**Corporate Incident Management Process**

SiteScope, a commercially available application, is used to monitor **all** hardware and software, including the Data Center & applications supporting Customer transactions, and corporate functions (internal - financial and H/R applications).

All hardware is subject to industry accepted metrics (CPU, Disk, and Memory usage and availability) values for the metrics have been established through experience to allow for usage spikes and partial equipment failure (prior to executing a pre-established Business Continuity plan).

All software applications are monitored for availability and queue depth (as an indicator of performance). All backups, and internal reporting are monitored for failure. If an application or piece of H/W becomes unavailable or performance degrades to preset metric values the Incident Management Process is triggered.

An event interrupting service to Customers may occur; be detected by system monitoring tools, or be reported by internal or external customers.

Workflow

1. An incident occurs and is reported to Operations personnel via an email sent to the “Production Alert” group. Operations personnel may also detect an issue via system monitors and alerts.
2. The on call resources respond to the Production Alert and/or system alerts – initially sending an e-mail to acknowledge (or inform of) the incident and initiate a Track-It ticket.
3. The on call resources begin to research the incident.
4. If the incident is resolved within the Level-1 SLA criteria, send a follow up message to the Production Alert group stating that the incident has been resolved (include following sub-bullet info) & continue with Step 5.  
   Else  
   if it is not immediately resolved go to Step 8
   1. The last response message is also forwarded to helpdesk
   2. All the required information is recorded in the ticket:
      1. Date/Time
      2. Category / Type / …
      3. Description
      4. Detection Time (24hour format)
      5. Recovery Time (measured from detection time to resolution time)
      6. Root Cause
      7. Actions
      8. Owners (of actions)
      9. Status of each action
5. The incident is discussed at the Daily Incident meeting and any new or additional information is gathered, any next steps are identified, the “last” owner documents all discussion in the Track-It Incident Ticket.
6. Is the incident closed?
   1. Yes – close the ticket
   2. No – continue to step 7
7. Incident is “escalated” to Problem Resolution and the Change Management process is followed.
8. If the incident requires internal escalation, continue with Step 9  
   Else  
   if it requires external escalation, go to Step 14.
9. Escalate the incident to Level-3 Support (Members of the Technology Team).
10. Level-3 Resources assist with researching the issue, defining options, and identifying a recommended resolution.
11. If the incident resolution requires production change, continue with Step 12  
    Else  
    if a production change is not required, go to Step 13.
12. A production change requires following of the Change Management process.
13. Complete Steps 4 through 6a.
14. If the incident is an anomaly and is corrected by restarting the service, proceed to follow steps 4 through 6a.
15. Open the incident with the vendor through their documented channels – online, email, telephone, etc.
16. Response from vendor is received with the next steps. Follow steps 11 through 13, if applicable.