# Reviewing the Daily SLA Report Procedure

Service Level Management

**Purpose**

The SLA Report is ran and reviewed daily by Service Level Management so that error minutes for monitored services can be investigated in a timely manner. Error minutes indicate an issue in which an SLA may be missed or breached, or the monitor that is checking the SLA is not working correctly. An investigation incident ticket is created and research is performed to identify the cause.

**Related Policy**

* [IT Service Management Policy](https://sharepoint.jackson.com/sites/integrity/_layouts/15/WopiFrame.aspx?sourcedoc=%7be34fe42a-654a-469a-9d38-6612f00486dc%7d&action=view)

**Audience**

The following groups are responsible for adhering to this document:

* Service Level Management

**Procedure**

|  |  |
| --- | --- |
| Step | Action |
| 1 | To create the Daily SLA Report, follow the instructions in the ***SLM Running the SLA Load Utility*** and ***SLA Report Generation Procedure***. |
| 2 | Open the current month’s “SLA Spreadsheet for Month YYYY” located at:  [O:\Service Delivery\Service Level Management\SLA Information\SLA Excell Spreadsheet](file:///O:\Service%20Delivery\Service%20Level%20Management\SLA%20Information\SLA%20Excell%20Spreadsheet)   1. In the spreadsheet, create a new tab. 2. Rename the tab to the current date (example; 10-09).      1. Copy the entire spreadsheet from the Excel report created in the ***SLA Report Generation Procedure***. 2. Paste the data into the new tab that has been created. |
| 3 | Review the SLA Report:   1. The service name, the compliance target percentage and service target days and time frame appear for each service. 2. Examine each service that appears on the SLA Report, paying attention to the “Errors” column. This will show if an SLA is missed or breached. If an SLA is missed or breached, see **Step 4** for the course of action to take.   ***Note:*** *If the “Actual %” is less than 100% but is above the compliance target percentage, the SLA is considered “Missed”. If the “Actual %” is less than the compliance target, the SLA is considered “Breached”.*   1. Ensure that the current date appears on the report for each service. Not all services have an SLA for Saturday and Sunday so those days may not be present on the report. |
| 4 | Actions to take if an SLA is missed or breached:   1. Copy the row in which the missed / beached SLA appears. 2. Click on the “Master” tab of the spreadsheet and locate the service that is showing a missed / breached SLA.      1. Paste the row under the correct service that had a missed / breached SLA. 2. Highlight the “Comments” section in yellow to indicate that it is unresolved. 3. Create an Incident Request ticket to investigate the missed / breached SLA.  * Fill in the general information: * **Summary** – Investigate *Service Name* Missed SLA *Date*   *Example: Investigate J2K Missed SLA 01/29/2018*   * **Environment** - Production * **Service** – Use the drop down list to add the service name that is missed or   breached.   * **Notes** – Add the following information in reference to the Missed SLA form   that will be attached (see f) below).  *See attachment for SiteScope Alerts, Details that feed the*  *monitor, research that was performed and General SLA*  *information.*  *Fill out the section in the attachment that is highlighted in blue and*  *Re-attach to this ticket.*  *Missed SLA: SLA is below the 100% goal*  *Breached: SLA is below the Service Target percentage.*   * **Target date** – Fill in the date to be two days away from current date. * **Impact** – 4-Minor/Localized * **Urgency** – 3-Medium * **Priority** – Medium (This will auto populate) * **Incident Type** – User Service Request * **Reported Source** – Direct Input      * In the “Categorization” tab, use the drop down lists to fill in the Operational Categorization information: * **Tier 1+** – Investigate * **Tier 2+** - Application/Service      * In the “Categorization” tab, the Production Categorization will auto-populate based on the service that was selected.      * Click the “Save” button      1. Create a Missed SLA form that will be attached to the Investigation ticket.   See the ***SLM Create Missed SLA Form*** procedure.   1. Attach the Missed SLA form to the Work Detail log of the investigation ticket and request that SIG or JTS complete the section highlighted in blue and re-attach to the ticket. 2. Use the assignee information (above the comment line on the master tab) in the “SLA Spreadsheet for Month YYYY” to assign the investigation ticket to the appropriate SIG or JTS team. |
| 5 | Continue to check the status of the investigation ticket when reviewing the Daily SLA Report:   1. If the investigation ticket is not resolved within two business days, send an email to the group, the group’s manager, and SLM Management. 2. In the event that the investigation ticket is not resolved with four business days, notify the SLM Manager to contact the group’s manager.      1. When the ticket is resolved, review the completed Missed SLA form:  * If SIG or JTS agrees that your findings were the cause of the missed / breached SLA,   relate the incident or change ticket to the investigation ticket.  ***Note:*** *When relating to a change ticket, use the “caused by” relationship.*   * If SIG or JTS states that something else was the cause of the missed / breached SLA, relate the incident or change ticket that they provide to the investigation ticket. * If it is noted that there were no issues found, assign the ticket to Technical Services to verify if there was a true outage or if there was a monitoring error.   ***Note:*** *Re-attach the original Missed SLA form for Technical Services to fill out*.   * If Technical Services states it is a monitoring issue, create a Problem ticket for the monitoring issue. * If neither team provides outage data SLM management will work with JTS and SIG management to identify the cause.  1. Add information to the “Comments” section of the SLA spreadsheet’s “Master” tab for the service in question.  * If the issue is under investigation, make a note of that.   *Example: INCXXXXXX AC Incident Management investigating.*  This should also be added to the SLA Report while the investigation is pending. See Step 6.   * If the issue is resolved, note the cause of the missed / breached SLA. Be sure to include any incident or change tickets that were discovered and highlight the section in green. * All finalized comments should include an incident, change, or problem number. * Example:      * Exceptions to including an incident, change, or problem number are: * Holidays * File Transmit deliveries – Information from the Morning Cycle Report for late file deliveries will be used. |
| 6 | Update the SLA Report with a comment as to why the SLA was missed / breached or that the issue is being investigated.  *See the* ***SLM Annotate SLA Outages Procedure****.* |
| 7 | Apply a blackout if an SLA is missed for the following reasons:   * Pre-Approved Change Window * Monitoring issue * A report was not printed on a holiday * Outages reported by SiteScope in which no user impact was found   *See the* ***SLM******Applying Post Blackouts Procedure*** |
| 8 | Publish the Daily SLA Report to Sharepoint:   1. After comments and any appropriate blackouts have been applied, run the SLA report again following the instructions in the ***SLA Report Generation Procedure***, saving the report as a PDF file. 2. Save the report to [O:\Service Delivery\Service Level Management\Reporting\Daily SLA](\\\\jacksonnational.com\\SHARE\\hq\\vol3\\share\\Service Delivery\\Service Level Management\\Reporting\\Daily SLA Report)   [Report\month](\\\\jacksonnational.com\\SHARE\\hq\\vol3\\share\\Service Delivery\\Service Level Management\\Reporting\\Daily SLA Report)     1. Upload the Daily SLA Report to [Sharepoint](http://docs.jackson.local/it/sites/rs/_layouts/15/start.aspx#/Daily%20Reporting/Forms/current.aspx?RootFolder=%2Fit%2Fsites%2Frs%2FDaily%20Reporting%2FSLM&FolderCTID=0x012000AF1427B489A1CD4BA12B90F950303DFE&View=%7B1D5400F7%2DF40D%2D4DC8%2DAED7%2DCCDABECB8C2F%7D) in the appropriate Year / Month folder. |
| 9 | The Daily SLA Report must be kept current with the status of the investigation tickets, the reasons behind the missed / breached SLAs, and any necessary blackouts in order for the Monthly SLA Report to be ready for review on the first business date of the following month.  *See* ***The Monthly SLA Report Procedure*** *for more information.* |

**Appendix A – SLA Report Definitions**

1. **Business Unit** – This identifies what team of Business Users has requested the service to be monitored. Examples (JNL Operations, Broker Dealer, Financial, etc.,)
2. **Service Name** – The name of the service being monitored. It should match what is on the SLA Run Sheets and what is set up within the SLA monitors.
3. **Target** – Appears on the same line as the service name. It displays the compliance target percentage and the expected days and hours of availability.
4. **Date** – Shows the day and date that the service is being monitored.
5. **Verified** – This column tells the number of minutes that the service was available. It is based on the specified time frame that that service is expected to be up.
6. **Errors** – Shows the number of minutes a service was not available. The number will only show the unavailability during the specified time frames. If a service is set to be available between 7:00 AM and 9:00 PM, but the service happens to be unavailable between 10:00 PM and 10:15 PM, this will not appear on the SLA report.
7. **Blacked Out** – This column shows if a block of time had to cancelled out for any of the following reasons; change windows, planned deployments, or monitoring issues.
8. **Actual** – Displays the exact percentage of time that the service was available during the specified time frame. Any interruption in service will cause this number to drop. If a valid blackout is applied, the percentage will go back to 100%.
9. **Rolling 30-day** – This column tracks the actual percentage for 30 day increments. If the actual percentage goes down on any given day, this will affect the Rolling 30-day percentage. Even if the actual percentage is back to 100% the following day, the Rolling 30-day percentage will continue to be lower than 100%. It may take a few days for it to get back to 100%. If there are several days in which the actual percentage is under 100% and the Rolling 30-day percentage drops below the compliance target percentage, it will cause the rows from that point on to turn red. The rows will not return to black until the Rolling 30-day percentage meets the expected compliance target percentage
10. **Comments** – An annotation will be made if an SLA is missed / breached or if a blackout is applied. The comment should include an Incident or Change number and a brief description of the outage.
11. **Total Days** - The total amount of days a service has been monitored for the specified date range. Some services are only monitored five days a week and some are seven, so the total may be different from service to service.
12. **Actual Days SLA Met** – The total amount of days in which the compliance target percentage matched or was above the expected target.
13. **Percentage of SLA Met** – Shows the total percentage of the service’s availability during the dates in which the SLA report was run.
14. **30-day Rolling Average Days SLA Met** – The total amount of days in which the Rolling 30-day percentage met or was above the compliance target percentage.
15. **Percentage of 30-day Rolling Avg Days SLA Met** – The percentage of time that the Rolling 30-day percentage met or was above the compliance target percentage.

**Modification**

The following associates can make modifications to this document:

* Manager, Service Level Management
* Director, IT Service Management
* Vice President, Service Delivery
* Chief Technology Officer, PGDS

|  |  |
| --- | --- |
| Service Level Management Process | |
| Responsible Party: Anna Carter, Manager, Service Level Management Approving Authority: Abdul Golden, Director, IT Service Management | Date Created: 03/02/2017 Last Modified:  Last Reviewed: |