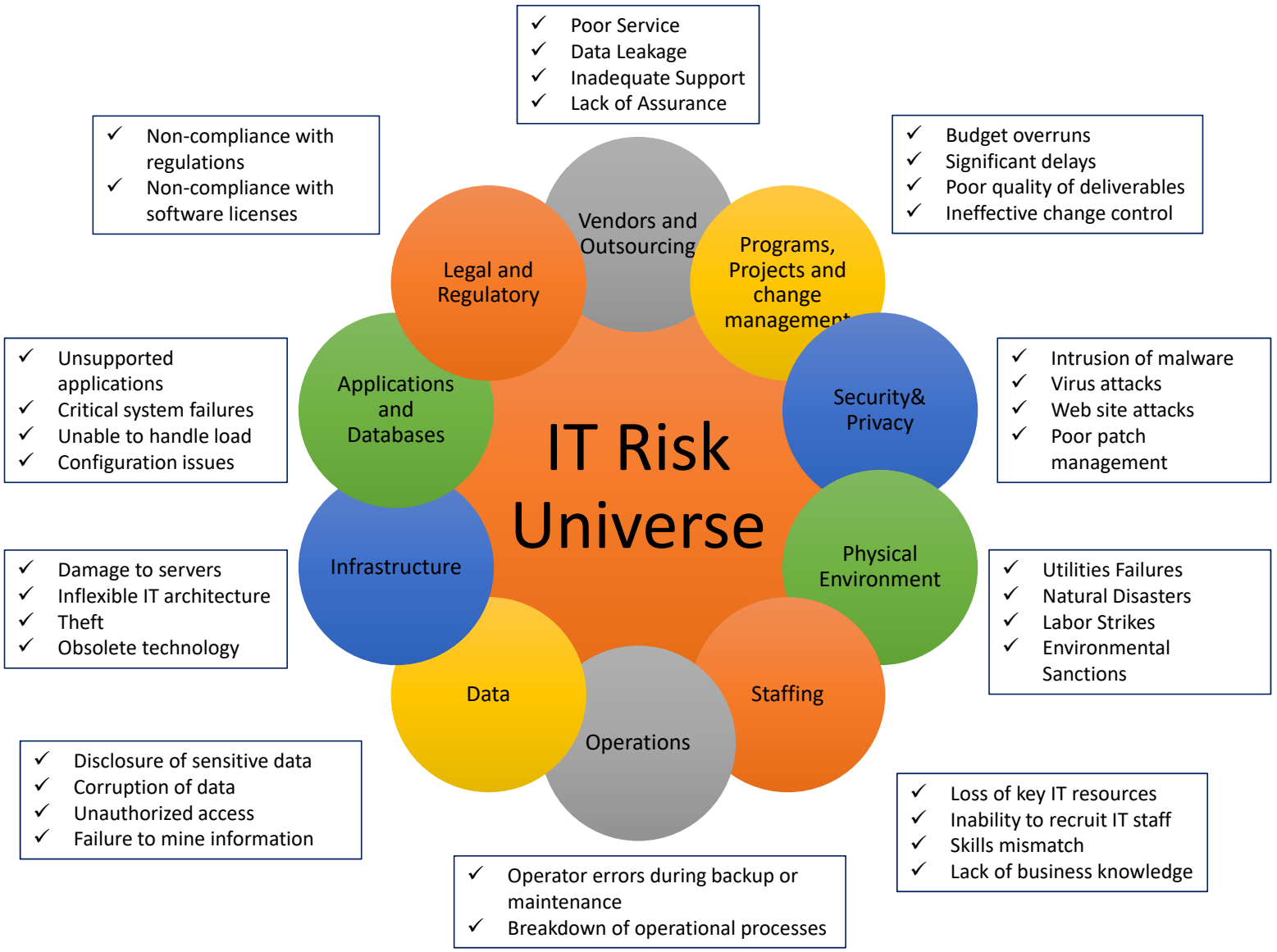
FOX | ITACS
Master of IT Auditing & Cyber Security

IT Audit Process

Mike Romeu-Lugo MBA, CISA

February 20, 2017


IT Risk Universe
Vendors and Outsourcing
Programs, Projects and change management
Security& Privacy
Physical Environment
Staffing
Operations
Data
Infrastructure
Applications and Databases
Legal and Regulatory
✓ Poor Service
✓ Data Leakage
✓ Inadequate Support
✓ Lack of Assurance
✓ Budget overruns
✓ Significant delays
✓ Poor quality of deliverables
✓ Ineffective change control
✓ Intrusion of malware
✓ Virus attacks
✓ Web site attacks
✓ Poor patch management
✓ Utilities Failures
✓ Natural Disasters
✓ Labor Strikes
✓ Environmental Sanctions
✓ Loss of key IT resources
✓ Inability to recruit IT staff
✓ Skills mismatch
✓ Lack of business knowledge
✓ Operator errors during backup or maintenance
✓ Breakdown of operational processes
✓ Disclosure of sensitive data
✓ Corruption of data
✓ Unauthorized access
✓ Failure to mine information
✓ Damage to servers
✓ Inflexible IT architecture
✓ Theft
✓ Obsolete technology
✓ Unsupported applications
✓ Critical system failures
✓ Unable to handle load
✓ Configuration issues
✓ Non-compliance with regulations
✓ Non-compliance with software licenses

Risk Management

- What is Risk?

"The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization."

- Threat: Anything (e.g. object, substance, human) that is capable of acting against an asset in a manner that can result in harm.")

- What is Business Risk?

"the likelihood of those threats that may negatively impact the assets, processes or objectives of an organization."

  - Financial Risk – e.g. not meeting earning expectations
  - Operational Risks – e.g. increase in backorders
  - Regulatory Risks – e.g. longer product registrations

Risk Management

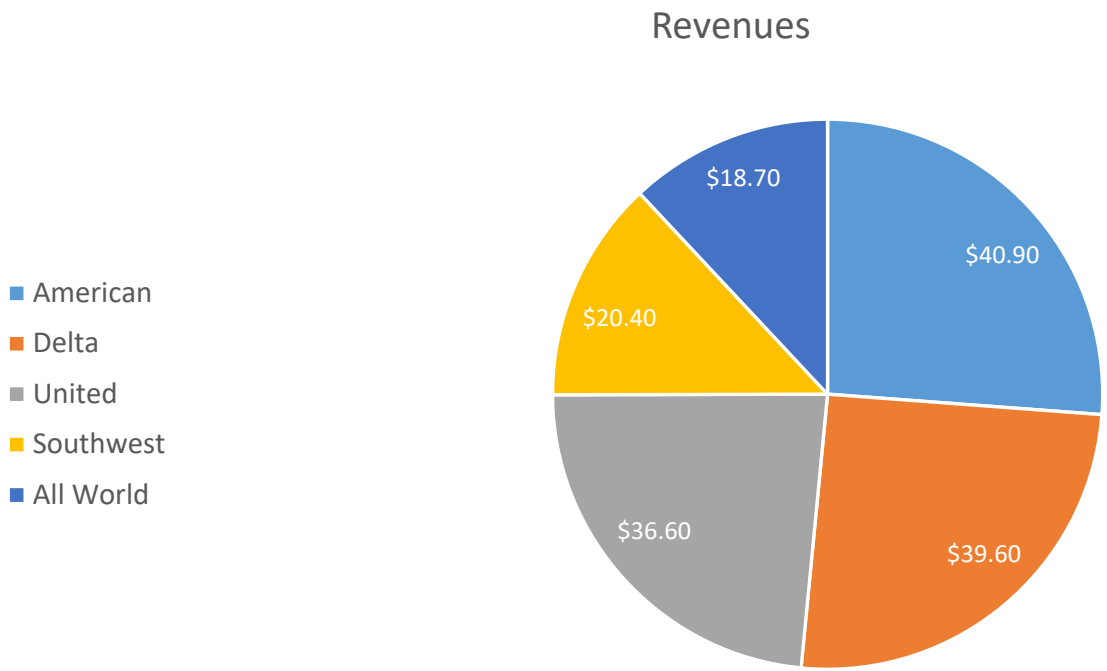
- What is **IT Risk**?

  "the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise."

- Defined in terms of
  - Uncertain Frequency (Probability of occurrence)
  - Magnitude (Impact)

- Risks cannot be eliminated. Appropriate responses to risk:
  - Accept
  - Reduce
  - Transfer
  - **Never ignored!**

US Airline Industry – Net Income 2015



AWA – Risk: System Availability

- Expected Availability: 100%
  - Annual Revenue: $ 18,700,000,000.0 (2015)
  - Hour per Day: 8,760.0 hours
  - Revenue per hour: $ 2,135,000.0

  For every hour the Reservation System is not available AWA looses $2,135,000.0 Million

AWA – Risk: Recruitment and Retention

- COBOL Programmer Salary: $85,000
- Recruitment Costs
  - Job Board Memberships – $2,200/Annually
    - LinkedIn
    - Monster
  - Sign-in Bonus: $12,750 (15% salary)
- Benefit Costs: $25,500 (30% of Salary)
- Severance Payments: $7,000

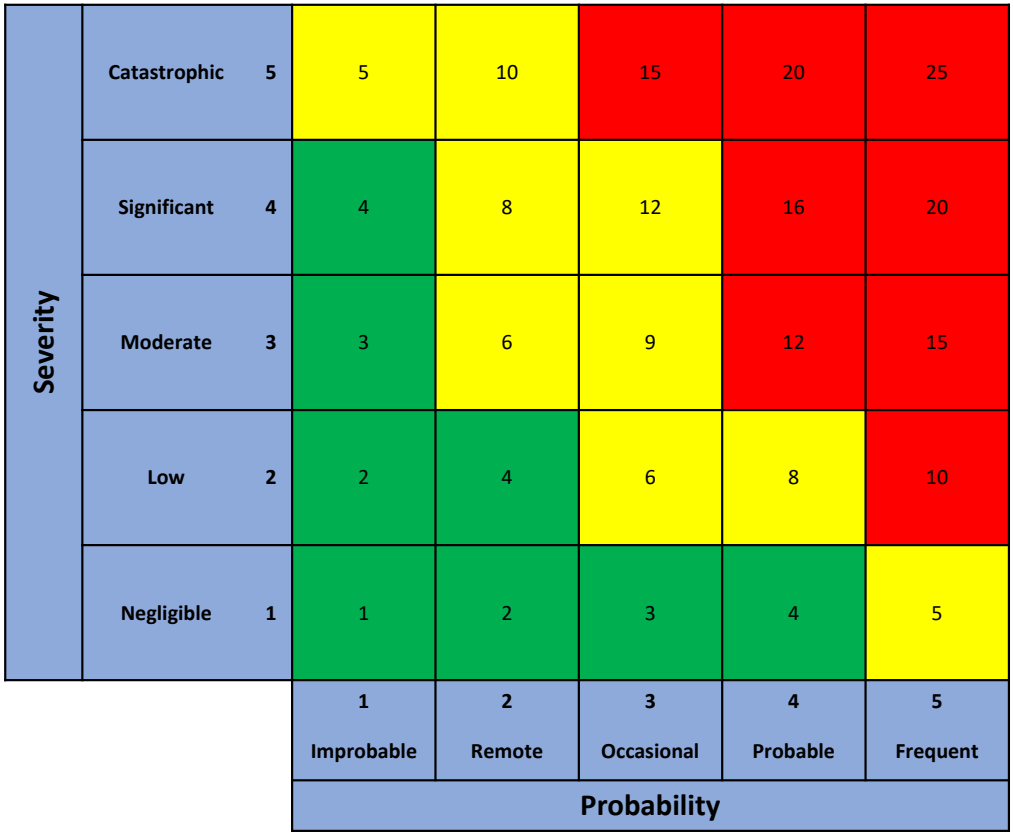
Total Cost for replacing 1 COBOL Programmer: $132,400

AWA – Risk: Loss of Tax Incentives / Service Costs

- Current Tax Rate: 7% of Total Revenues $ 1,309 Million (Economically Depressed Area)
- Actual Tax Rate: 13% of Total Revenues $ 2,431 Million
- Tax Rate Increase (Decrease) $ 1,122 Million

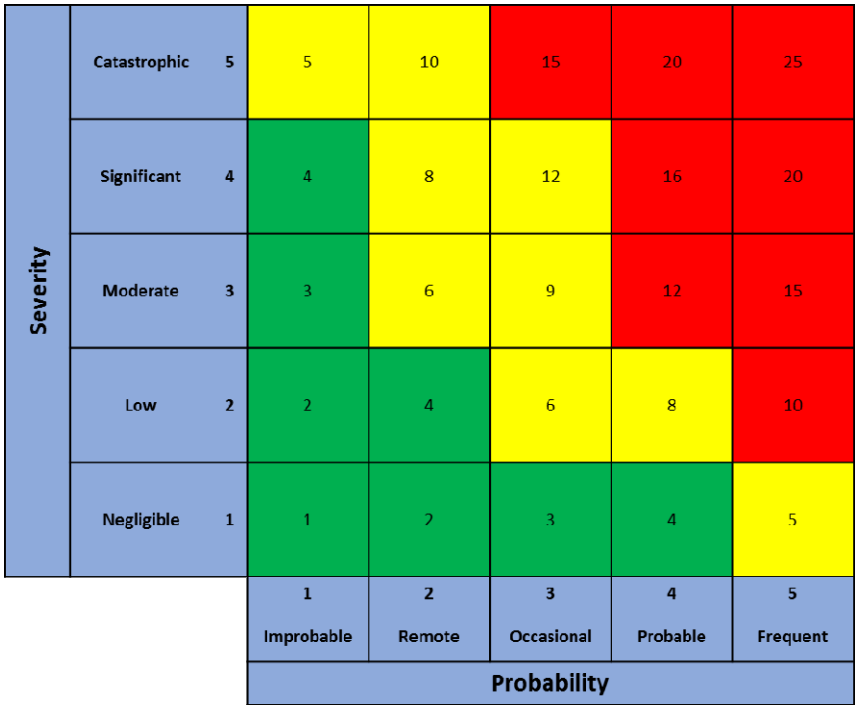
- Unexpected Service Costs: $75,000

AWA - Risks


Severity
Catastrophic 5
Significant 4
Moderate 3
Low 2
Negligible 1
5 10 15 20 25
4 8 12 16 20
3 6 9 12 15
2 4 6 8 10
1 2 3 4 5
1 Improbable
2 Remote
3 Occasional
4 Probable
5 Frequent
Probability

AWA – Risk Assessment

- Service Availability not met – 12 (Severity: 4; Probability: 3)
- Retention and Recruitment – 16 (Severity: 4; Probability: 4)
- Loss of Tax Incentives – 4 (Severity: 1; Probability: 4)
- Unforeseen Costs – 12 (Severity: 3; Probability 4)



Other Risks

- **Inherent Risk** – The risk level or exposure without taking into account the actions that management has taken or might take.
- **Residual Risk** – The remaining risk level after management has implemented a risk response (accept, reduce, transfer)
- **Control Risk** – The risk that a material error exists that would not be prevented or detected on a timely basis.
- **Detection Risk** – The risk that the IS Ausitor's substantive procedures will not detect an error that could be material, individually or in combination with other errors
- **Sampling Risk** – Risk that the sample selected is not representative of the population
  - Alpha
  - Beta

Risk Assessment

- Qualitative vs. Quantitative
  - No method is fully objective
  - IT Risks are very difficult to quantify due to subjectivity and poor quality of IT Risk-related data.
  - Over-confidence of qualitative approaches.
- Qualitative Approach – Relies on expert opinion to estimate frequency and impact.
  - Catastrophic, Significant, Moderate, Low, Negligible…
  - When to use: in situations when limited or low quality information is available
  - Strength: less complex and less expensive
  - Weakness: high level of subjectivity, great variance in human judgement, no standard approach
- Quantitative Approach – based on statistical methods.
  - More objective due to empirical data
  - Requires sufficient complete and reliable data on past or comparable events… hard to get
  - Some things just cannot be quantified… human life, terrorist attacks, loss of reputation

Internal Controls

Definition: “The means of managing risks.”

- Policies
- Procedures
- Guidelines
- Practices
- Organizational Structures

- Administrative
- Technical
- Managerial
- Legal

Control Types

- **Preventive**
  - Detect problems before they arise
  - Monitor both operation and inputs
  - Attempt to predict potential problems before they occur and make adjustments
  - Prevent an error, omission or malicious act from occurring.
- **Detective**
  - Use controls that detect and report the occurrence of an error, omission or malicious act.
  - Example: missing required field in a form.
- **Corrective**
  - Minimize the impact of a threat.
  - Remedy problems discovered by detective controls
  - Identify the cause of a problem
  - Correct errors arising from a problem
  - Modify the processing system(s) to minimize future occurrences of the problem