

North Carolina

Statewide Technical Architecture

Enterprise Management Domain

© 2005 State of North Carolina
Office of the State Chief Information Officer
Enterprise Technology Strategies
PO Box 17209
Raleigh, North Carolina 27699-7209
<http://www.ncsta.gov>
ets@ncmail.net

All rights reserved. No part of the material protected by this copyright notice may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording or by any informational storage system without written permission from the copyright owner.

Table of Contents

1. PRINCIPLES:..... 4

1.1. LIMITED PRODUCT VARIATIONS FACILITATE SUPPORT EFFORTS AND REDUCE LONG-TERM SUPPORT COSTS. 4

2. TECHNICAL TOPIC: CONTACT CENTER..... 4

2.1. PRACTICES: 4

2.1.1. Provide customers multiple means for interacting with the contact center. 4

2.1.2. Enable self-directed customer service. 5

2.1.3. Develop a single consolidated contact center design that supports an enterprise model..... 5

2.1.4. Personalize interaction with customer. 5

2.1.5. Establish and document multiple levels of support to leverage resources and provide effective service..... 5

2.1.6. Align the contact center and user support functions to provide a comprehensive support services environment..... 6

2.1.7. Define reliable metrics and reports to assist managers, contact center staff, and the citizen community in assessing the effectiveness of the center in meeting organizational goals..... 6

2.1.8. Maintain a resolution database containing solutions to recurring problems to improve service quality and contain costs. 6

2.1.9. Provide access to inventories of hardware and software configurations, including all physical components (processor, RAM, disk drive, network cards, add-on cards) and other types of relevant information for the contact center..... 6

3. TECHNICAL TOPIC: OPERATIONS MANAGEMENT 7

3.1. PRACTICES: 7

3.1.1. Design data center environmental systems to eliminate any single points of failure and allow for components to be maintained on or off line as required without impact to the service by that system. 7

3.1.2. Design the air-conditioning system to provide adequate air-flow for all the network equipment to operate within requirements..... 7

3.1.3. Locate data centers in areas not exposed to storage or process areas in which explosion potential may exist. 7

3.1.4. Protect data centers located in a multi-story or multi-occupancy building against the entrance of water by water-tight ceilings and water-tight seals between walls, floors and ceilings. ... 8

3.1.5. Maintain an effective preventative maintenance and emergency response program for every data center. 8

3.1.6. Limit the amount of "unique" performance tuning to existing individual network components, particularly servers and desktops. 8

3.1.7. Remotely perform systems management functions for virtual data centers in a secure manner. 8

3.1.8. Provide means for laptop data backup. 8

3.2. STANDARDS: 8

3.2.1. Use Remote Monitoring (RMON2) products. 8

4. BUSINESS CONTINUITY 9

4.1. PRACTICES: 9

4.1.1. Establish an Emergency Operation Center (EOC) to be used as a command center during an incident response. 9

4.1.2. Review and update agency business continuity plans no less than annually, or as warranted by changes in the business or information system environments. 9

4.1.3. For each system, perform a business impact analysis at least annually..... 10

4.1.4. Establish both Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for every system, in accordance with the results of the business impact analysis. 10

4.1.5. *Redundant copies of business critical data must be stored in secured and geographically diverse locations, and made readably available for use during an emergency within the stated recovery objectives.*..... 11

4.1.6. *Implement and test procedures for incident response and stabilization.*..... 11

4.1.7. *Institute a desktop management system that relies upon standard configurations and PC imaging to meet the desktop business impact analysis (BIA) recovery objectives.* 11

4.1.8. *Business continuity plans must be available to those who are authorized access.* 11

4.1.9. *Maintain a system inventory with a complete list of devices, vendors, used services, and contract names for all locations.*..... 12

4.1.10. *Develop and maintain comprehensive disaster recovery plans that address all the critical operations and functions for each line of business.* 12

4.1.11. *Establish business continuity teams, detailing the management structure with clearly defined roles and responsibilities.* 12

4.1.12. *Integrate business continuity plans into an agency's project life cycle to ensure that recovery needs are identified in the initial phases of new projects, or of changes in business process and information systems.* 12

4.1.13. *Maintain a service-level classification system with associated development, infrastructure, and operations architecture requirements.* 12

4.1.14. *Develop and exercise communication plans for handling crises with key stakeholders.* 13

4.1.15. *Document and test Incident Response procedures at least bi-annually.*..... 13

4.1.16. *Deploy performance management tools that have common interfaces such that collected metrics may be directed to the common data repository.*..... 13

4.1.17. *Provide regular reports on performance against service level agreement (SLA) targets.*13

4.1.18. *Produce regular management reports, which include current usage of resources as well as trends.* 13

4.1.19. *Measure, trend, and forecast peak period utilization and plan resource capacity with ongoing periodic reviews.*..... 13

4.1.20. *Identify and develop measurements for critical work processes and customer requirements, by establishing performance goals, standards, and baseline metrics.* 14

4.1.21. *Minimize the number of performance monitoring tools deployed in order to facilitate metric collection into a central repository.*..... 14

4.1.22. *Deploy enterprise level tools that provides real time performance monitoring and anomaly detection capabilities as well as usage trending and forecasting functionality.* 14

4.1.23. *Re-use existing infrastructure, systems, and applications before investing in new solutions.* 14

4.1.24. *Configure production environment equipment based on comprehensive testing results.* 14

4.1.25. *Employ tools that provide functionality to isolate application workloads from operating systems functions in order to accurately measure application resource requirements and forecast future requirements.*..... 15

1. Principles:

1.1. Limited product variations facilitate support efforts and reduce long-term support costs.

Rationale:

- Uncontrolled product deployment contributes to a level of complexity that exceeds the support capability of current distributed systems management, DSM, tools and increases staff and training costs. Choices for managing this difficult situation include the following:
 - Scaling back deployment to a manageable range.
 - Reducing complexity through consistent product selection.
 - Planned retirement of applications, hardware and operating systems with performance problems and/or that are difficult or impossible manage and support.
- Deployment of consistent environments enables the systems management infrastructure to adjust to change. For example, when all users of a particular system have a recommended standard desktop software configuration, this common basic environment makes it easier to plan and install system upgrades and to isolate problems.
- A finite and identifiable product range facilitates centralized support and planned operational changes.
- Careful selection of products that can be supported centrally is more cost effective because it reduces the support burden of 'shadow' or peer to peer support. Support costs are one of the more expensive systems management components.
- Established product selection criteria contributes to cost savings through discounts provided for state-wide software product licenses. Business managers need to be aware of the impact that business decisions have on support costs.
- The learning curve and associated training costs for technical staff are reduced when products are carefully selected to comply with architectural requirements.

2. Technical Topic: Contact Center

2.1. Practices:

2.1.1. Provide customers multiple means for interacting with the contact center.

Rationale:

- Customers expect several service options available for interaction with the contact center. The services offered must be by the customer's standards and by the media of their choice. Widely available means for interaction include telephone, fax, email, and web.
- Customers expect Internet services that provide comprehensive information access and the ability to initiate transactions.

2.1.2. Enable self-directed customer service.

Rationale:

- Self-service or agent-assisted service should be options for customers. Many customers will prefer to find information or initiate transactions on their own. As such, means should be provided that offer customer self-service.

2.1.3. Develop a single consolidated contact center design that supports an enterprise model.

Rationale:

- A consolidated contact center does not have to be physically located in one place. However, it should have a common constituency, phone number, set of procedures, set of defined services, and set of integrated network systems management (NSM) platforms and applications.
- The implementation of the virtual data center (VDC), where many remote LANs are managed as a single entity, supports the corresponding development of consolidated help desk services.
- Agencies intending to implement a contact center should leverage the existing state contact center infrastructure and services.

2.1.4. Personalize interaction with customer.

Rationale:

- Transactions can be customized to provide a unique customer focused service. This level of customization may be based on the type of citizen, their past transaction history, or other critical flags that may be set by the business.

2.1.5. Establish and document multiple levels of support to leverage resources and provide effective service.

Rationale:

- Regardless of the size of an organization, effectively prioritizing contact calls is a critical process for providing high-quality and efficient services.
- Examples of levels and criteria include the following:
 - Level 1 customer support should have end-to-end responsibility for each request. The contact center analyst should be empowered to resolve as many requests as possible. Level 1 provides the central contact point (CCP) or call ownership, which is the single point of contact for the end user to request a service. Agencies should retain control of the level 1 help desk in order to ensure the quality of the relationship.
 - Level 2 support provides advanced technical expertise to the level 1 contact points. Their responsibility is to analyze the requests routed to them and resolve the problems. Resources at this level can be composed of staff specialists and/or third party providers/vendors.
 - Level 3 support is composed of highly specialized technical experts. Calls which cannot be solved at levels 1 and 2 are routed to this level. Resources at this level can be comprised of staff specialists and/or third-party providers/vendors.
- The different call levels within a call level system require different types of skills. A level 1 staff person might be quite skilled but prefer the faster pace at that level. A

level 2 staff person may not know everything about a system but could be good diagnostician and researcher. Staff at each level should be respected for the resources they each bring to a support team.

2.1.6. Align the contact center and user support functions to provide a comprehensive support services environment.

Rationale:

- The contact center should be elevated in the organization and reporting structure to operate independently of other units, making customer service needs its top priority.
- The role of the contact center analyst is changing. Center staff should serve on project teams, and participate in training, application design, testing, and maintenance.
- All requests for service should be channeled through the contact center when feasible.

2.1.7. Define reliable metrics and reports to assist managers, contact center staff, and the citizen community in assessing the effectiveness of the center in meeting organizational goals.

Rationale:

- Both consolidated high level and low level detailed measures are critical to successful service desk operations.
- Metrics should be used to identify trends and to support a proactive management approach that anticipates and avoids problems. For example, monitoring server information and trend analysis of performance statistics for comparing LAN operations generates important information necessary to remotely support many LANs.
- Methods and procedures to solve problems should be developed, published and followed and measured.
- Service level agreements (SLA's) should be developed stating responsibilities of both the contact center and its clients. SLA criteria are one method to evaluate help desk performance.

2.1.8. Maintain a resolution database containing solutions to recurring problems to improve service quality and contain costs.

Rationale:

- Building and using a knowledge base of prior resolutions to solve problems improves the quality of resolutions.
- Contact Center operations should include problem resolution links to external systems, for example, frequently asked questions (FAQ) files.

2.1.9. Provide access to inventories of hardware and software configurations, including all physical components (processor, RAM, disk drive, network cards, add-on cards) and other types of relevant information for the contact center.

Rationale:

- Current inventories are critical to support functions.
- Maintenance of current inventories are critical to support functions.
- Inventory "agents" or applications that survey and record current inventory facilitate collection from desktops and servers.

- An inventory of hardware and software configurations will assist contact center staff in identifying and rectifying issues related to configuration.

3. Technical Topic: Operations Management

3.1. Practices:

3.1.1. Design data center environmental systems to eliminate any single points of failure and allow for components to be maintained on or off line as required without impact to the service by that system.

Rationale:

- Maintain alternative paths, and backup components for telecommunication lines and power supplies.
- Allowing off-line service with minimum impact requires an effective preventative maintenance and emergency response program. This program should be established utilizing results from your organizations business impact analysis.
- Maintain a document library to include change management procedures, equipment manuals, and system schematics.

3.1.2. Design the air-conditioning system to provide adequate air-flow for all the network equipment to operate within requirements.

Rationale:

- System overheating could result in intermittent hardware failure. Thus, air-conditioning systems play an important role in maintaining a stable computer environment.
- If using under floor cooling, perforated floor tiles should be properly placed to allow under-floor cooling to feed the air inputs of the chassis design.
- Maintaining a well ventelated data center will limit the risk of equipment trouble and help preserve the quality of the equipment over its lifecycle. This can be accomplished by maintaining the data center air quality to be free of any particle larger than 0.5 of a micron.
- Data center should be kept between 70 and 73 degrees Fahrenheit and 45% to 60% humidity.

3.1.3. Locate data centers in areas not exposed to storage or process areas in which explosion potential may exist.

Rationale:

- Piping for flammable or combustible fluids and gases should not be run through computer rooms. Single story structures housing computers should not be located over, or adjacent to, high pressure gas mains.
- Where an explosion hazard exists from other properties, computer rooms should be located on the opposite side of the building to that hazard.

3.1.4. Protect data centers located in a multi-story or multi-occupancy building against the entrance of water by water-tight ceilings and water-tight seals between walls, floors and ceilings.

Rationale:

- Water in a data center can cause a business to come to a complete halt. Careful examination of your organization's site for the susceptibility to flooding from either natural or man-made sources should be examined. Avoid basement locations. These spaces can bring with them issues resulting from drainage problems.

3.1.5. Maintain an effective preventative maintenance and emergency response program for every data center.

Rationale:

- An effective preventive maintenance and emergency response program should include at least the following items: documented change management, equipment manuals, posted system schematics, equipment labeling, and maintenance document library.

3.1.6. Limit the amount of "unique" performance tuning to existing individual network components, particularly servers and desktops.

Rationale:

- Performance tuning for unique/non-standard components is often not worth the increased maintenance costs of multiple configurations.
- Performance tuning can inhibit change by encouraging comfort with the status quo.
- It may be less expensive to increase performance by upgrading to an architecturally compliant hardware configuration than to spend time tuning an application.

3.1.7. Remotely perform systems management functions for virtual data centers in a secure manner.

Rationale:

- Some examples of remote systems management services include:
 - Backup, archiving and recovery
 - System, database and application monitoring
 - Software distribution to the server and/or desktop

3.1.8. Provide means for laptop data backup.

Rationale:

- Only non-sensitive and expendable data should be stored on a laptop. The authoritative source must be on a server, and data should be replicated to the laptop as needed and appropriate.
- When data is stored on a laptop, provide easy-to-use backup facilities. Implement policies to ensure and automate backup.

3.2. Standards:

3.2.1. Use Remote Monitoring (RMON2) products.

Rationale:

- The Simple Network Management Protocol (SNMP) is a group of internet protocols that is the standard for managing TCP/IP based networks.
- RMON products are predicted to become increasingly used in most enterprise networks.
- RMON products provide packet collection, decoding and analysis to the Data Link layer of the Open Systems Interconnection (OSI) stack using a combination of consoles and hardware and software probes that relied on SNMP management information base (MIB) data collections.
- In 1992, the Internet Engineering Task Force, IETF, specified the RMON1 standard in RCF 1271. The RMON1 MIB extends SNMP capability by monitoring sub-network operation and reducing the data collection burden on management consoles and network agents.
- The RMON2 standard was approved by the IETF in January 1997 in RCF2021. RMON2 includes a new MIB to extend network monitoring into the application monitoring layer.
- RMON functionality is growing to include functions like applications monitoring, report generation and bandwidth allocation.
- All major network device vendors have added RMON MIB collection capability to their products, although the depth of implementation relative to the full RMON specification varies among vendors and products.

4. Business Continuity

4.1. Practices:

4.1.1. **Establish an Emergency Operation Center (EOC) to be used as a command center during an incident response.**

Rationale:

- The location for an emergency operation center may need to occur in a location physically separated from the organization headquarters.
- Establishing an EOC can be accomplished as a reciprocal agreement with another agency or as a contract with a vendor.
- Organizations housed in a single facility may need to make arrangements quickly to accommodate staff and new equipment in the case there is destruction to the facility.

4.1.2. **Review and update agency business continuity plans no less than annually, or as warranted by changes in the business or information system environments.**

Rationale:

- According to Article 3 of Chapter 147 of the North Carolina Administrative Code, each state agency shall develop and continually review and update as necessary a business and disaster recovery plan with respect to information technology.
- Each state agency shall submit its disaster recovery plan on an annual basis to the State Chief Information Officer.
- Critical to the success of any business continuity plan is effective maintenance. Without efforts to keep documentation updated, ensure the availability of emergency

resources and promoting on-going user involvement much if not all of the value of the plan will be lost.

4.1.3. For each system, perform a business impact analysis at least annually.

Rationale:

- The business impact analysis is the cornerstone of the business continuity planning process. The impact analysis identifies the impacts resulting from disruptions and disaster scenarios that can affect the organization and techniques that can be used to quantify and qualify such impacts.
- This process will allow an agency to examine all the system risks, and rank those risks by level of severity. It will also allow for cost-effective decision on what to protect at what cost. Agencies do not want to spend more to protect the systems than those systems are actually worth.
- For each agency the basic goals of security are availability, confidentiality, and integrity. Each threat should be examined with an eye to how the threat could affect these areas.
- Sample list of system assets:
 - Hardware: CPUs, interface cards, keyboards, monitors, workstations, printers, communication lines, switches, routers
 - Software: Source programs, diagnostic programs, operating systems, communication programs
 - Data: During execution, stored on-line, archived off-line, backups, audit logs, databases
 - People: Users, administrators, hardware maintainers
 - Documentation: On programs, hardware, systems, local administrative procedures
 - Supplies: Forms, magnetic media
 - Service and maintenance contracts.

4.1.4. Establish both Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for every system, in accordance with the results of the business impact analysis.

Rationale:

- Recovery Time Objective: the time period from the disaster declaration to the recovery of the critical functions.
- Recovery Point Objective: the point in time to which data must be restored in order to resume processing transactions. This quantifies the acceptable amount of data loss that can be endured based on business requirements.
- Establishing recovery time objectives and recovery point objectives in the business continuity plans will assist organizations in prioritizing systems from low concern to mission critical. It also allows organizations to identify the associate resources and cost to ensure that the objectives are met.

4.1.5. Redundant copies of business critical data must be stored in secured and geographically diverse locations, and made readably available for use during an emergency within the stated recovery objectives.

Rationale:

- Agencies with document retention requirements must ensure that all business critical data are stored in a secure and environmentally controlled area. Electronic copies of the original document should be stored separately from the original. This will decrease the risk of losing both sets of documents due to natural disasters or theft, and will help ensure that data will be available in the case of disruption to meet the stated recovery objectives.
- Agencies need to be aware of the location of their business critical data and establish an adequate protection program (i.e., fireproof cabinets, offsite duplication, clear desk policy, etc).
- All business processes must be recoverable no matter what their dependence upon information systems. The recovery strategies must focus on the business process and not only on the technology components of the process. It is not a "data center problem."

4.1.6. Implement and test procedures for incident response and stabilization.

Rationale:

- A key determinate to ensure a successful business recovery is both the implementation and testing of procedures for re-establishing business processes.

4.1.7. Institute a desktop management system that relies upon standard configurations and PC imaging to meet the desktop business impact analysis (BIA) recovery objectives.

Rationale:

- Making computers available quickly can greatly increase an agency's recovery time from a business interruption.
- A standard configuration image can help reduce configuration variance; thus, assisting in the management of state owned assets.

4.1.8. Business continuity plans must be available to those who are authorized access.

Rationale:

- Business continuity plans, which may contain sensitive information, must be secured. However, they should readily available for those that need them.
- It is prudent to keep several copies of the plan off-site to quickly recovery operations at a pre-determined location.
- Plans may include recovery procedures, recovery point lists, a map to a pre-established location, an organizational call list of employees, vendors, and critical services.

4.1.9. Maintain a system inventory with a complete list of devices, vendors, used services, and contract names for all locations.

Rationale:

- This information will allow a business to more quickly assess the course of action and resume business operation after a business disruption.

4.1.10. Develop and maintain comprehensive disaster recovery plans that address all the critical operations and functions for each line of business.

Rationale:

- Disaster Recovery Plans should include documented and tested procedures, which will help ensure the ongoing availability of critical resources and continuity of operations.
- Disaster Recovery Plans should consider how to deal with events such as the following:
 - Terrorist Acts
 - Power outages or spikes
 - Computer failures due to viruses, etc
 - Software or hardware failures
 - Natural disasters from flooding, etc.

4.1.11. Establish business continuity teams, detailing the management structure with clearly defined roles and responsibilities.

Rationale:

- Pre-defined business continuity teams with clear delineation of roles and responsibilities will help improve response time and coordination during an incident.
- Without a dedicated staff to conduct business continuity planning and recovery, it is likely that the activities will never get done.

4.1.12. Integrate business continuity plans into an agency's project life cycle to ensure that recovery needs are identified in the initial phases of new projects, or of changes in business process and information systems.

Rationale:

- A business impact analysis (BIA) is a key starting point in incorporating a business continuity plan into a critical business process project life cycle. The BIA should be performed by a project team consisting of business unit, security and IT personnel.
- It is also important that business continuity be built into the life cycle for business process enhancements projects so that availability and recovery requirements are built into the architecture and design.

4.1.13. Maintain a service-level classification system with associated development, infrastructure, and operations architecture requirements.

Rationale:

- The development of a classification scheme of supported service levels to include scheduled uptime, percent availability in scheduled uptime, and recovery time and point objectives will assist to identify the necessary resources required and the associate costs.

4.1.14. Develop and exercise communication plans for handling crises with key stakeholders.

Rationale:

- Develop, coordinate, evaluate, and exercise plans to communicate with key personnel, key constituents, critical suppliers, senior government officials, the media, and provide trauma counseling for employees and their families.

4.1.15. Document and test Incident Response procedures at least bi-annually.

Rationale:

- Even the best security practices and technology can be compromised. Planning is essential in responding to disruptions or disaster to ensure the protection of valuable data, collecting evidence to be used in prosecution efforts and in recovering from an incident.
- Review and propose procedural changes gleaned from lessons learned.

4.1.16. Deploy performance management tools that have common interfaces such that collected metrics may be directed to the common data repository.

Rationale:

- Limiting the deployment of differential common interfaces reduces software and support costs. Most enterprise level vendors provide monitoring agents for all major platforms/OS types. If a unique vendor is required, ensure that the tool supports a protocol compatible with the primary performance monitoring toolset.

4.1.17. Provide regular reports on performance against service level agreement (SLA) targets.

Rationale:

- Regular reports may be used to compare performance over time, highlight potential response issues, and identify possible system upgrade requirements.

4.1.18. Produce regular management reports, which include current usage of resources as well as trends.

Rationale:

- Providing management with regular utilization reports as well as trends over time will aid in the justification and budgeting of hardware upgrades or purchases.

4.1.19. Measure, trend, and forecast peak period utilization and plan resource capacity with ongoing periodic reviews.

Rationale:

- Employing data management practices whereby historical data may be maintained over a representative period of time facilitates the identification of peak usage

patterns from month to month and enables accurate forecasting of resource requirements.

4.1.20. Identify and develop measurements for critical work processes and customer requirements, by establishing performance goals, standards, and baseline metrics.

Rationale:

- Engaging the citizen to establish expected performance results, will assist in the customization of rules and policies in order to focus and prioritize monitoring of critical applications and the consistent establishment of baseline behaviors for trending analysis.

4.1.21. Minimize the number of performance monitoring tools deployed in order to facilitate metric collection into a central repository.

Rationale:

- Restricting the number of deployed tools expedites data management functions such as database queries, web posting and report extraction by directing collected metrics to a single repository.
- Eliminates the requirement for multiple proprietary data stores.

4.1.22. Deploy enterprise level tools that provides real time performance monitoring and anomaly detection capabilities as well as usage trending and forecasting functionality.

Rationale:

- Deploying a single robust, feature rich tool suite provides real time monitoring and alerting capabilities as well as trend analysis functionality reduces both software costs and support resource requirements.

4.1.23. Re-use existing infrastructure, systems, and applications before investing in new solutions.

Rationale:

- Build only those systems or applications that will provide clear business advantages and demonstrate cost savings versus existing comparable systems or applications available from vendors or other government entities.
- The use and availability of effective package solutions is ever growing. Using commercially available solutions reduces the risk associate with in-house development and reduces the total cost of ownership.

4.1.24. Configure production environment equipment based on comprehensive testing results.

Rationale:

- A properly tested environment will reveal the specific environment that is required to successfully run the system for a predetermined user base. A properly tested environment will include, but not be limited to, load and stress testing on the round trip transaction measuring minimum and maximum on both concurrent users and response time requirements.

- After the production environment has been properly tested, then the test environment must be updated to match the production environment.

4.1.25. Employ tools that provide functionality to isolate application workloads from operating systems functions in order to accurately measure application resource requirements and forecast future requirements.

Rationale:

- Utilizing workload characterization tools to segregate application resource utilization from operating system and support functions such as backup activities and security scans enables more granularity in the areas of troubleshooting, trending, and forecasting.