Session 13
Adding Value Through Integrated Audits

Scot Glover, Partner
Governance, Risk & Compliance
Armanino McKenna, LLP

Mike O. Villegas, CISA, CISSP, GSEC, CEH, QSA, PA-QSA
Director of Information Security
Newegg, Inc.

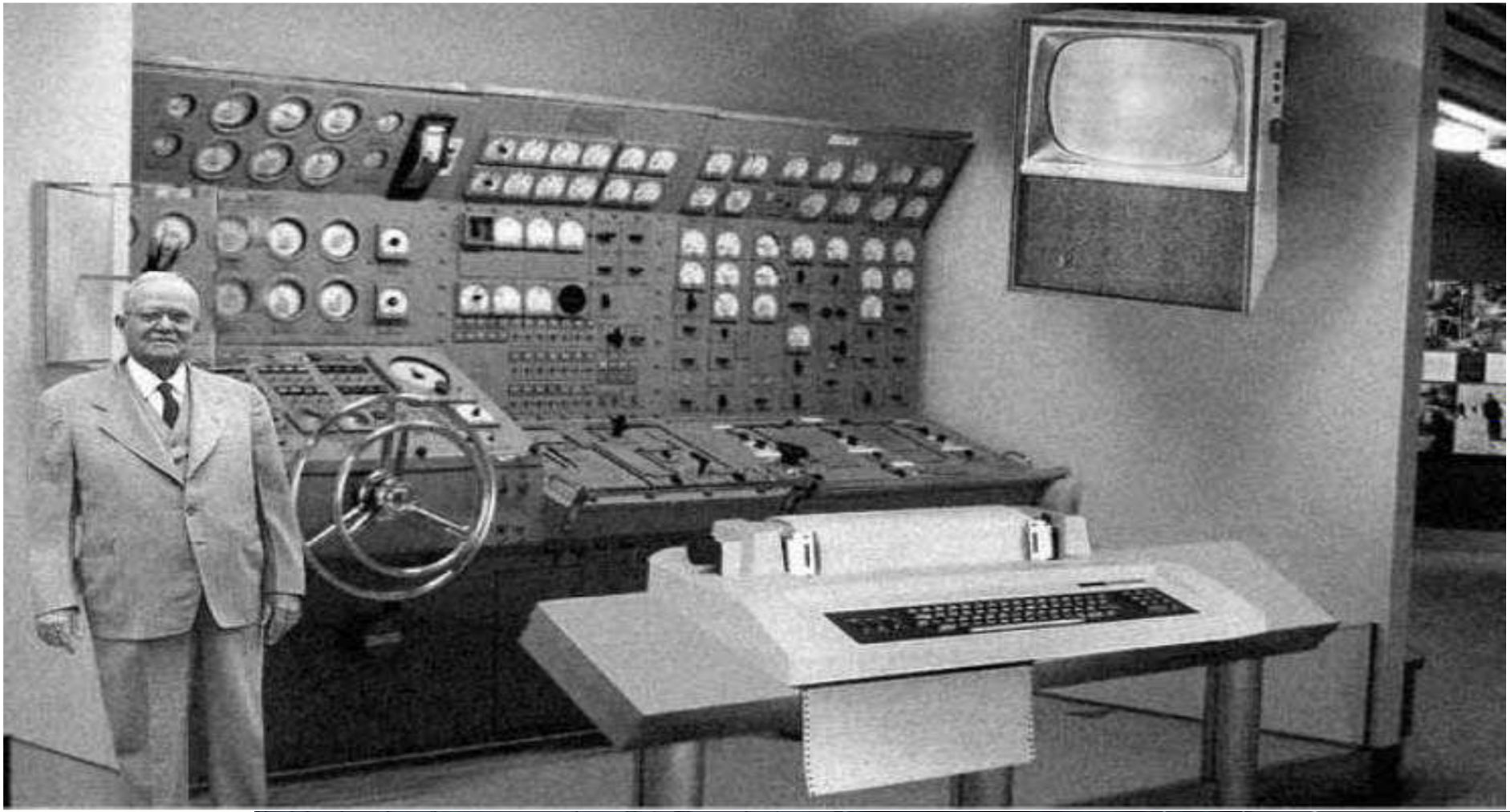
“Fun Fact”

What was the first major US corporation to use a computerized accounting system?

General Electric, 1954

– Source - AICPA

The *Future* of Computing . . . in 1954



ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Back to Business

A Quick Poll to Level Set . . .

- Who is the room today?
  - Chief Audit Executives?
  - IT Audit Directors?
  - Other IT Professionals?
  - Service Providers?
  - Others?

Course Objectives

- Why Conduct Integrated Audits??
- Challenges
- Integrated Audit Baselines
- Suggested Solutions
- Wrap-Up and Questions

Founders: Eugene Frank, Howard “Bud” Friedman, Stuart Tyranuer

They were in their early forties at the time and believed that auditing was more than just looking at general ledgers, accounting books and operational controls.

ISACA

ISACA (EDPAA) got its start in 1967, when a small group of individuals in Los Angeles, CA, with similar jobs—auditing controls in the computer systems that were becoming increasingly critical to the operations of their organizations—sat down to discuss the need for a centralized source of information and guidance in the field.

In 1969, the group formalized, incorporating as the EDP Auditors Association. In 1976 the association formed an education foundation to undertake large-scale research efforts to expand the knowledge and value of the IT governance and control field.

Today, there are 99,309 members, 192 chapter in over 160 countries.

Classification of Audits

- Financial audits
- Operational audits
- Integrated audits
- Administrative audits
- IT audits
  - Application Audits
  - IT General Controls
- Specialized audits
- Forensic audits

IT Audits

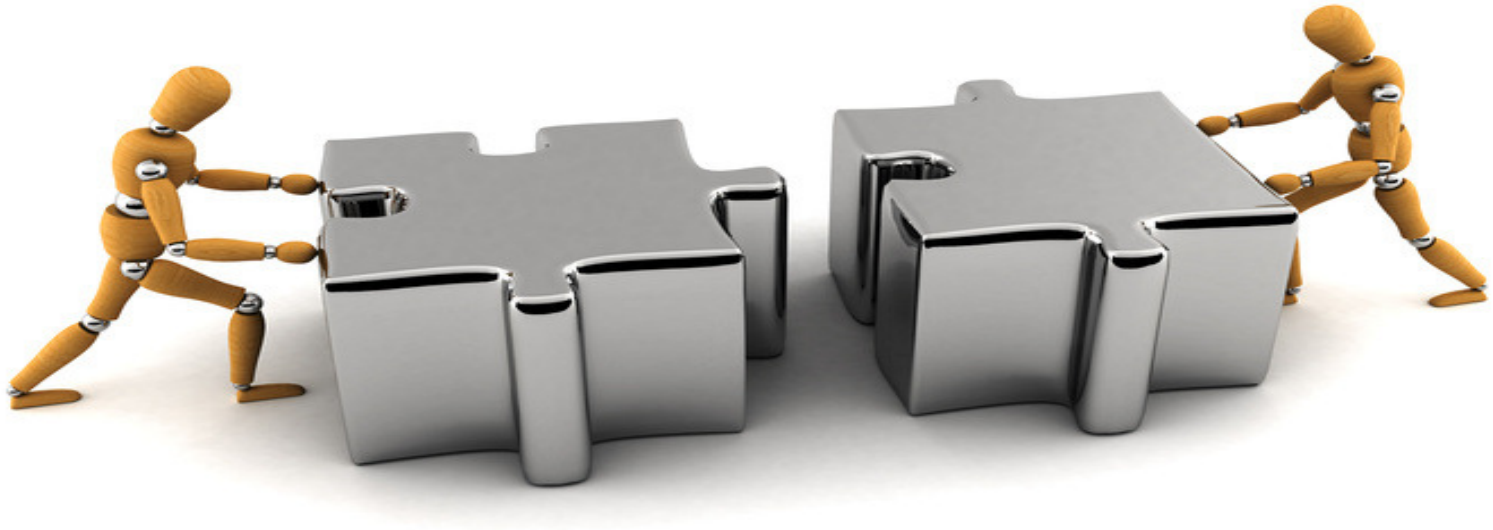
Definition of auditing

Systematic process by which a competent, independent person objectively obtains and evaluates evidence regarding assertions about an economic entity or event for the purpose of forming an opinion about and reporting on the degree to which the assertion conforms to an identified set of standards.

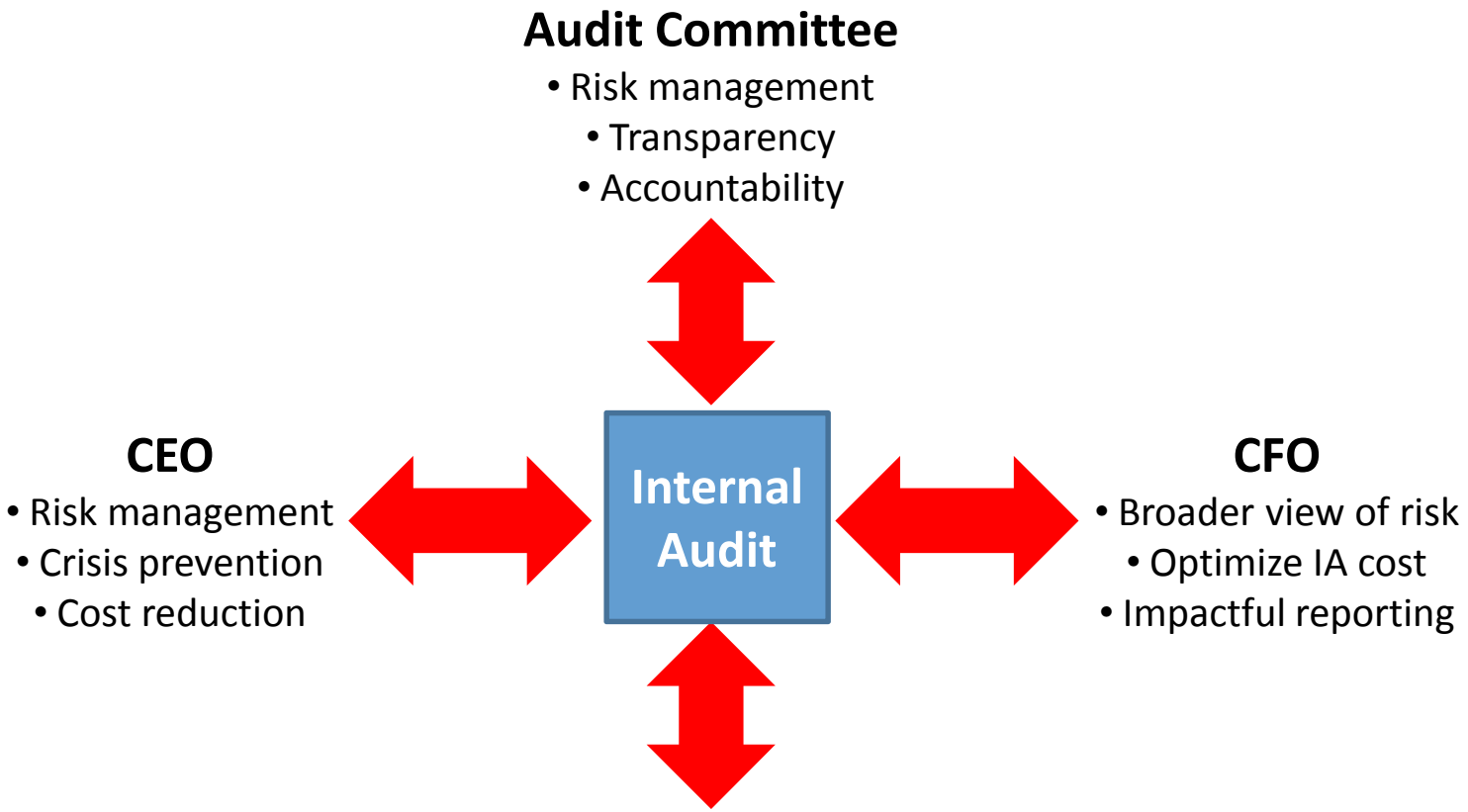
Definition of IT auditing

Any audit that encompasses review and evaluation (wholly or partly) of automated information processing systems, related non-automated processes and the interfaces between them.

WHY CONDUCT INTEGRATED AUDITS?



IA is Expected to Do More

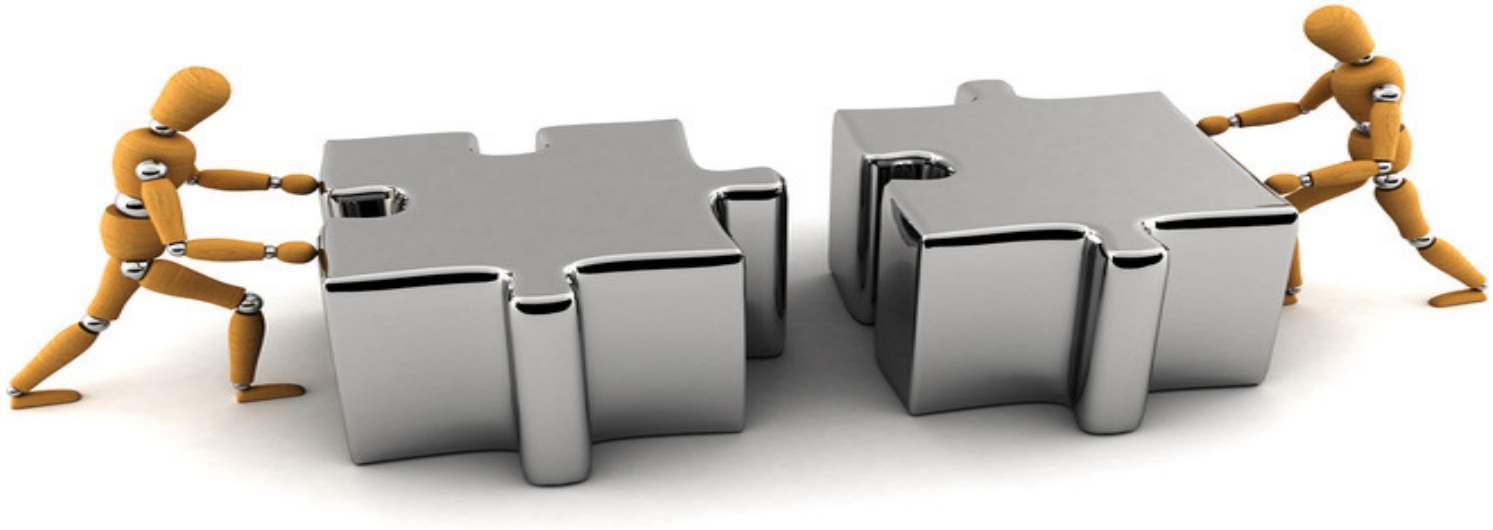


Common Expectations

- Improve risk assessment
- Better integration with other risk and compliance functions
- Optimize internal audit's efficiency and effectiveness

DO MORE WITH LESS

CHALLENGES TO EFFECTIVELY INTEGRATING OUR AUDITS



ISACA®
Trust in, and value from, information systems
San Francisco Chapter

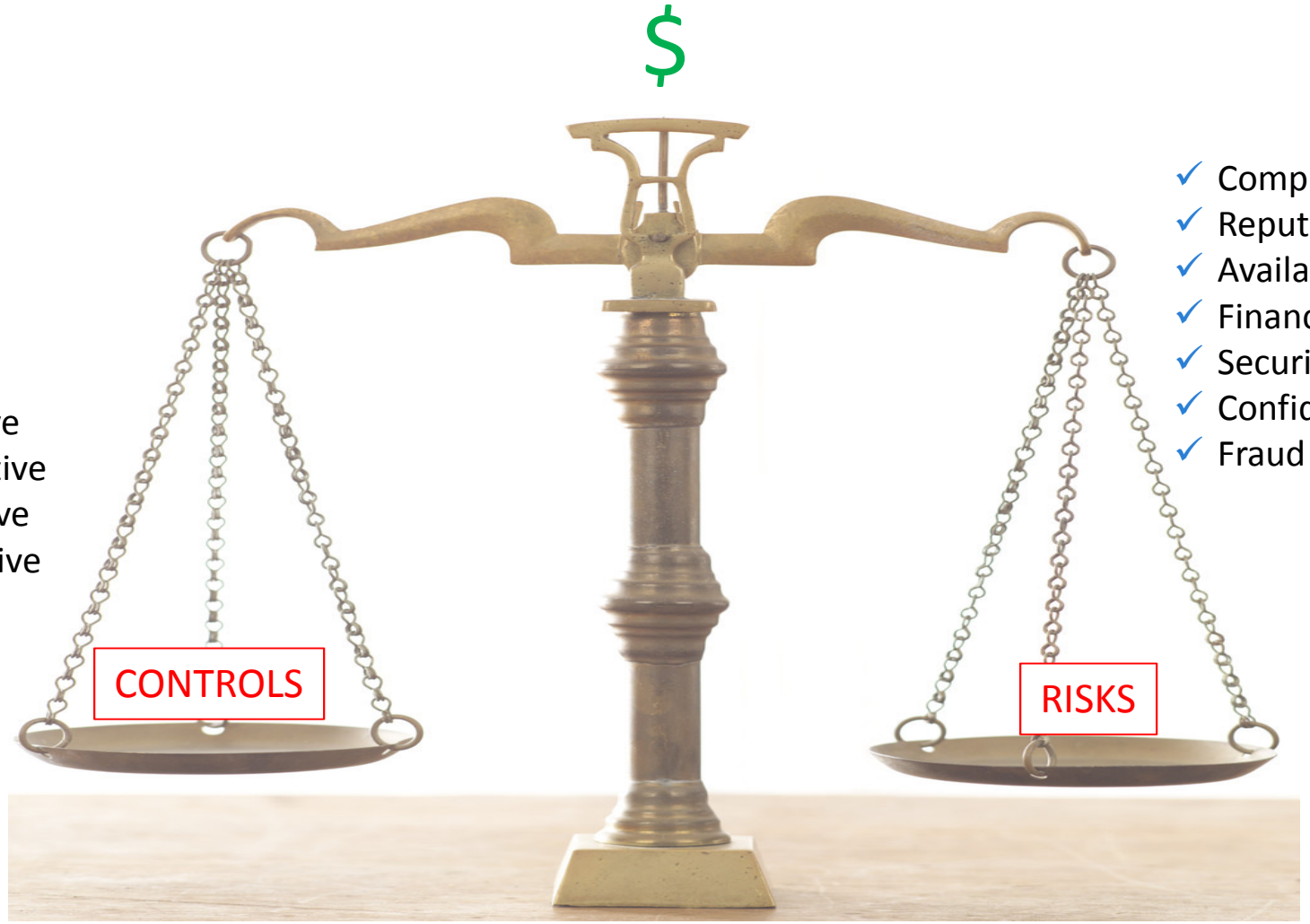
Back to Business

Challenges to Adding Value

- Unlike auditing financial statements, there are no “standard principles” for conducting IT audits
  - GAASIT?

- Rapid technological change does not allow for “leading practices” to fully develop or be recognized

Balanced View of Controls



- ✓ Directive
- ✓ Preventive
- ✓ Detective
- ✓ Corrective

- ✓ Compliance
- ✓ Reputation
- ✓ Availability
- ✓ Financial
- ✓ Security
- ✓ Confidentiality
- ✓ Fraud

STRATEGIC BUSINESS OBJECTIVES

Classification of Internal Controls

- Directive controls – training, policies
- Preventive controls – closest to point of input
- Detective controls – audit trails, logs
- Corrective controls – backup, recovery

More Challenges . . .

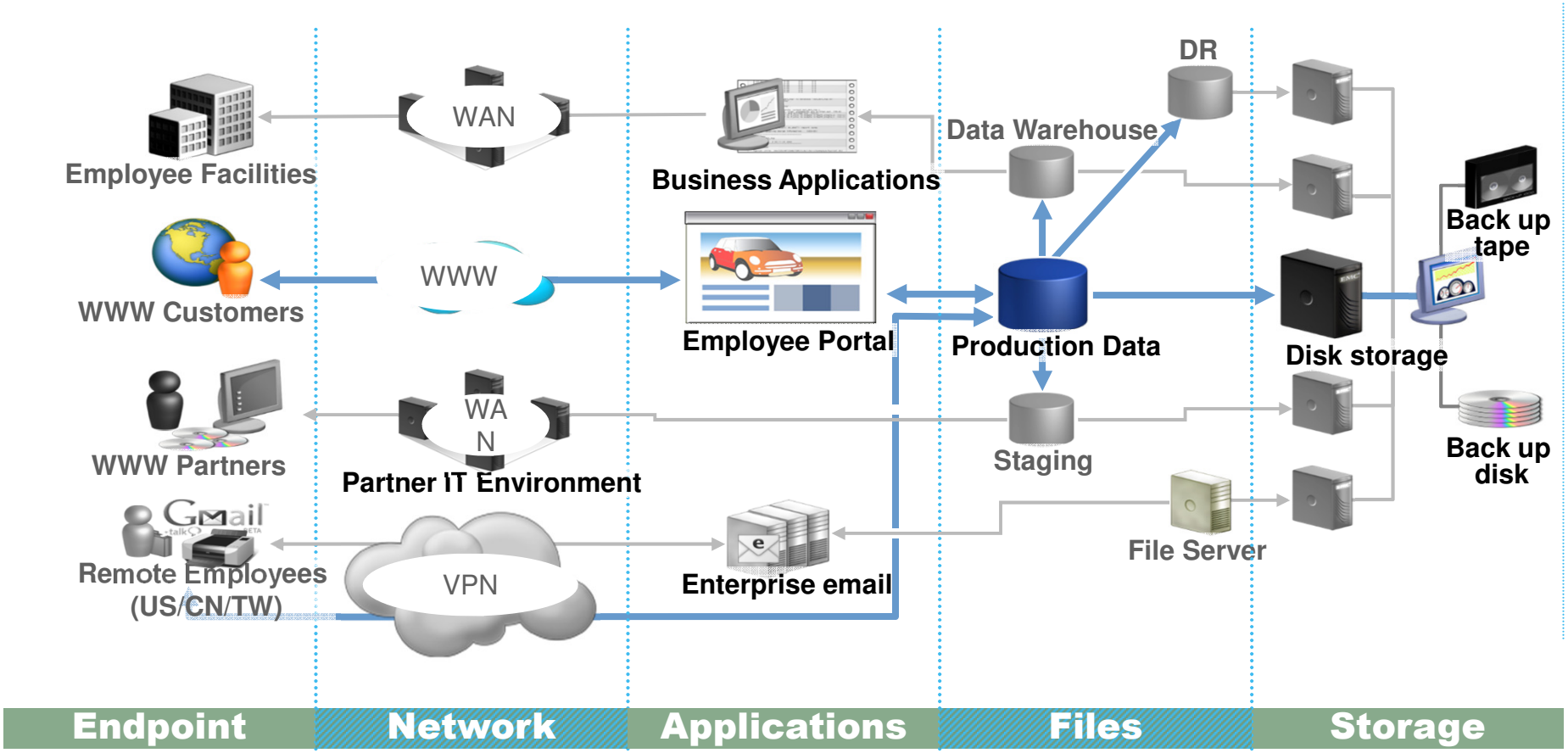
- Many different IT specialties
  - Security
  - Infrastructure
  - Operations, etc.

- IT Auditing has become a separate discipline over time

IT Controls Topology

- Why IT Controls So Difficult?

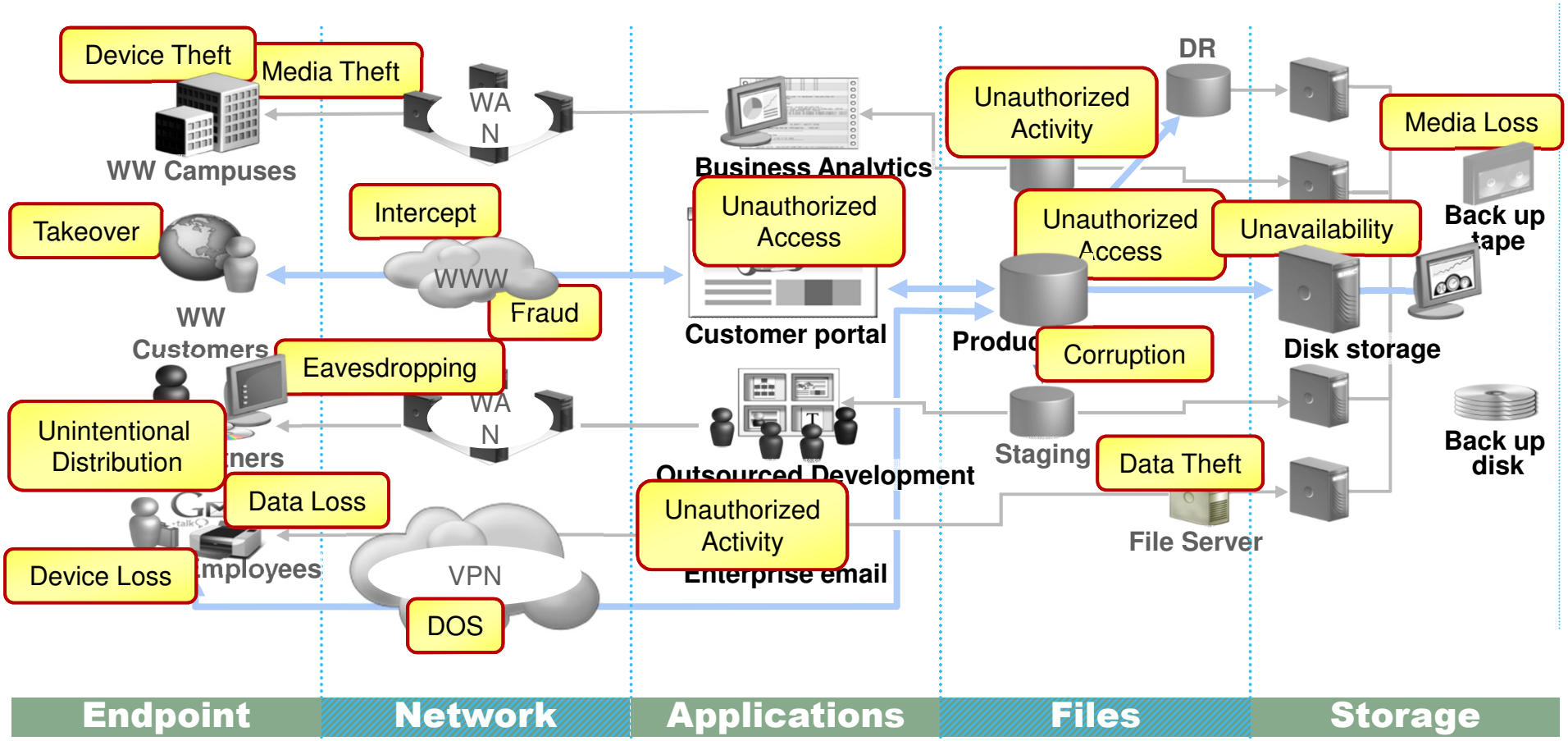
  …because sensitive information is always moving and transforming



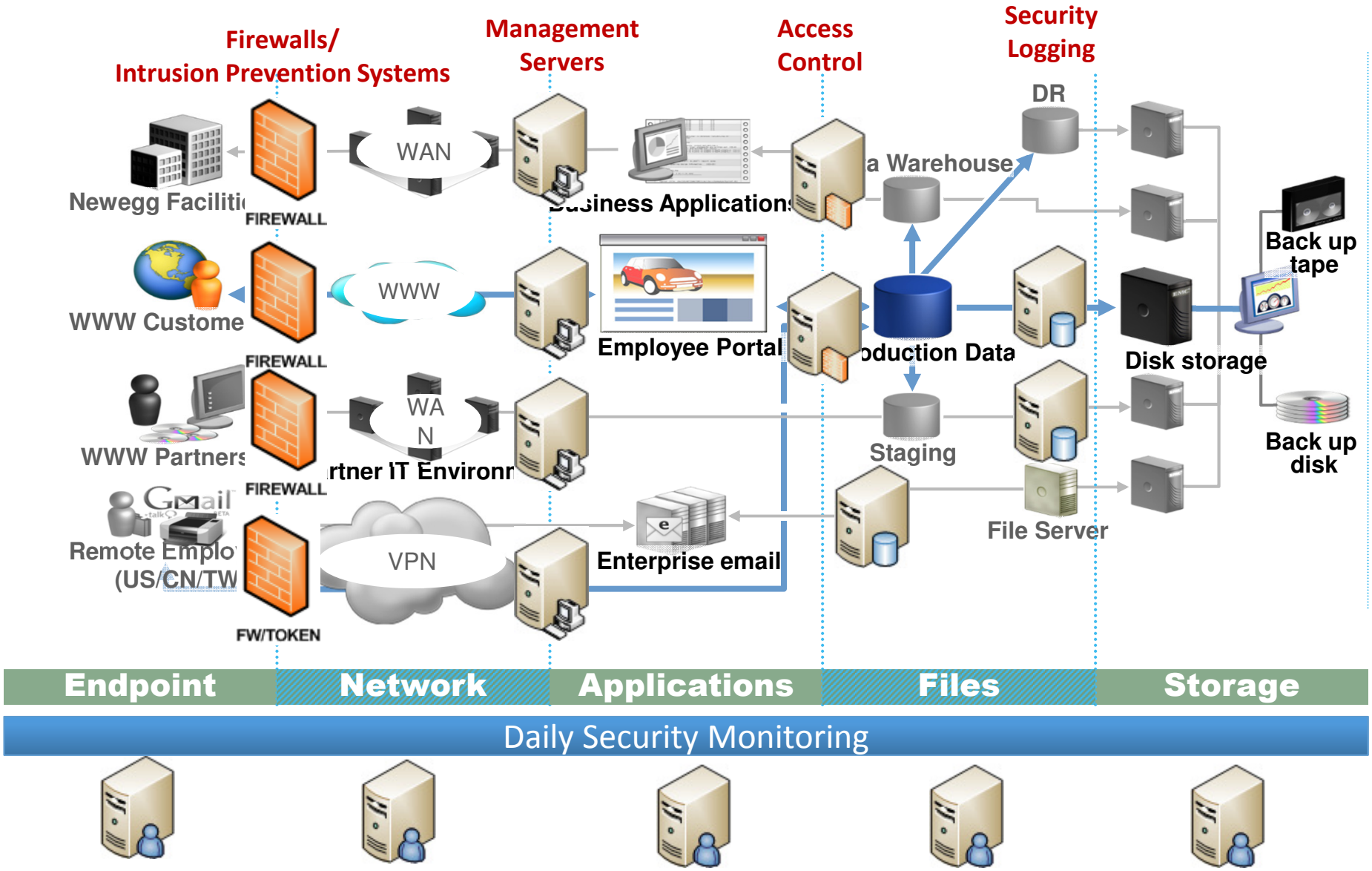
IT Controls Topology

- Why are IT Controls So Difficult?

  …because sensitive information is always moving and transforming



How Do You Manage IT Controls?

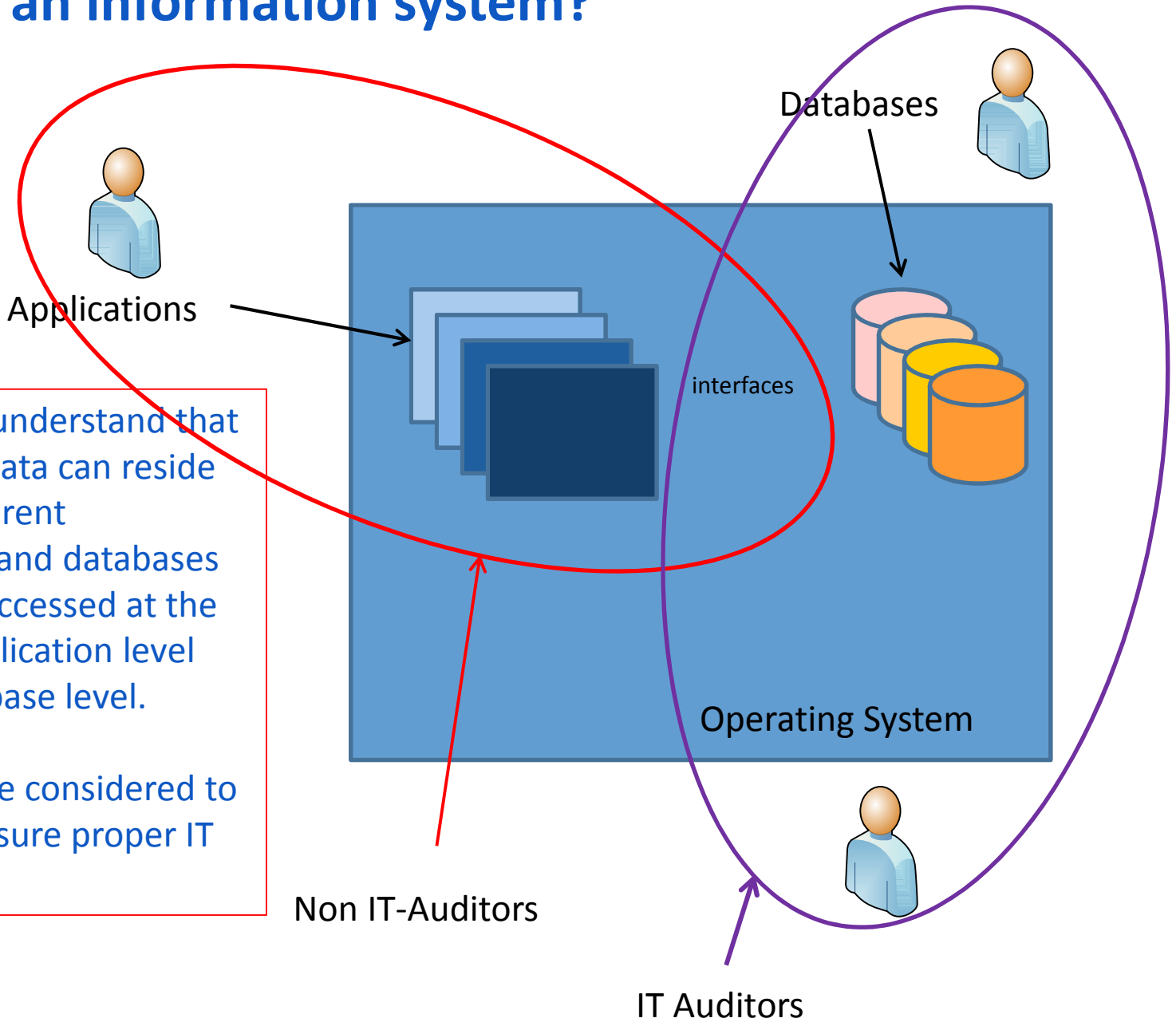


Practical Challenges . . .

- Should IT auditors address application controls because a computer system is involved?
- Should financial auditors address application controls because the processes are related to business objectives?

What is an information system?

- Hardware
- Software



We need to understand that application data can reside in many different applications and databases and can be accessed at the OS level, application level and/or database level.

All need to be considered to adequate ensure proper IT controls.

I – O - P

INPUT

OUTPUT

PROCESSING

Input / Origination Controls

Input control procedures must ensure that every transaction to be processed is entered, processed and recorded accurately and completely.

The controls should ensure that only valid and authorized information is input and that these transactions are only processed once.

- Input Authorization
  - Signatures on batch forms or source documents
  - Online access controls
  - Unique passwords
  - Terminal or client workstation identification
  - Source documents
- Batch Controls and Balancing
  - Total monetary amount
  - Total items
  - Total documents
  - Hash totals
  - Batch registers
  - Control accounts
  - Computer agreements

Input / Origination Controls

- Error Reporting and Handling
  - Rejecting only transactions with errors
  - Rejecting whole batch of transactions
  - Holding the batch in suspense
  - Accepting the batch and flagging error transactions
- Input Control Techniques
  - Transaction log
  - Reconciliation of data
  - Documentation
  - Error correction procedures
    - Logging of errors
    - Timely corrections
    - Upstream resubmissions
    - Approval of corrections
    - Suspense file
    - Error file
    - Validity of correction
  - Transmittal log
  - Cancellation of source documents

Output Controls

Output controls are meant to provide assurance that the data delivered to users will be presented, formatted and delivered in a consistent and secure manner.

- Logging and storage of negotiable, sensitive and critical forms in a secure place
- Computer generation of negotiable instruments, forms and signatures
- Report distribution
- Balancing and reconciling
- Output error handling
- Output report retention
- Verification of receipt of reports – to provide assurance that sensitive reports are properly distributed, the recipient should sign a log (manual or electronic) as evidence of receipt of output

Processing Controls

Processing controls are meant to ensure the reliability of application program processing. Auditors need to understand the procedures and controls that can be exercised over processing to evaluate what exposures are covered by these controls and what exposures remain.

- Data Validation and Editing (see next page for descriptions)
- Processing Controls
  - Manual recalculations
  - Editing
  - Run-to-run totals
  - Programmed controls
  - Reasonable verification of calculated amounts
  - Limits checks on amounts
  - Reconciliation of file totals
  - Exception reports
- Data file controls
  - System control parameters
  - Standing data
  - Master data/balance data
  - Transaction files

Processing Controls

Data Validation and Edit Controls

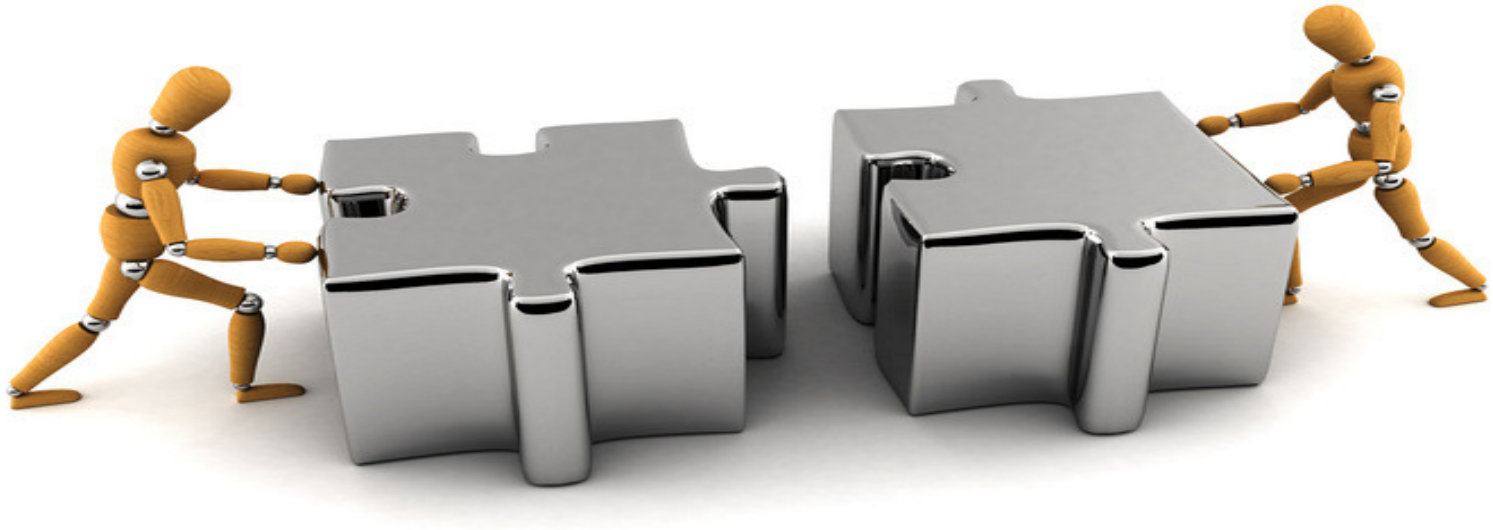
Edits	Description Examples
Sequence checks	Invoice numbered sequentially
Limit checks	Data should not exceed a predetermined amount (not > $4,000)
Range checks	Product type codes range from 100 – 250
Validity checks	Payroll record with marital status can only be M or S
Reasonableness checks	Input are matched to predetermined limits (order not > 20 items)
Table lookups	Input clerk enters a city code of 1 -10 corresponding city name
Existence check	Valid transaction code must be entered in the transaction field
Key verification	Keying process is repeated by a separate individual – re-verification
Check digit	Calculated numerical value of field to prevent transposition errors
Completeness check	Value is not left blank and complies with expected data format
Duplicate check	Invoice numbers not entered twice to prevent vendor paid twice
Logical relationship check	Employee hire date must be more than 16 years past his date of birth

Compliance vs Substantive Testing

Compliance testing is evidence gathering for the purpose of testing an organization's compliance with control procedures. Compliance tests determine if controls are being applied in a manner that complies with management policies and procedures.

Substantive testing is where evidence is gathered to evaluate the integrity of individuals transactions, data or other information. Substantive tests substantiates the integrity of actual processing. It provides evidence of the validity and integrity of the balances in the financial statements, and the transactions that support their balances.

CHANGING CHALLENGES INTO OPPORTUNITIES



ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Back to Business

We Have an Important Role

- 70% of CEOs are ***increasing*** spending on IT to reduce overall business costs

- 90% of CAEs will ***increase*** their plan hours devoted to new systems, processes and controls in the next two years

Changing Challenges into Opportunities

Audit Planning

Audit Execution

Training & Development
Audit Assignments/Opportunities
Audit Rotations

Audit Planning . . . A Team Effort

IT Auditors

- Operating platform
- Database structure
- IT infrastructure

Financial Auditors

- Business processes
- Segregation of Duties
- Understand materiality and account significance

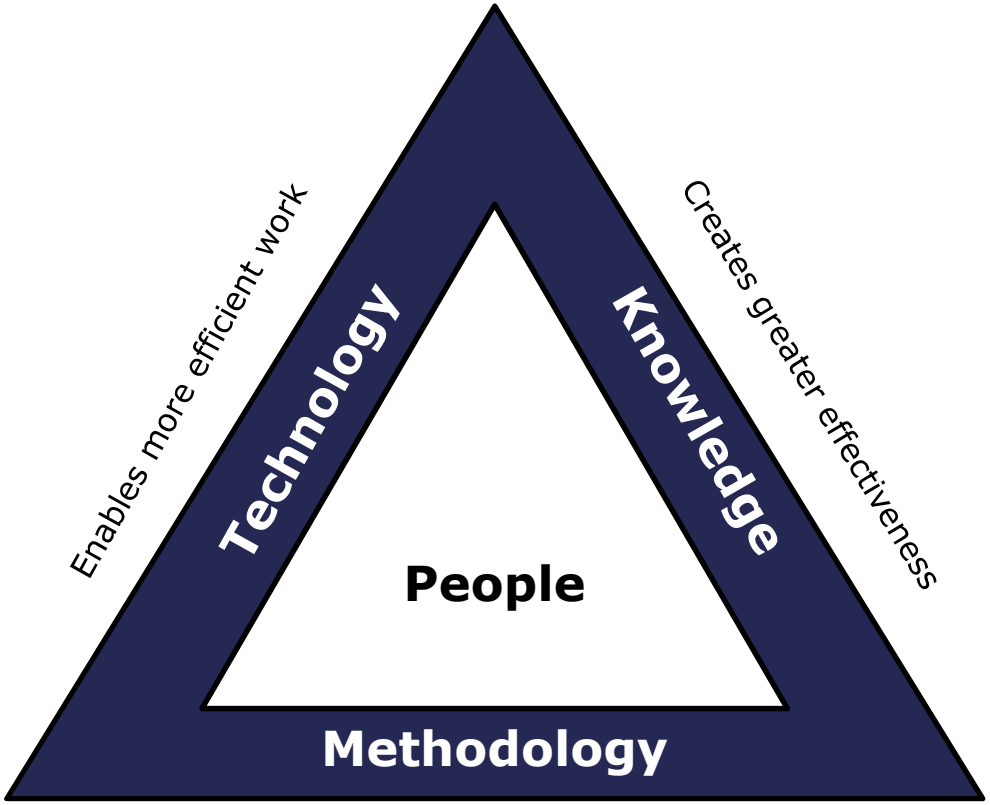
Audit Planning . . . A Team Effort

Audit and Advisory Professionals

- Start with a business process approach
- Develop a better understanding of the key business cycles
  - Operations - Processes
  - Systems - Controls

    - Do not separate process/cycles into IT and operational components

Audit Execution



Provides the foundation for how the department operates

Training and Development

Financial/Operational Auditors

- Business processes
- Control documentation

- ERP systems
- ERP infrastructure
- Privacy, Security, BCP
- IT general controls
- Application controls
- Data analytics

Information Technology Auditors

- Business processes
- Control documentation

- Financial, compliance, operational and strategic risks
- Financial and operational cycles
- Internal audit report writing

Training Plan Foundation

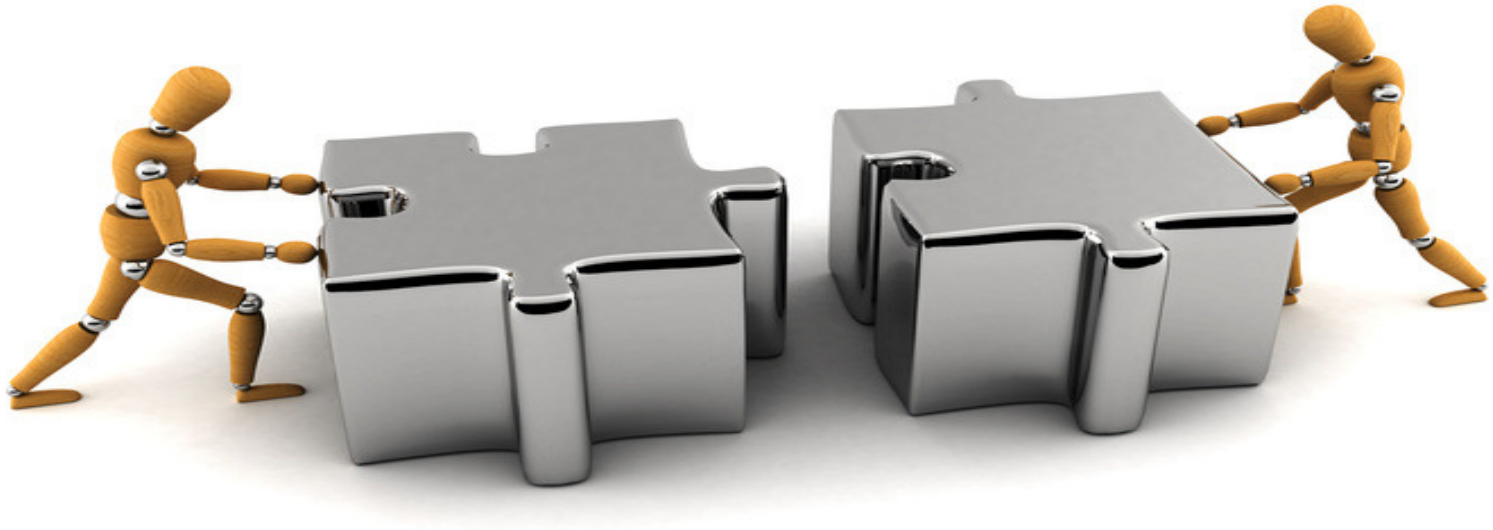
Staff Rotation

All Auditors

- 6 to 9 months in financial audit
- 6 to 9 months in IT audit
- 6 to 9 months in operational audit

- Assess and re-evaluate staff accomplishments and competencies
- Case study discussion from EY

CONCLUSIONS . . .



Absolute Security Does Not Exist

But We Still Put in Controls

- Alarms
- Locks
- Sensors
- Video Cameras
- Guard Dogs
- Alert Authorities
- Insurance
- Security Awareness
- Training
- Contingency Procedures
- Stay informed / trained

AUDITORS DO NOT HAVE TO BE ACCURATE

An auditor is having a hard time sleeping and goes to see his doctor. "Doctor, I just can’t get to sleep at night.”

"Have you tried counting sheep?“

"That’s the problem - I make a mistake and then spend three hours trying to find it."

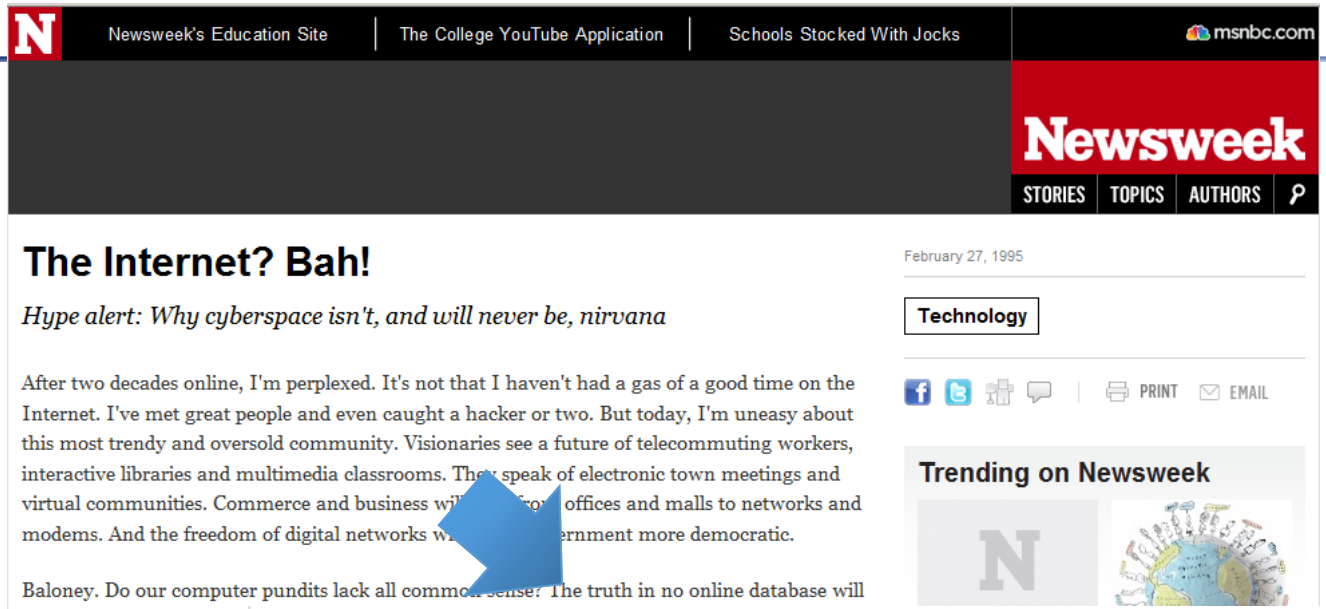
THEY JUST HAVE TO BE RIGHT!

Don’t Be Quixotic

Experts Can Be Wrong

1981: No one will ever need more than 640K

1995 Prediction



Newsweek's Education Site | The College YouTube Application | Schools Stocked With Jocks

msnbc.com

Newsweek

STORIES TOPICS AUTHORS

The Internet? Bah!

Hype alert: Why cyberspace isn't, and will never be, nirvana

February 27, 1995

Technology

PRINT EMAIL

Trending on Newsweek

After two decades online, I'm perplexed. It's not that I haven't had a gas of a good time on the Internet. I've met great people and even caught a hacker or two. But today, I'm uneasy about this most trendy and oversold community. Visionaries see a future of telecommuting workers, interactive libraries and multimedia classrooms. They speak of electronic town meetings and virtual communities. Commerce and business will shift from offices and malls to networks and modems. And the freedom of digital networks will make government more democratic.

Baloney. Do our computer pundits lack all common sense? The truth in no online database will replace your daily newspaper, no CD-ROM can take the place of a competent teacher and no computer network will change the way government works.

ISACA

Trust in, and value from, information sys

San Francisco Chapter

Staff Rotation

- Internal audit is pulled in many directions
  - Expectations increase every year
- We must do more with less
  - Or more with the same
- Better integration between IT and Financial IA team members
  - Increase value add and effectiveness
- Planning, training and staff rotation are keys to success

BIOGRAPHY

Miguel (Mike) O. Villegas is the Director of Information Security at Newegg, Inc. and is responsible for Information Security and PCI DSS (Payment Card Industry Data Security Standard) compliance. Newegg, Inc. is a PCI Level 1 Merchant and Service Provider. It is one of the fastest growing E-Commerce companies established in 2001 and exceeded revenues of over $2.8 Billion in 2010.

Mike has over 30 years of Information Systems security and IT audit experience. Mike was previously Vice President & Technology Risk Manager for Wells Fargo Services responsible for IT Regulatory Compliance and was previously a partner at Arthur Andersen and Ernst & Young for their information systems security and IS audit groups over a span of nine years. Mike is a CISA, CISSP, GSEC, CEH, PA-QSA and PCI-QSA (K3DES).

Mike is the current LA ISACA Chapter President and was the SF ISACA Chapter President during 2005-2006. He was the SF Fall Conference Co-Chair from 2002–2007 and also served for two years as Vice President on the Board of Directors for ISACA International.

mike.o.villegas@newegg.com (626) 271-1420 x22511

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Contact Information:

Scot Glover, Partner
Governance, Risk & Compliance
Armanino McKenna, LLP
925.790.2622
scot.glover@amllp.com

ARMANINO McKENNA LLP
Certified Public Accountants & Consultants