

# How Can the Security and Integrity of Data Resources be Ensured in a Downsizing Climate?

Lowell Smith  
Manager  
RSM McGladrey  
[lowell.smith@rsmi.com](mailto:lowell.smith@rsmi.com)



**April 16, 2009**

© 2009 RSM McGladrey, Inc.

**RSM! McGladrey**

RSM McGladrey, Inc. is a member firm of RSM International – an affiliation of separate and independent legal entities.

# Data and Systems Support Areas with Greatest Security Risk

- Logical security
- Physical security
- Monitoring of activity
- Segregation of duties
- Training and documentation
- Data integrity and confidentiality
- Vendor and patch management
- Change management

# RSM McGladrey, Inc.

## Company services and sectors

- Fifth largest U.S. accounting, tax and business consulting services provider
- Manufacturing, distribution, financial, real estate, government, healthcare and not-for-profits

## Technology Risk Management Services group

- IT compliance and security services

# Reactions to the Economic Downturn

- Downsizing activity at clients
- Changes in organizational focus
- IT management reactions
- Less attention to detail

# MWD National Survey

- Conducted annually
- Respondents in 2008 included a total of 967 CEOs, CFOs and other senior executives
- Distributed geographically across U.S.
- 10 major industry sectors
- Mid-sized companies

# MWD National Survey – Growth Expectations

- Question: How optimistic are you about your industry's growth prospects in 2008?
  - Declines in all industries over 2006 and 2007
  - Transportation equipment respondents: 42 percent decline from 2006
  - Building materials respondents: 55 percent decline from 2006
- Question: How optimistic are you about the U.S. economy's growth prospects in 2008?
  - 77 percent were pessimistic

# MWD National Survey – Downturn strategies

- What are the strategies planned or adopted to cope with downturn?
  - 77 percent consider IT increasingly critical to survival
    - Innovation including increased use of IT
    - New product development or new features
    - Increase operational effectiveness—most relied upon strategy
    - Cost reduction through increased use of IT

# MWD National Survey – Areas at risk

- Most critical risk areas
  - Financial 68 percent
  - Operational 65 percent
  - Legal and regulatory 48 percent
  - Supply chain 38 percent
  - Technology 25 percent

# MWD National Survey – IT Security and Staffing

- Information security
  - 25 percent indicate information security is a top three priority
  - 38 percent plan to spend more
  - 44 percent see increased network security testing and monitoring
- 78 percent did not intend to hire

# MWD National Survey – Summary

2008 responding companies:

- Business will slow down
- Do not plan to hire
- Understand that business risks will not go away
- See an increasing need for IT resources
- Believe that the use of IT critical to survival
- Place a high priority on IT security

More survey results can be found at:

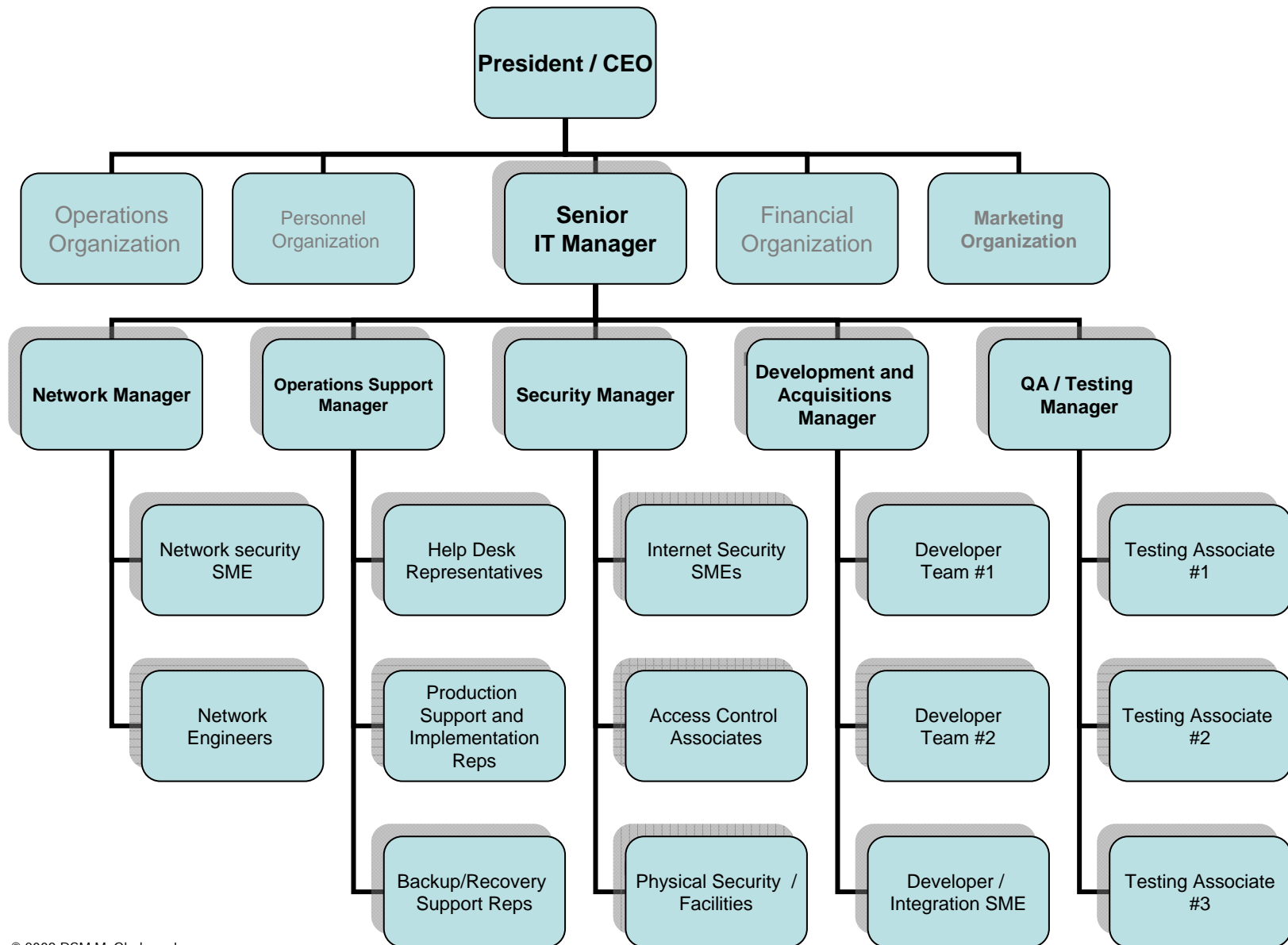
2008 RSM McGladrey Manufacturing and Wholesale Distribution Survey

– [www.rsmmcgladrey.com/images/stories/2008survey.pdf](http://www.rsmmcgladrey.com/images/stories/2008survey.pdf)

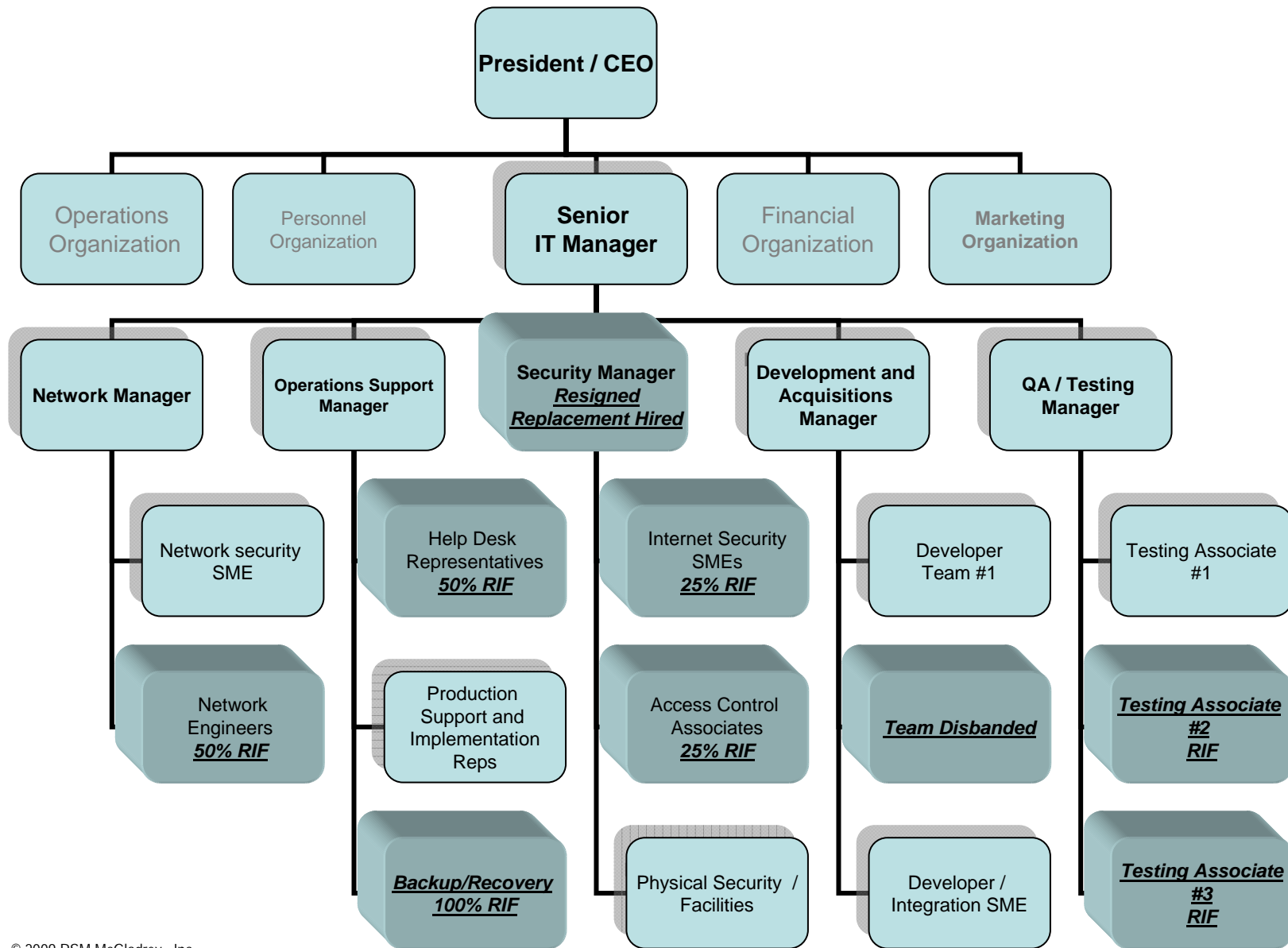
Join the 2009 Survey

– [www.rsmmcgladrey.com/mfgsurvey](http://www.rsmmcgladrey.com/mfgsurvey)

# An Example IT Org Chart For a Midsize Company



# An Example IT Org Chart For a Midsize Company (Downsized)



# Downsizing as a Solution

Downsizing reduces operating costs, but does not reduce:

- Risks to business and IT
- Dependency on IT for production support and risk mitigation
- Client demands
- Production costs, including data security and availability
- Compliance requirements

# Data Security and Integrity Risks after Downsizing

- Staff-related risks
  - Reduction in IT security staff
  - Reduction in development staff
  - Reduction in QA/testing staff
  - Reduction in operational and business staff
  - Segregation of duties
- Threats by employees
- Increase in cybercrime
- Decrease in vendor support
- Net increase in risks to data and information systems

# Security Areas at Greatest Risk

- Logical security
- Physical security
- Monitoring of activity
- Segregation of duties
- Training and documentation
- Data integrity and confidentiality
- Vendor and patch management
- Change management

# Presentation Approach

- Defining the scope of the security area
- Identifying controls to address downsizing risks
- Describing most effective actions to implement the controls

# Logical Security - Scope

- User access
  - Outwardly facing services, external connectivity
  - Internal network segmentations
  - Server access
  - Application and database functional access
- File transmissions and data exchange
  - Secure Sockets Layer (SSL)
  - Secure File Transfer Protocol (SFTP)
  - Secure email
- Intrusion detection and prevention
  - Antiviral tools
  - Management of ports and services
  - Firewalls, Web page blocking, intrusion detection system (IDS) and intrusion prevention system (IPS) applications

# Logical Security - Controls

- User access
  - Password and passkey rules and management
  - Termination notifications, access review
- File transmissions and data exchange
  - Data transmission tunneling and encryption
  - VPN solutions for working remotely
- Intrusion detection and prevention
  - Hardening of outward-facing servers, firewalls
  - Monitoring of access logs
  - Antiviral software for all servers and user systems

# Logical Security - Actions

- User access
  - Enforce strong password policies and procedures
  - Review user lists, roles and access levels
- File transmissions and data exchange
  - Review transmission connections, change passkeys, encrypt
  - Review VPN access and limit or remove all other remote access
- Intrusion detection and prevention
  - Penetration testing
  - Standardized server configurations
  - Configure firewalls to exclude all but known and trusted
  - Frequently monitor access and intrusion detection logs
  - Enable automatic update features for trusted antiviral sources

# Physical Security - Scope

- Physical access
  - Secured entry
  - Visitor policy and procedures
- Environmental conditions
  - Datacenter environment
  - Backup power sources and power distribution units (PDUs)
  - Vendor management for facilities

# Physical Security - Controls

- Physical access
  - Key and keycard control facilities, centralized management
  - Notification procedures for terminations
  - Entry logs and visitor logs created and reviewed
- Environmental
  - System maintenance schedules
  - Alert notification systems inform responsible staff
  - Contact information for facilities vendors

# Physical Security - Actions

- Physical access
  - Review all physical security systems and access lists.
  - Require all access be approved
  - Inspect all entry points and logs office suite and data center.
  - Ensure reception staff enforce employee and visitor access
  - Ensure doors require entry by keycard or keys,
  - Visitors met at the door, logged and escorted
- Environmental conditions
  - Review and update contact information for facilities vendors
  - Ensure preventative maintenance schedules are kept
  - Install alert systems to cover off-hour environmental risks
  - Adjust environmental controls

# Monitoring of Activity - Scope

- Monitoring controls—mostly detective controls
- Electronic monitoring of activity, including:
  - Access logging
  - Database change logs
  - Production module change logs
  - Source code control
  - Problem logging
  - Administration activity
  - Firewall logs of attempted external access
- Regular review of the logs for suspicious activity
- Automated alerts for access beyond tolerance levels
- Retention of logs for long-term investigation

# Monitoring of Activity - Controls

- Properly installed logging tools recording detailed targeted activity
- Automated log review capabilities
- Secured and archived logs
- Updated contact information for alerts
- Prepared procedures for removing access and isolating unauthorized users

# Monitoring of Activity - Actions

- Review current logging and expand
- Implement automated log reviews and alert tools with current contact lists
- Enhance electronic network monitoring with management alerts
- Implement data base logging with alerts of excessive activity
- Develop and install electronic dashboards with alerts on management desktops

# Segregation of Duties - Scope

- Business roles and IT support roles
  - Access to resources
- Conflicting responsibilities in IT
  - Development, testing, promotion to production
- Downsizing results in elimination of people not responsibilities
  - Responsibilities reassigned
- Management downsizing results in loss of oversight
  - Logging, monitoring and upper management approvals

# Segregation of Duties - Controls

- Review regularly
- Definition and adoption of appropriate roles
- Implementation of access controls to enforce segregation
- Delegation and documentation of reviews and approvals

# Segregation of Duties - Actions

- Management should meet prior to the downsizing to reassign roles and tasks, to review and revise matrices for any conflicts.
- Create current process flows that include roles and responsibilities.
- Update segregation of duties matrices for all critical business and support functions.
- Complete segregation of duties procedures for dual access, management review and management approval.
- Develop mitigating manual and system controls to provide improved management oversight of activities.

# Training and Documentation - Scope

- Support group training
- User training
- Technical documentation
  - System configuration settings
  - Application design and source code documentation
  - Quality assurance (QA) test plans and results
  - Implementation instructions
  - End user documentation

# Training and Documentation - Controls

- Documentation creation
- Documentation secure storage
- Documentation review and update
- Training for operational roles
- Training for developmental roles
- Training for QA and testing procedures
- User training

# Training and Documentation - Actions

- All existing documentation gathered and evaluated
- Close all remaining documentation gaps
- Organize training sessions
- Ensure data security and integrity are addressed

# Data Integrity and Confidentiality - Scope

- Integrity
  - Incoming data sources
  - Internal datasets
  - Outbound data
- Confidentiality
  - Client data
  - Compliance with privacy laws
  - Proprietary data including intellectual property

# Data Integrity and Confidentiality - Controls

- Incoming data receipt, verification, transformation and database insertion
- Outgoing data file creation, verification and transmission
- Data access on in-house servers
- Secure database backup and recovery

# Data Integrity and Confidentiality - Actions

- Update documentation of operational procedures
- Adopt enhanced encryption methods and procedures
- Reinforce, limit access to, and further automate data transmission procedures
- Partition data storage in secure partitions
- Add data validation procedures to ensure data is not corrupted during processing
- Limit administrative access to systems and data
- For critical systems, log activities and review logs
- Develop recovery programs for all critical data that provide roll-back capabilities

# Vendor and Patch Management - Scope

- Software vendors for production services
- Hardware vendors for network infrastructure
- Vendor sourced software changes for production environment
- Out-sourced providers of support and development services

# Vendor and Patch Management - Controls

- Related controls and administration of controls
  - Vendor communication for update notifications
  - Vendor contract terms
  - Patch acceptance procedure and logs

# Vendor and Patch Management - Actions

- Make full use of automated options for installing patches and updates in firewalls and anti-virus software
- Document acceptance testing procedures and follow change control procedures
- Reduce seat license levels in software contracts
- Negotiate service contracts more vigorously to receive reduced rates
- Ideal time to upgrade hardware at much reduced costs
- Consider vendor support of servers to replace in-house system administrators

# Change Management - Scope

- Software Development Life Cycle for internal application and database changes
  - Change request process
  - Phases of designing, development, testing, documentation and implementation
- Hardware acquisitions and installations
- Software purchases, upgrades and installations
- New client activations
- Departing client removals
- Outsourcing or co-oping support functions

# Change Management - Controls

- Management oversight of change process
- Re-assignment of duties in compliance with segregation of duties
- Place higher requirements on initial request and approval process

# Change Management - Actions

- Software development life cycle adjustments:
  - Increased management oversight for request and approval
  - Extend development periods
  - The reassignment of roles to remaining staff
  - Additional management review and approval at each development stage
  - Outsource of the entire development cycle or portions
  - Consolidation of applications and decommissioning of aging servers and applications
- Prioritize changes, test thoroughly, approval and acceptance procedures

# Final Thoughts

- Begin now to prepare for contingencies if downsizing occurs within the IT area
- Preparing strategies for handling downsizing events
- Do more with less
- Remember Murphy's law
- To maximize results, concentrate efforts on the eight security areas with greatest downsizing risk
- Be vigilant