41cd62&FolderCTID=0x0120004BA5AF59AFAE114982A364515D8C2437&id=%2Fsites%2FGLBITSSCloudServices%2FShared%20Documents%2FGeneral%2FPatching&viewid=14a24c73%2D5079%2D426b%2D8f8e%2De76d995bde9a) |
| Incident request form |  |
| Change Request Form |  |
| Email communication Matrix |  |