Committee members: Bill Chollett (chair), Steve Conway, John Norton, Jim Rosser, Peter Walsh, Monica Weintraub

Committee charter:

1. Define mission critical (essential functions) services, common dependencies and collect information relevant to Business Continuity (BC) and/or Continuity of Operations (COOP).

2. Recommend a framework to evaluate and communicate priorities, Recovery Time Objectives (RTOs) and dependencies.

3. Recommend methods to communicate practical requirements to achieve RTOs and to include IT components as part of unit testing of BC plans.

DELIVERABLES

Charge 1
A. define mission critical services (essential functions) as determined by any division/department - Tiers I, II and III
B. define central provider dependencies for mission critical functions services
C. centralize information about critical functions and dependencies

Charge 2
A. divisions/departments enumerate/categorize services and determine RTO
B. divisions/departments centrally report dependencies and RTOs
C. collect/publish central service provider response team contact/info

Charge 3
A. develop a template for IT to present to business units to define/explain IT dependencies on unit BCP
B. provide definitions/references for Essential Function Tiers and corresponding RTO requirements

This report contains all of the deliverables cited above.
Executive Summary:

The committee conducted a thorough review of TAMU Business Continuity rules, SAPs, TACs and planning documents along with existing initiatives, pilot projects and reporting tools for suitability and adaptability to this purpose. Additionally, the committee met with representatives from multiple units involved with Business Continuity planning and readiness.

It is the assessment of the committee that the most expedient method of achieving departmental compliance with Business Continuity is to go through the Continuity of Operations workshops offered by the Office of Safety and Security. This assessment is based on the thoroughness of the workshop methodology, availability of the resource and the fact that there is no cost to the individual unit.

It is also our recommendation that units responsible for providing central services have access to the plans that result from completion of these workshops. These central service providers should make use of this information in regards to priority and capacity planning.

A final recommendation is to create a university-wide centralized repository for all mission critical/essential services in compliance with Appendix A: Information Technology Continuity of Annex J – Institutional Continuity Plan.
Methodology:

The committee reviewed current TAMU BC/DR related rules, SAPs, TACs and planning documents, and ongoing initiatives within the VP-APIT division and in the Office of Safety and Security (SASE). The committee also reviewed common elements and dependencies of the IT component of BCPs.

The committee reviewed existing tools used for central reporting of information related to IT including: Information Security Awareness Assessment, and Compliance (ISAAC); Living Disaster Recovery Planning System (LDRPS); and the Continuity of Operations (COOP) model. The committee then assessed what changes might be made to central reporting tools/databases to provide a common procedure for assessing dependencies and reporting them to the central service providers.

Committee members met with various representatives from each area or service related to BCP, including: Susan Cook for ISAAC; Debra Dandrige regarding applicable SAP updates; and Joe Mancha from University Risk and Compliance.

The committee feels that the original charter outlined by the exploratory committee was very broad with some items outside the scope of what it could accomplish. Thus, we have attempted to address the charter, goals, charges and deliverables within the scope of IT.

Deliverables:

Charge 1 - Define mission critical (essential functions) services, common dependencies and collect information relevant to Business Continuity (BC) and/or Continuity of Operations (COOP).

A. define mission critical services (essential functions) as determined by any division/department - Tiers I, II and III

   A review of existing rules and documents show there is little commonality in the definition of these "functions" or "services." TAC Rule 202.74, 1, A refers to "mission critical information resources" while Annex J, section VII of the TAMU Crisis Management Plan refers to "essential functions" and defines Tiers I, II and III in terms of Recovery Time Objectives (RTO). The committee recommends that all essential IT functions be defined as per Annex J.

B. define central provider dependencies for mission critical functions services

   It is apparent from our review that all campus IT organizations are dependent upon two primary service providers: - VPAPIT for network/telecommunications and VP Facilities for power, environmental controls and facilities.

   Information reported through official channels should be used by the respective
administrators to determine which systems are the most critical based on the numbers and types of dependencies reported.

C. centralize information about critical functions and dependencies

It is our assessment that information resources supporting essential functions should be identified and reported in one of three venues: ISAAC (CIS); LDRPS (CIS); or the COOP model (SASE). Aggregate information self-reported through these venues should be made available to central providers responsible for support and maintenance of these services.

Charge 2 - Recommend a framework to evaluate and communicate priorities, RTOs and dependencies.

A. divisions/departments enumerate/categorize services and determine RTO

Information technology departments routinely list information resources that support essential functions as part of their annual ISAAC reports. To the extent possible, IT should encourage their department to make use of this information while using the COOP model (SASE) to conduct departmental BCP planning. Furthermore, IT departments should collaborate with other functional departments in their unit to understand dependencies and priorities, and set realistic expectations for RTOs.

Though the COOP model (SASE) is a no cost, widely adopted and freely available option for individual units, use of a web-based, central tool such as LDRPS is the best option for long term management and communication of priorities. If adopted campus wide, such a tool would help eliminate data stovepipes and offer planners a means to access and analyze critical, shared information with a common vocabulary and format.

The committee believes the Continuity and Recovery Group referenced in Annex J (Institutional Continuity Plan) would be better able to execute the plan (identify resources, coordinate responses and prioritize needs) with a central reporting tool in place. Moreover, a centralized TAMU planning tool would be more cost-effective than time and expenditures incurred by a decentralized, departmental approach.

B. divisions/departments centrally report dependencies and RTOs

Our review of information determined that the Office of Safety & Security (SASE), which offers excellent COOP planning workshops, is best situated to serve as a central repository for departmental BCPs. Based on their extensive knowledge and expertise, we recommend SASE maintain a repository of
COOPs on file and make this information available to the Continuity & Recovery Group referred to in Annex J.

C. collect/publish central service provider response team contact/info

Without access to departmental BCPs the committee was unable to determine who on campus are deemed as the specific central service providers. The committee made some general assumptions based on committee member dependencies on central providers and thus offers this list:

i. Networking and Information Services (DNS, networking) 845.8300
ii. Telecommunications, 845.1020
iii. Facilities, Utilities & Energy Services, 458.5500 business hours, 845.4311 after hours
iv. Office of Facilities Coordination, 845.8661

Charge 3 - Recommend methods to communicate practical requirements to achieve RTOs and to include IT components as part of unit testing of BC plans.

A. develop a template for IT to present to business units to define/explain IT dependencies on unit BCP

"Business continuity is truly an institutional activity. IT must play an integral part, as IT’s role in academic and business operations has grown enormously in the past decade. At the same time, business continuity's holistic nature means that IT cannot "own" it or deliver it single-handedly."^{1}

The committee strongly recommends that departments serious about BCP contact SASE and take advantage of their free workshop. Additionally, IT department representatives should encourage their chain of command to make this a unit exercise with full participation by all functional units, including IT, which can provide assistance by offering realistic IT RTOs.

B. Provide definitions/references for Essential Function Tiers and corresponding RTO requirements

This information is quoted from section VII, “Annex J – Recovery – Institutional Continuity Plan”

Essential Functions – “…functions that they must perform in order to continue to operate and provide necessary services.”

- Critical Infrastructure: Uninterrupted or resumed within a few hours
- Tier I: 0 – 12 Hours, Must be restored to minimum level of service within 12
hours of event

- Tier II: 12 hours to Two Weeks, Must reach an operational status within 12 hours to two weeks of activation
- Tier III: Two Weeks to 30 Days

REFERENCES

Texas Administrative Code (TAC)

- §202.1 Applicable Terms and Technologies for Information Security
- §202.70 Security Standards Policy
- §202.73 Managing Physical Security
- §202.74 Business Continuity Planning
- §202.75 Information Resources Security Safeguards

TAMU Rules and Standard Administrative Procedures (SAPs)

- 29.01.99.M1.32 Information Resources – Disaster Recovery Planning

Texas A&M University: Review of Business Continuity Planning – audit report 2011

Institutional Continuity Plan – Annex J

Office of Safety and Security – COOP presentation as CSABA workshop, Spring 2012

**Business Continuity Exploratory Committee Report**

Date: 11 Oct 2011

Membership:
- Andy Bland
- John Chivvis
- Steven M. Conway – Chair
- Leslie Lutz - outside member Office of Safety and Security
- David Sweeney

Recommendation: To proceed with establishment of a Business Continuity Sub Committee. Appropriate IT related Business Continuity efforts include; supporting the business units in development of the business continuity plan, developing resources to support business continuity and recovery timeframes (this might include a remote hot site), develop IT plan to support disaster recovery and restoration of services within the required time frame (this might include contracts with vendors for critical replacement equipment).

Charter / Goals / Charges:

1. Identify and Connect TAMU IT Units for items related to Business Continuity and Disaster Recovery efforts. Define IT components of the BCP that are common for all IT organizations (least common denominator) and create deliverables.
2. Create methods of coordinating communications between central and decentralized units prior and during a disaster.
3. Support business units in developing plans for periodically testing business continuity plans. Develop a system and/or recommendations for including appropriate IT components in tests of unit’s BCPs.

Deliverables:
- **Charge 1**
  - Identify current locations of physical servers
  - Identify virtual servers and shared space
  - Identify funding issues
- **Charge 2**
  - Recommend procedures for ITAC response to critical incidents
  - Review and report campus teams that respond to critical events.
  - Explore submitting BCP dependencies list through ISAAC
  - Make recommendations to CIS on how to use/coordinate submitted dependencies
- **Charge 3**
  - Recommend a Framework
  - Identify resources
  - Prepare presentation to business units

Timeline or Timelines
- FY 12

Membership recommendations (to include outside membership as applicable)
- Current members unable to serve include