Emergency Response

The identification and remediation of any major incident is critical to ensure that RISD can quickly recover and return to full operations in a timely manner. The ability of the OIT organization to react nimbly and effectively is essential. An organized and rehearsed process that combines communication, documentation and coordination is the key to showing the value of OIT when a major issue arises.

Objectives

In the event of a major incident, this framework is designed to provide OIT with guidance to quickly and effectively demonstrate the following:

- ✓ Responsibility
- ✓ Communication
- ✓ Documentation
- ✓ Coordination
- ✓ Lessons learned
- ✓ Process improvement

Procedure

1. Upon notification (or suspicion) that a major incident is happening, the recipient of the "information" will contact the other members of OIT management (Director of Enterprise Systems, Director of Network Services, Director of Personal Computing Services, Help Desk Manager and Associate VP of OIT) and ask them to participate in a Situation Review. The situation review begins with the initiation of a bridge line. Once opened, the bridge line is to remain open until resolution is achieved. Notification of an incident can come from sources such as the RISD Emergency Operations Command Team (EOCT) or directly to OIT management. OIT staff members are to use the emergency bridge line that has been programmed into their smart phones.

2. The purpose of the Situation Review is to reconcile the available information and to confirm that a major incident is occurring. If an incident is occurring, a member of OIT management will be named as the OIT Incident Manager during the call. A different member of OIT management must also be identified as the backup coordinator who remains on the bridge line in the event that the OIT Incident Manager is called away.

   If this is an incident reported by the EOCT, the AVP of OIT will participate as a member of the EOCT committee and will be the communications point on the EOCT with the OIT Incident Manager.

3. During the conference call, the OIT management team will determine what additional key resources (staff, vendors or other RISD departments) are required to address the

issue. The OIT Incident Manager and/or designee will contact the identified resources to ensure awareness, understanding and ability to respond to the issue. These resources will be asked to join the conference line to review the incident. The collective group is known as the OIT Incident Response Team.

OIT staff contact information (Google doc) available here:
https://docs.google.com/a/risd.edu/document/d/1ym3EsyxxP-jI0L7DZxSVL5WKAPHn5LQVOOWpcKk5z4M/edit

Vendor contact information (Google doc) available here:
https://docs.google.com/a/risd.edu/file/d/0B16aAwSPfQOsYnhNcHhISVNVWVE/edit

4. In the event of a major incident, an email communication will be sent by the OIT Help Desk Manager (or designee) to all OIT Staff apprising them of the situation, identifying who has been named the OIT Incident Manager as well as the members of the OIT Incident Response Team. The email will also include the details of the bridge line. This collective email thread will serve as a secondary communication vehicle for OIT staff to post questions, thoughts and report additional issues. Staff will be advised to *RESPOND TO ALL*.

5. The OIT Incident Response Team plans the approach to incident resolution. (If this is an off-hours incident requiring on-site support, travel time to RISD must be considered.) Any resources required to assist in the resolution of the major incident should be notified and requested to have a representative join the bridge to provide updates. The OIT Incident Response Team is responsible for the creation of the communication plan. Often major incidents require communication with multiple groups including OIT, supporting departments and other groups such as the EOCT.

6. The OIT Incident Response Team prepares customer notifications which will be distributed by the Help Desk Manager (or designee). Once the OIT Incident Response Team has an understanding of the issue, what actions are to be taken and an estimated time to repair, a customer notification is sent. The customer notification can occur in one of many ways including: email, phone or RISD Alerts.

7. Continual updates to customers should be sent based on the communication plan. This can be based on how severe the issue is, or how many end users are impacted. It may also depend on the estimated time to restore service. Each update will conclude by indicating when the next update will occur.

8. All changes to the infrastructure and systems must follow emergency change procedures, as defined by OIT change management processes to mitigate risks.

9. Once issue resolution is achieved, and it is agreed that the repair has resolved the issue, the major incident process can be concluded. The wrap-up of the major incident process follows these steps:

    - Customer notification utilizing the aforementioned methods is sent to the customers. If a root cause analysis must also be distributed, it should be noted in the resolution email as to when end users can expect to receive that information. It is a good practice to remind customers that although the major incident has been resolved, if they are still experiencing an issue, it is imperative that they contact the OIT Help Desk for assistance (or if after hours, the OIT Incident Response Manager.)

    - Internal OIT notification occurs, notifying members of teams working on the issue that it has been fully resolved.

    - The conference bridge can be closed out.

    - The OIT Incident Response Manager should conduct a post-incident review to identify improvement opportunities and perform a root cause analysis.

OIT Incident Response Workflow

April 2012