ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Inside the Data Center

What an auditor needs to know

Course Objectives

- Understand what a data center looks and “feels” like
- Know what to look for in a data center and what questions to ask
- Deepening understanding of controls that are typically performed within a data center
- Learn a bit (but not too much) about your presenter

Agenda

- Data Center audits in today's world ?
- Introduction: What is a data center ?
- Key audit considerations.
- Industry Good Practice Considerations
- Sample Audit Objectives
- Key takeaways

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

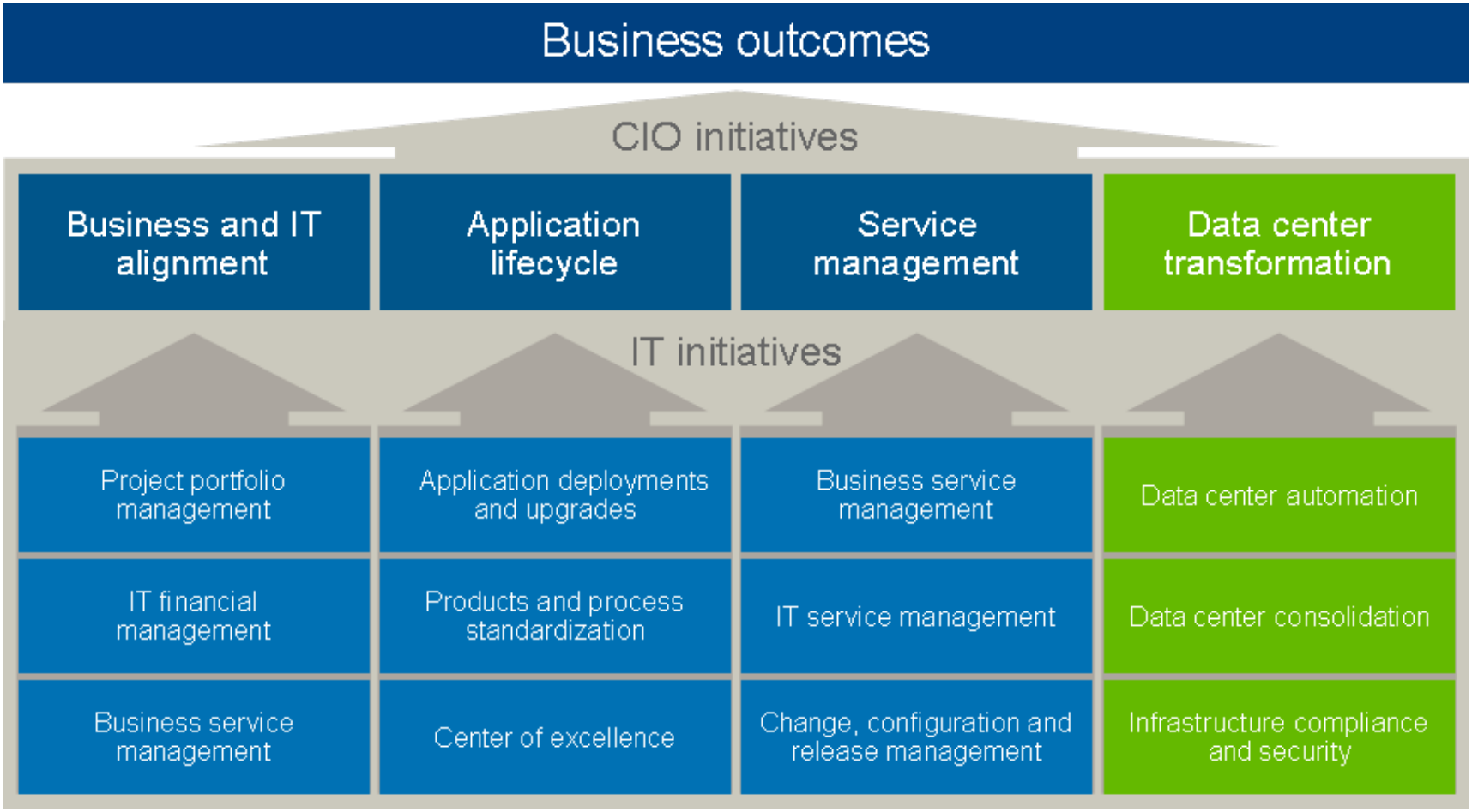
ISACA
Serving IT Governance Professionals
San Francisco Chapter

Data Center audits in today's world ?

The Corporate Business Challenge

- Reduce organization and infrastructure complexity
- Reduce and effectively manage the IT budget
- Increase systems availability and reliability
- Improve overall asset utilization
- Improve overall ease of services deployment
- Simplify and standardize processes and procedures
- Effectively scale to meet growing business needs

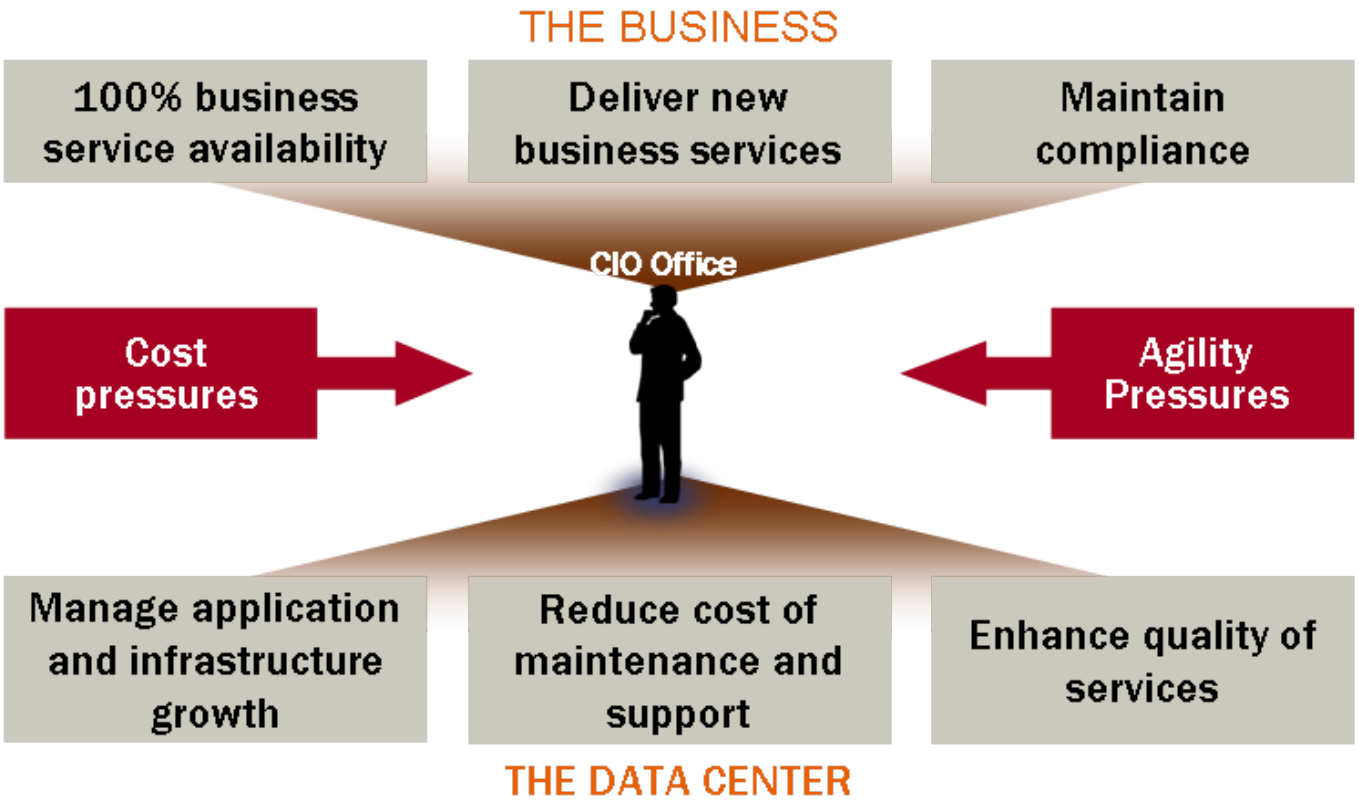
The CIO's challenge



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

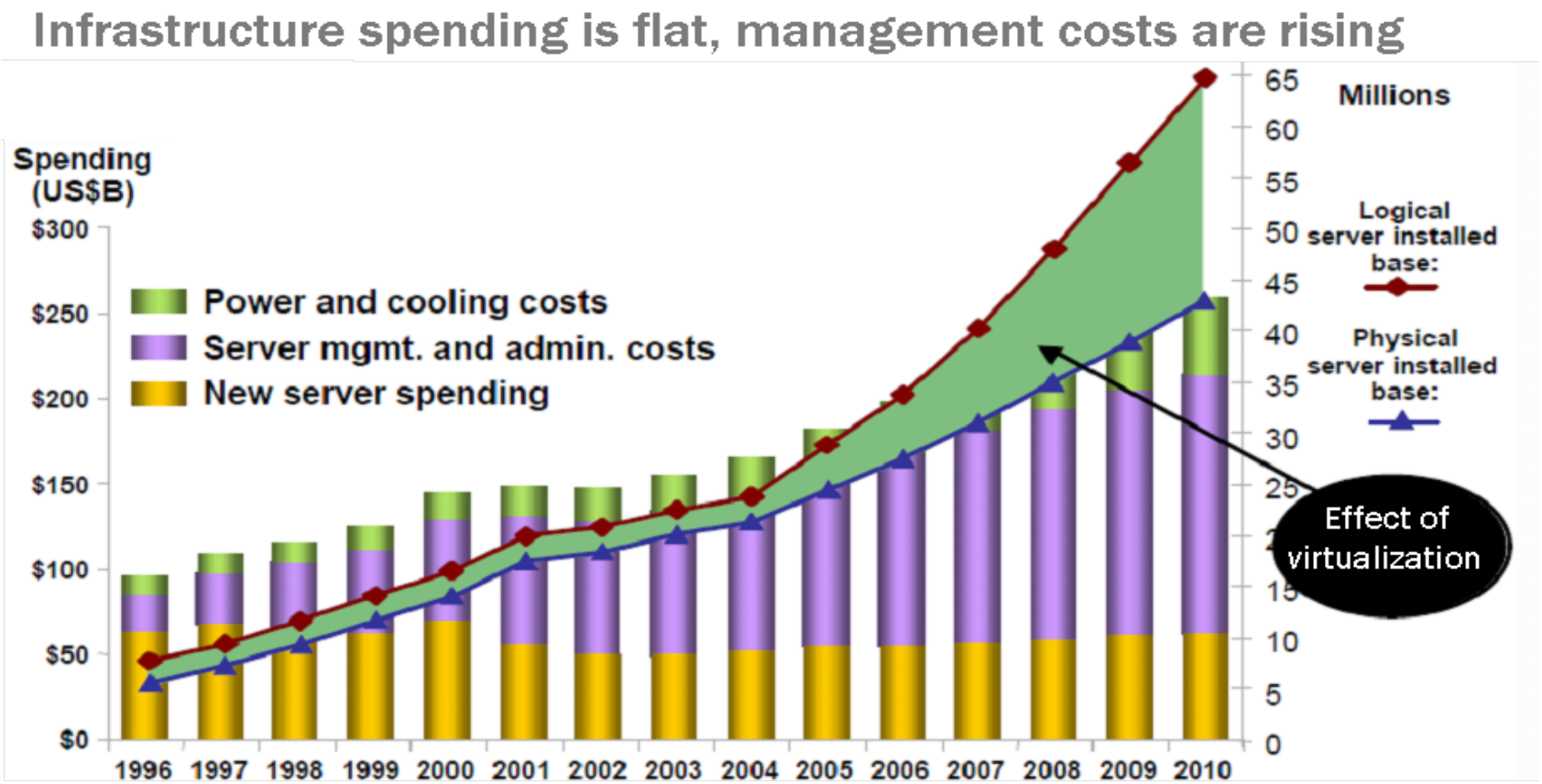
Data Center priorities
Reduce Costs, Increase Agility

Easy to say, difficult to do



ISACA
Serving IT Governance Professionals
San Francisco Chapter

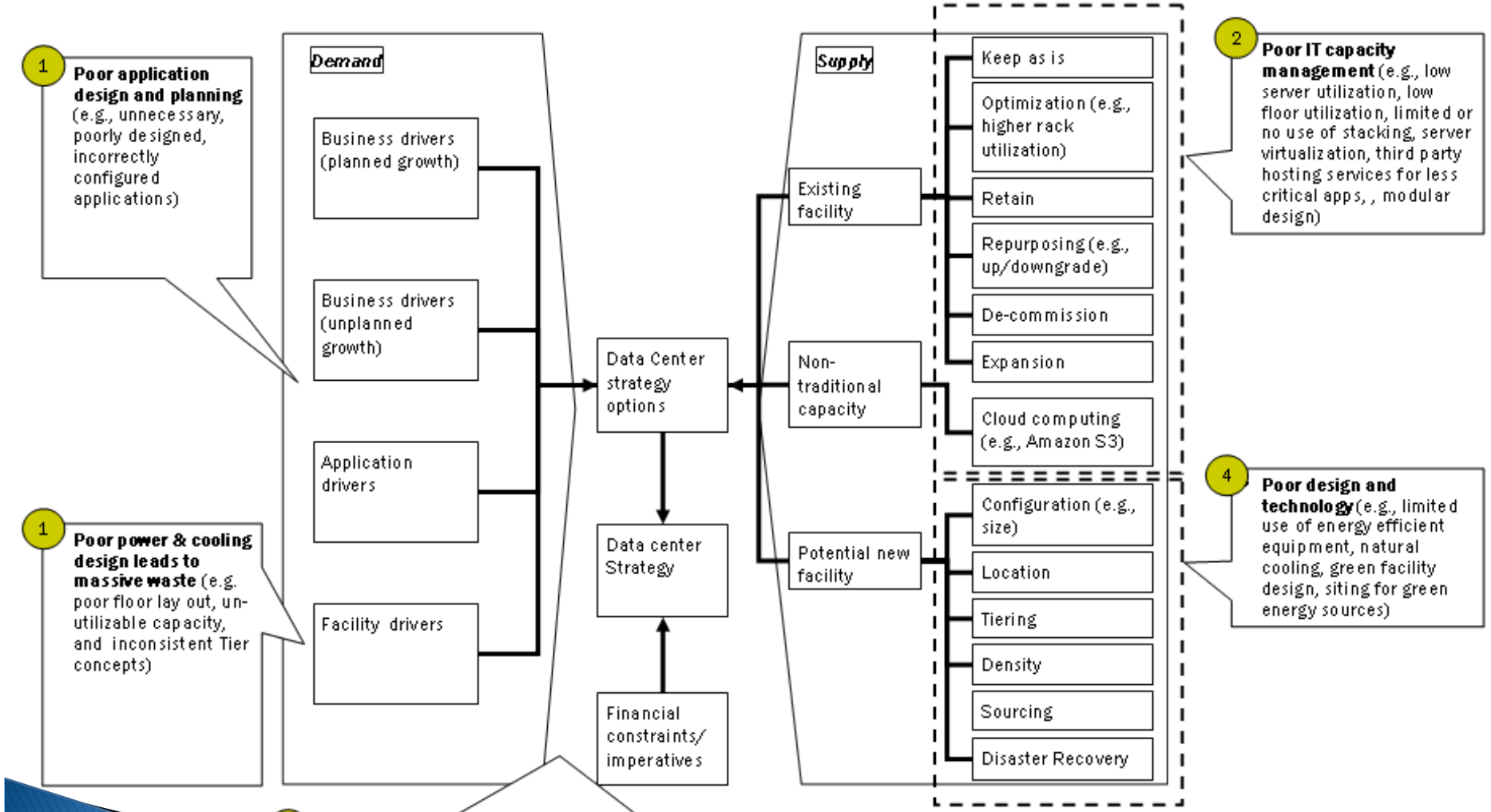
Data Center Economics



Source: IDC, "CIO Strategies to Build the Next Generation Data Center," Doc # DR2007_5VT, February 2007.

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Data Center Inefficiencies



Source: McKinsey analysis

ISACA
Serving IT Governance Professionals
San Francisco Chapter

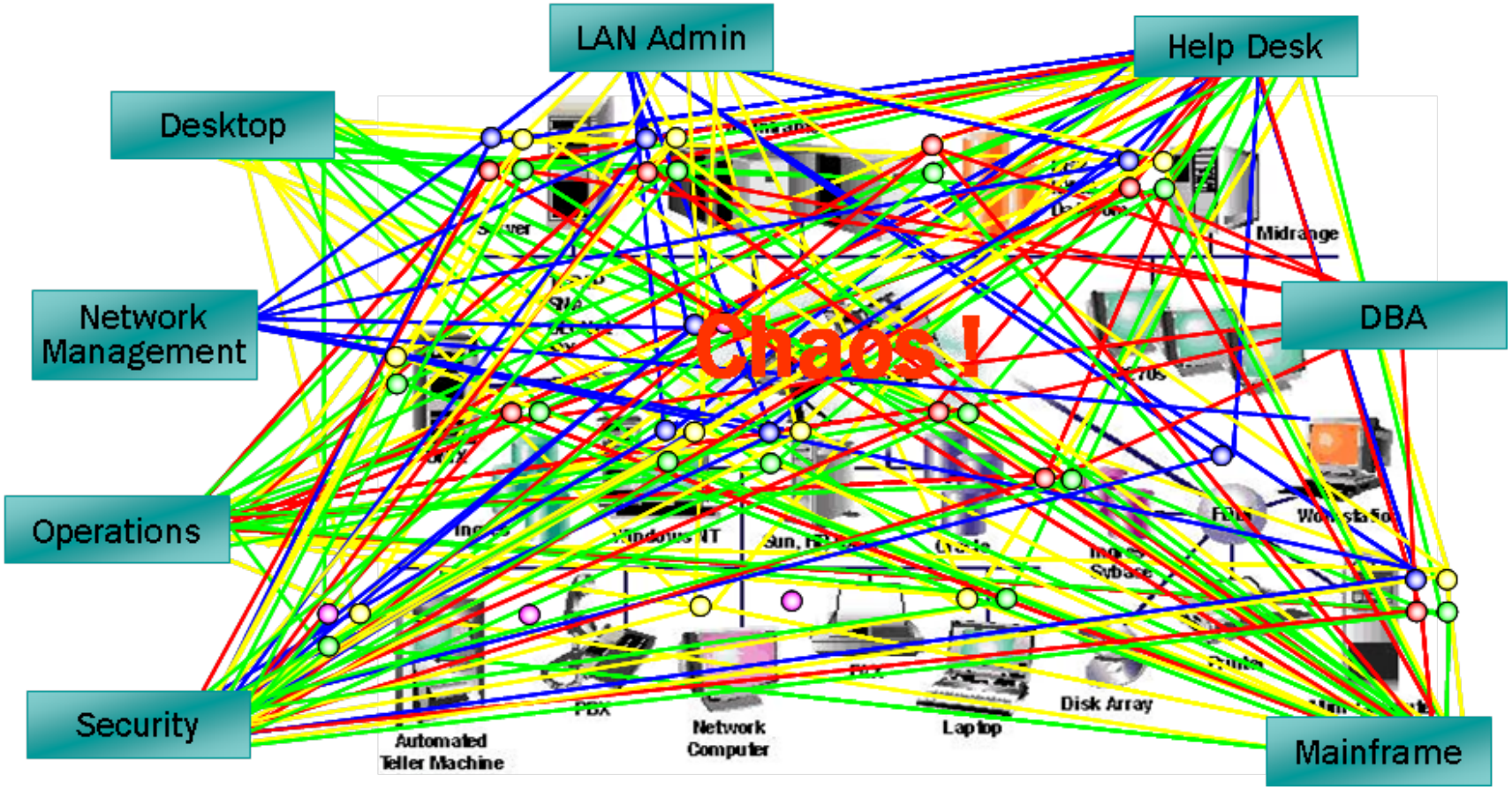
ISACA
Serving IT Governance Professionals
San Francisco Chapter

Introduction: What is a data center ?

Components of a Data Center

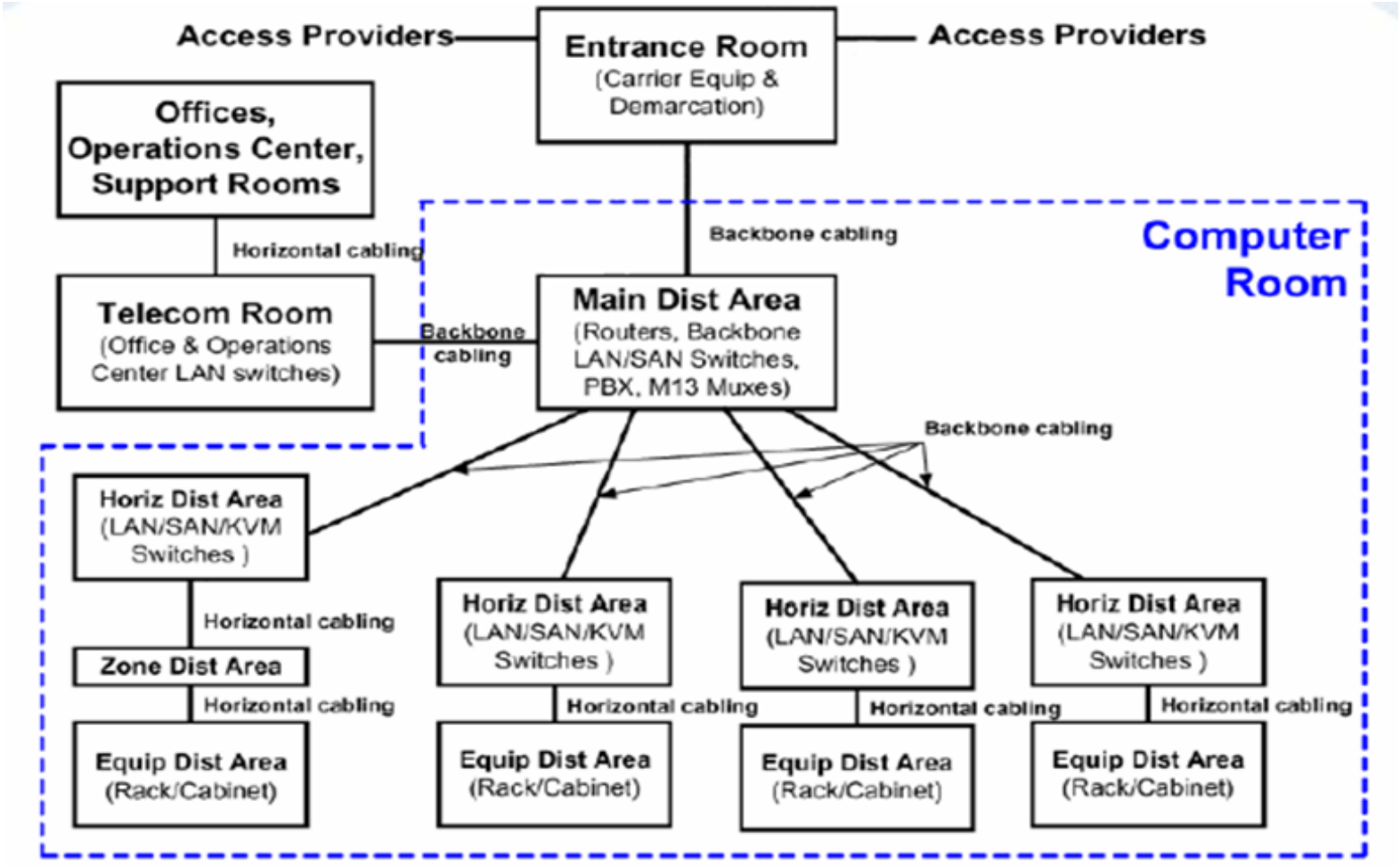
- Servers
- Legacy mini-computers
- SAN and NAS equipment
- Tape backup systems
- Network equipment
- Phone system (switch and/or servers)
- Video equipment/encoders
- Audio/paging system
- Security control system/server

Components of a Data Center



ISACA
Serving IT Governance Professionals
San Francisco Chapter

Example of basic center topology



Source: TIA 942

Types of Data Center

Tier	Availability	Description
Tier 1: Basic	99.671%	▸ Single path for power and cooling distribution, no redundant components ▸ May or may not have raised floor, UPS, generator ▸ 3 months to implement ▸ Annual downtime of 28.8 hours
Tier 2: Redundant Components	99.741%	▸ Single path for power and cooling distribution, includes redundant components (N+1) ▸ Include raised floor, UPS, generator ▸ 3 to 6 months to implement ▸ Annual downtime of 22 hours
Tier 3: Concurrently Maintainable	99.982%	▸ Multiple power and cooling distribution paths but with only one path active, includes redundant components (N+1) ▸ Includes raised floor and sufficient capacity and distribution to carry load on one path ▸ 15 to 20 months to implement ▸ Annual downtime of 1.6 hours
Tier 4: Fault Tolerant	99.995%	▸ Multiple active power and cooling distribution paths, include redundant components (2 (N+1), i.e 2 UPS each with N+1 redundancy) ▸ 15-20 months to implement ▸ Annual downtime of 0.4 hours

Source: Uptime institute.

ISACA® Serving IT Governance Professionals
San Francisco Chapter

Sites: Where are Data Centers

- Closets
- Part of Buildings, stand alone
- Geography
- Co-sourcing
- Out-sourced

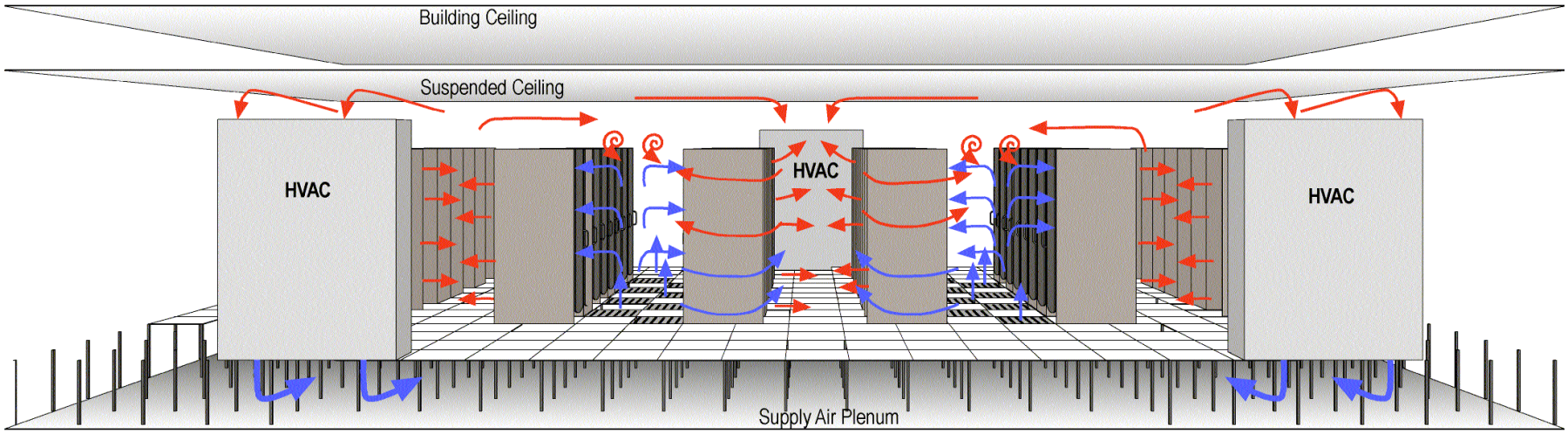
Considerations

- Telecommunications cabling system
- Equipment floor plan
- Electrical plans
- Proximity to electrical service and electro-magnetic interference (EMI) sources
- Architectural plan
- HVAC
- Security
- Lighting system

Inside the Raised Floor – Functional Areas

- Server and storage areas
- Tape library
- Network areas
- Power

The Raised Floor



The Data Center

- Walls within Walls
  - Segregate systems and support staff
  - Slab-to-slab
  - “Cages”
  - Locked racks
- Beneath the tiles and over the head
  - Look and feels
  - Cables
  - Cooling
- Access
  - Mantraps
  - Biometrics vs. keycard access
  - Front door facility access
- Power
  - Redundancy at the PDU level
  - Redundancy at the power feed level
  - Dual grids
  - Backup generators
  - Battery backup
  - N+1 Redundancy and PDU Failure

The Data Center

- Server and Storage Areas
  - Rows or racks and how they are anchored
  - Concept of patch panels
  - Storage – Disk arrays
  - Servers – Mainframe, midrange, and Intel
  - Exotic (e.g. VRUs) and appliances

- Network Area
  - Entry to the Data Center and redundancy
  - Central and distribution areas
  - Patch panels

- Layout & Thermal Considerations
  - Hot/cold zones
  - In-rack configurations

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Key Audit Considerations

Data Center – Areas of Audit Focus

- Overall Data Center
- Consoles and Terminal Servers
- Physical locks and equipment access
- Surveillance systems
- Vendor Management
- Tape Management
- Efficiency Audits
- Industry Good Practice Considerations

Overall Data Center

What to look for ?

- Disaster Recovery
- Business Continuity Plan
- Data Integrity
- Data Security

Consoles and Terminal Servers

- What they are
- What is the risk
- What to look for (“heads”, KVM)
- Controls to identify
- Sample recommendations

Physical Locks and Equipment Access

What to look for:

- Keys/keycards
- Access logs
- Number of systems accessed per key/keycard
- Controls to identify
- Sample recommendations

Surveillance Systems

What to look for:

- Camera's visible or obscured/motion driven
- Real-time monitoring/archival
- Controls to identify
- Sample recommendations

Vendor Management

What to look for

- Escorts into the data center
- Logging of access
- In combination with access to consoles

Tape Management

What to look for

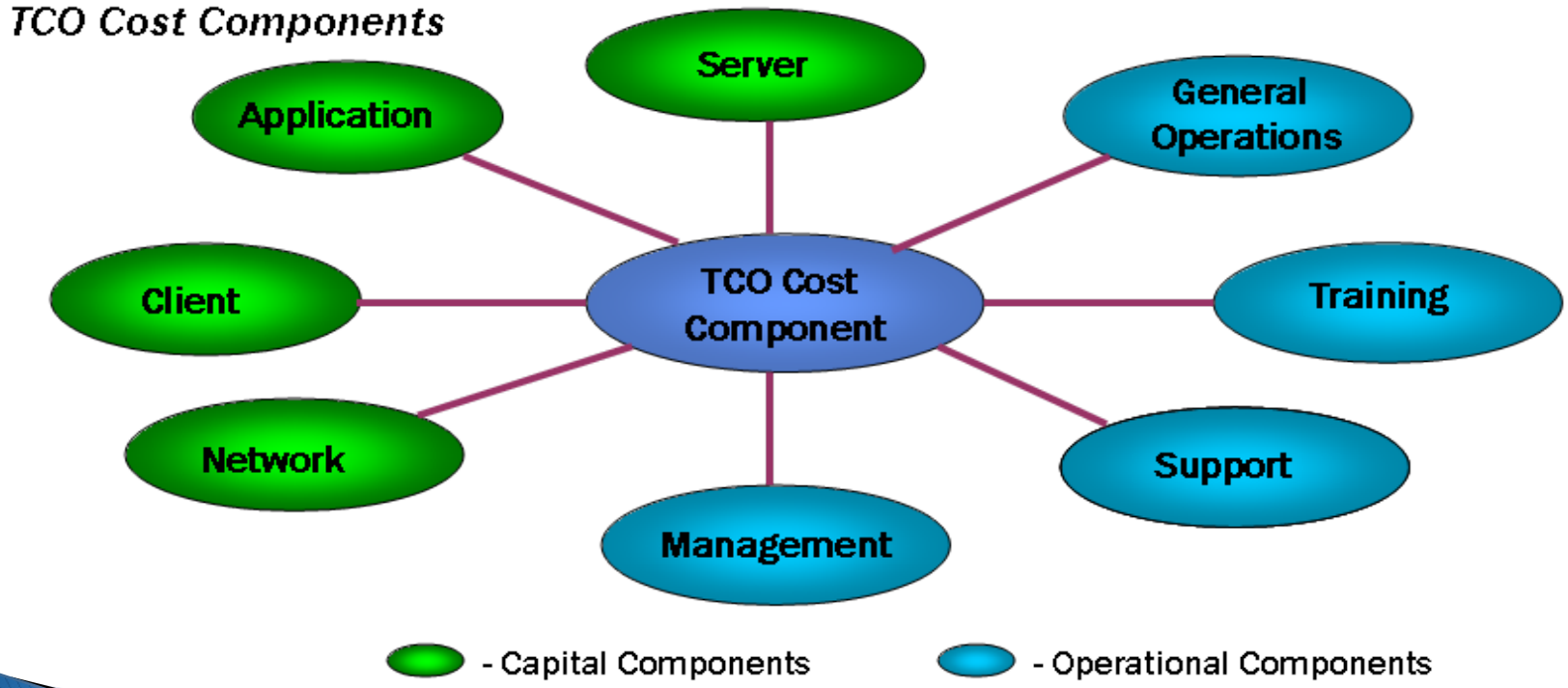
- Labels, loose media
- Qualified tape operators
- Locked transport cases
- Logs
- Libraries versus racks

Efficiency Audits

- CISA and efficiency audits ??
  - Current market scenarios demand this attention.
  - Opportunity to expand area of reach.
  - Opportunity to make an impact on the bottom line.

Total Cost of Ownership

Total Cost of Ownership (TCO) is the total cost per seat incurred across an information center through provision of continuous computing services to its users.



Total Cost of Ownership

TCO Cost - Capital Components Breakdown

Network

H/W
- Cable
- Hubs
- Routers
- Switches

S/W
- Network Mgt.

Client

H/W
- PC
- Monitor
- RAM upgrade
- Disk upgrade

S/W
- Operating Systems
- Utilities

Application

- Personal Prod.
- Group Prod.
- Business App.
- Database

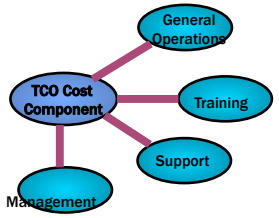
Server

H/W
- Server
- Ram upgrade
- Disk upgrade

S/W
- OS
- Utilities

Total Cost of Ownership

TCO Cost - Operational Components Breakdown



Management

- Asset Inventory
- Change/Config.
- Security
- Event/perform
- Storage
- User admin.

Support

- How to/break/fix Operating System
- Application
- Network
- Hardware

Training

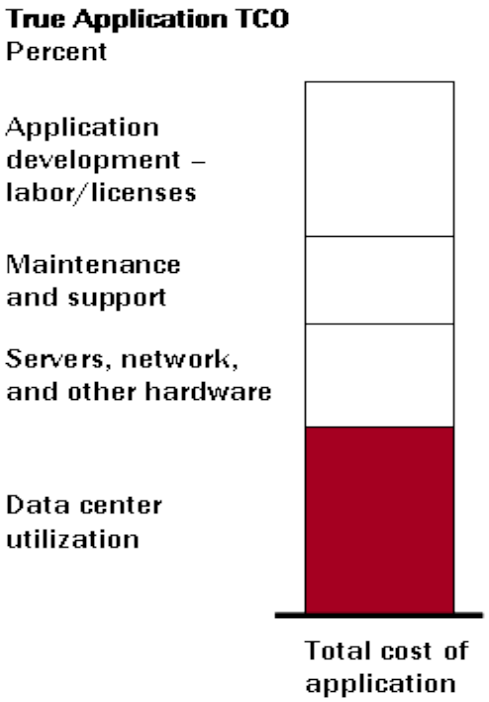
- End-user
- IT

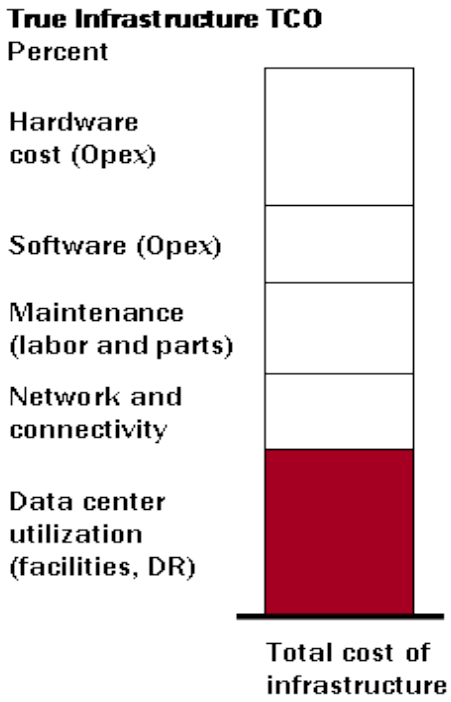
General Operations

- Architecture /Planning
- Product Testing
- Vendor Management

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Application & Infrastructure Decisions
Do they consider the TCO impact ?





Not considered in TCO business case for 'go/no-go' decision

ILLUSTRATIVE

- Limited understanding of data center TCO and limited access to relevant data
- Limited understanding of choices that can influence data center cost
- No representation of data center in design, planning, and approval process for new applications and hardware components

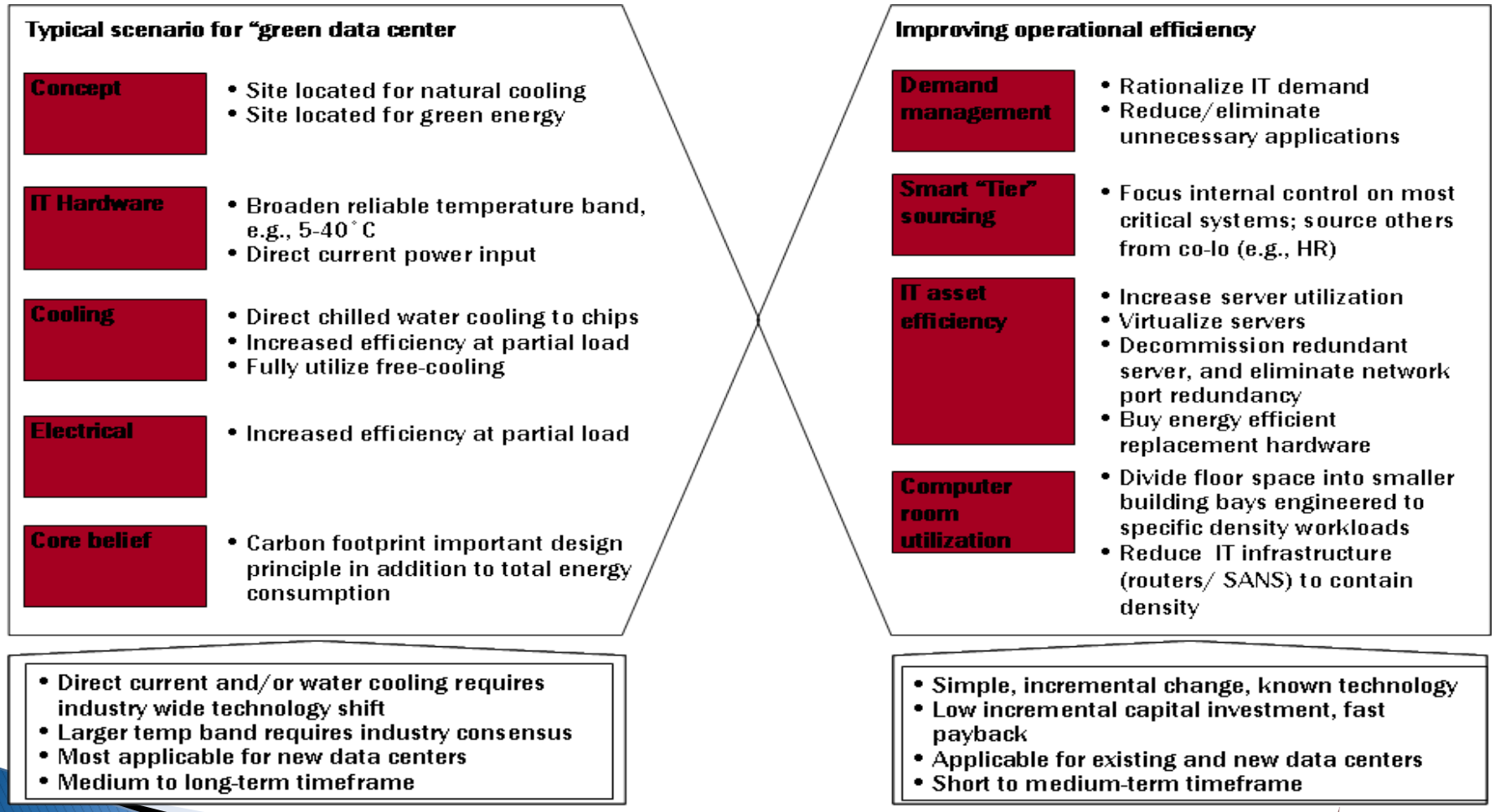
Examples of poor application decisions...
- Applications that don't reduce usage of monitors during off peak/closed hours
- Limited use of grid computing
- Computation load is not shifted among systems to maximize energy used

Examples of poor infrastructure decisions...
- Storage usage not maximized
- Limited use of MAID (massive array of idle disks)
- Poor layout design
- Equipment that is physically large

Source: Uptime Institute; EPA report; McKinsey analysis

ISACA® Serving IT Governance Professionals
San Francisco Chapter

Green vs. efficient data center.



Source: McKinsey analysis; Uptime Institute

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Industry Good Practice Considerations

Industry Good Practice Considerations

- Governance
  - CobIT
- Quality Management
  - TQM, Six Sigma, Deming, International Standards (ISO)
- Process Development & Refinement
  - ITIL/ASL, CMM/CMMI, SCOR
- Security
  - International Standards 27000 series
- Controls
  - Software as a Service (Saas)
  - SAS 70

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Sample Audit Objectives

Sample Audit Objectives

- General Review
- Financial Review
- Compliance Review
- Effectiveness & Efficiency Review
- Information and Communication Review

General Review

Audit Objective	Areas of Risk
Obtain an understanding of significant processes and practices employed, implementing, and supporting the Data Center operations specifically addressing the following components: ▸ Management philosophy, operating style, and risk assessment practices including: ◦ Awareness of and compliance with applicable laws, regulations and policies, ◦ Planning and management of Data Center Operations financial resources, ◦ Efficient and effective operations ▸ Organizational structure, governance and delegations of authority and responsibility ▸ Positions of accountability for financial and operational results ▸ Process strengths (best practices), weaknesses, and mitigating controls	▸ Data Center management systems may be ineffective and inefficient due to misalignment with their mission and not capable of meeting the business objectives ▸ Organizational structure may be inappropriate for achieving business objectives ▸ Lack of accountability could also lead to improper segregate of duties ▸ Internal controls could be assessed as not reliable where process weaknesses are substantial ▸ Information systems, applications, database, and limited electronic interfaces may be inappropriate for achieving the business objectives O ▸ perating systems may not be properly configured or maintained (patched) thus resulting in insecure systems.

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Financial Review

Audit Objective	Areas of Risk
Evaluate the adequacy of financial resources, and appropriate financial planning consistent with the objectives of the Data Center. Include the following components: • Compliance with the budgeting and approval process for the funding major equipment upgrades and replacement • Recharge for Data Centers services are consistent and appropriate. • Recharge rates are documented and approved • IT governance appropriate for adequate consideration of financial needs • Evaluate the cost benefit of lease vs. buy of capital assets • Evaluate the cost benefit of software purchases	▸ Servers and IT equipment may be acquired that are inadequate for the needs of its customers. ▸ Acquisitions of IT equipment may be made that have not been through the budget and approval process. ▸ Funding shortages may prevent the Data Center from achieving its business objective. ▸ Funding may be used to purchase resources that were inappropriate for the intended purposes ▸ Purchase versus lease decision may be flawed due to incorrect financial assumptions ▸ IT governance may not provide adequate considerations of the financial needs

Compliance Review

Audit Objective	Areas of Risk
Evaluate compliance with the regulations that the organization is expected to comply with.	▸ Non-compliance could result in the fines, penalties, and sanctions ▸ Poor security or poor performance, from lack of adequate guidance policy. ▸ Delegations of authority may be inappropriate.

Effectiveness & Effeciency Review

Audit Objective	Areas of Risk
Evaluate the adequacy of operational effectiveness and efficiency consistent with the objectives of Data Center Management. Include the following components: • Appropriate investment in human resources and equipment • Adequacy of Data Center personnel for skill and training • Self evaluation and improvement process • Personnel management • Specialization of work – centralized vs. decentralized • Appropriate management of contracts • Software and equipment changes review and approval processes • Patch vs. permanent fix problems • Process in evaluating the needs for new and/or upgrades to hardware, software, and facilities	▸ Operation effectiveness and efficiency could be compromised due to poor system performance ▸ Lack of proper planning could allow the condition of inadequate capacity to develop ▸ Self-evaluation and improvement processes may not be aligned with the directives of management ▸ Service levels may not satisfy the needs /requirements of the Data Center and its customers ▸ Paying more for services when less expensive alternatives are available.

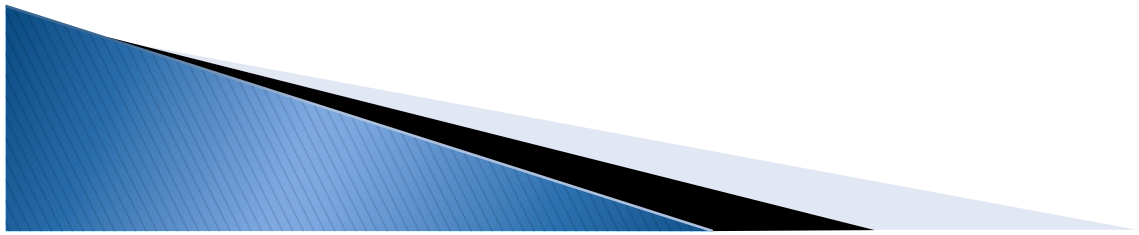
Information & Communication Review

Audit Objective	Areas of Risk
Evaluate the following routine operational activities regarding processing, applications and systems recovery, and system interfaces performance. • Logging, maintenance, and monitoring review of operational (daily computer processing) work. • Output controls and distribution • Scheduling, preparing, and running assigned processes • Incident handling, escalation and reporting as it pertains to recovery processes, hardware, software, or any operational failure • Work order process for assigning and monitoring non-operational work. • Process to communicate to management and users hardware and software system updates, changes prior to implementation. • Process to communicate to management and users any emergency hardware or software changes. • Process to communicate to management and users the status of all systems.	▸ Development and implementation of daily processes for the Data Center Operations may be inappropriate for achieving the management objectives ▸ Recovery processes may be too complicated for operational purposes and, therefore, not used ▸ Output distribution may be inappropriately distributed resulting in inefficiencies and possible compromise of sensitive data ▸ Lack of proper traffic monitoring tools may not achieve the results originally intended ▸ Lack standard procedures in logging, maintenance, and review of operational reports making the processes ineffective ▸ Improper defined backup procedures and standards may result in data unrecoverable ▸ Non-operations work may not be done properly or on a timely basis ▸ Management and users may be unprepared for system changes

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Key takeaways

Key Takeaways



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

About your speaker

Drew Luca
PricewaterhouseCoopers, LLP
(415) 498 7659
andrew.j.luca@us.pwc.com