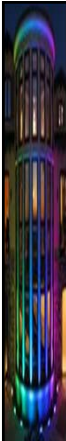


Risk Assessment in the Covid-19 Environment

Presented by
Steven L. Blake CPA, CFE, CICA, CGMA
SLBCPA@CHARTER.NET 864-680-6191


1



Agenda

- THERE WILL BE 4 2-HOUR SESSIONS
- First 2 Hour Session: Learning about the current risk environment.
- Second 2 Hour Session: Understanding the current risk environment
- Third 2 Hour Session: Specific risk assessment techniques and how to adapt them to the current risk environment.
- Fourth 2 Hour Session: Continuance of Third Session.
- Live Questions/Comments Period – Must Attend

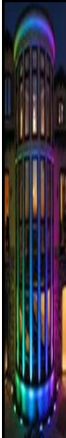
2



Learning Objectives

- Understand what risk is in this environment
- Increase awareness, assessment and responses to risk.
- Provide tools to both early detect and potentially deter fraud.
- Discuss security risk management techniques to monitor on an on-going basis.

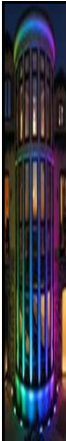
3



Learning Objectives


- Online learning requires Attendance Verification. We use Codes to verify.
- Nestled within this presentation is a 4 Place Alphanumeric Code you will use to “confirm” your attendance. It will appear twice in each two hour section, on two different slides at two different times during this presentation.

4




LEARNING ABOUT THE CURRENT RISK ENVIRONMENT SECTION 1

5



Parable of the Ten Virgins – Matthew 25


6



Inherent and Residual Risk

- Inherent risk exists in the system before any type of system/management intervention
- Residual risk exists in the system after system or management actions are taken.


7



Fraud Risk

- The risk/vulnerability an entity has to the possibility that someone can overcome the components of internal controls.
- This risk differs from any other risk because by nature it is intentional misconduct designed to evade detection.

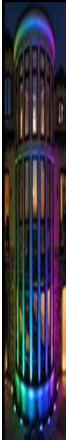
8



Fraud Risk

- INTERNAL: The risk/vulnerability that someone IN THE ORGANIZATION is capable of overcoming the components of internal control.
- EXTERNAL: Someone external to the organization is capable of overcoming the components of internal control.

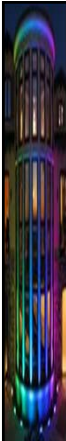
9



Risk in a Covid-19 Environment

- What is new and different as a result of THIS environment?
 - Social Distancing has created work from home:
 - Less aptitude for questioning/investigating
 - Less direct oversight and verification of process inputs
 - Can't help but slow the process due to distance in the current system(s) begging the need to "speed up"/cut corners.


10



Risk in a Covid-19 Environment

- What is new and different as a result of THIS environment?
 - The risk of the disease itself:
 - Uncertain legal liability environment
 - Highly contagious – risk of infection, sickness and/or death.
 - Business interruption(s) due to the first two points
 - Uncharted territory

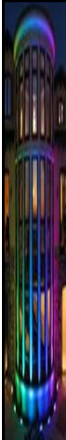
11



Risk Assessment Measurements

- Impact
- Likelihood
- To measure the impact and likelihood you must have INFORMATION. Herein lies the ultimate problem with uncharted territory; information is sparse and many times contradictory.

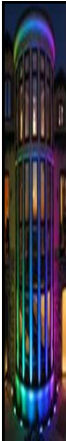
12



Video - Pay Attention to:

- Make notes and we'll discuss what we learned In the live Q&A session:
 - What issues did the Haskell County KS health authorities and the US Military consider in their risk assessments?
 - What physical limitations contributed?
 - What happened in Australia?


13



Pay Attention to:


- We'll discuss what we learned:
 - Notice the picture of the overwhelmed hospital at Ft. Devins MA, you will see this again.
 - What specific fraud issue occurred at Ft. Grant in IL? What other fraud issues occurred in Philadelphia?
 - What difference in risk assessment did San Francisco vs. Philadelphia make?

14



INFLUENZA
 FREQUENTLY COMPLICATED WITH
PNEUMONIA
 IS PREVALENT AT THIS TIME THROUGHOUT AMERICA.
 THIS THEATRE IS CO-OPERATING WITH THE DEPARTMENT OF HEALTH.
YOU MUST DO THE SAME
 IF YOU HAVE A COLD AND ARE COUGHING AND
 SNEEZING DO NOT ENTER THIS THEATRE.
GO HOME AND GO TO BED UNTIL YOU ARE WELL.
Coughing, Sneezing or Spitting Will Not Be Permitted in The Theatre. In case you must cough or sneeze, do so in your own handkerchief, and if the coughing or sneezing persists, leave the theatre at once.
 This Theatre has agreed to cooperate with the Department of Health in disseminating the truth about influenza, and thus serve a great educational purpose.
HELP US TO KEEP CHICAGO THE HEALTHIEST CITY IN THE WORLD
JOHN DILL ROBERTSON
 COMMISSIONER OF HEALTH

15



First Video

- YouTube link for “Deadliest Plague of the 20th Century – Spanish Flu of 1918”.
- Length: 39:36
- There are some pictures some would consider shocking.
- Imbed video ... October 2, 2018


16



First Video



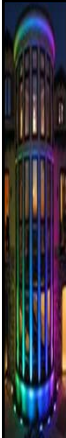
17



Pay Attention to:

- In the live Q&A session, make notes and we'll discuss what we learned:
 - What issues did the Haskell County KS health authorities and the US Military consider in their risk assessments?
 - What physical limitations contributed?
 - What happened in Australia?

18



Pay Attention to:

- In the live Q&A session, make notes and we'll discuss what we learned:
 - Notice the picture of the overwhelmed hospital at Ft. Devins MA, you will see this again.
 - What specific fraud issue occurred at Ft. Grant in IL? What other fraud issues occurred in Philadelphia?
 - What difference in risk assessment did San Francisco vs. Philadelphia make?


19



Lessons Learned – Post Pandemic

- Shortages – Food and Manufactured Goods
- Massive Social Displacement
- Economic Consequences

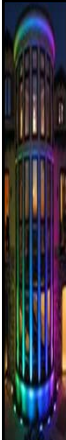
20



Second Video Pay Attention to:

- Responses of Wuhan government officials early and late
- Responses of Wuhan medical system
- Responses of Wuhan citizens especially to the late responses of the government

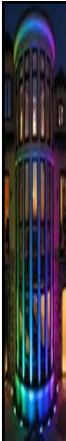
21



Second Video Pay Attention to:

- ZDUQQJ\$
- Graphic Language, Disturbing Images


22




Second Video

- YouTube link for "Coronavirus: How the deadly epidemic sparked a global emergency | Four Corners".
- Length: 45:52
- There is some rough language and potentially disturbing pictures.
- Imbed video ...


23



Second Video




24



What to do with Risk or “Risk Responses”

- Risk Avoidance,
- Risk Reduction,
- Risk Sharing,
- and Risk Acceptance


25



Risk Awareness

- Across departments
- By Type
- Embedded into existing management systems


26



Risk Appetite

- Can be Subjective, Individual and/or Corporate
- Based on Cost Benefit
- Capability Maturity Model

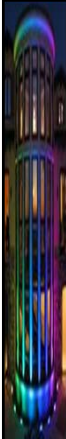
27



Risk Assessment in the Covid-19 Environment

Presented by
Steven L. Blake CPA, CFE, CICA, CGMA
 SLBCPA@CHARTER.NET 864-680-6191

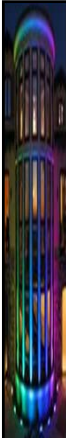
28



Agenda

- THERE WILL BE 4 2-HOUR SESSIONS
- First 2 Hour Session: Learning about the current risk environment.
- Second 2 Hour Session: Understanding the current risk environment
- Third 2 Hour Session: Specific risk assessment techniques and how to adapt them to the current risk environment.
- Fourth 2 Hour Session: Continuance of Third Session.
- Live Questions/Comments Period – Must Attend

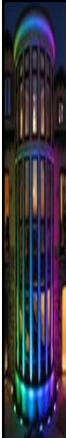
29



Learning Objectives

- Understand what risk is in this environment
- Increase awareness, assessment and responses to risk.
- Provide tools to both early detect and potentially deter fraud.
- Discuss security risk management techniques to monitor on an on-going basis.

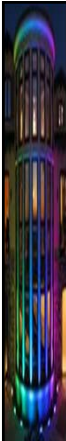
30



Learning Objectives


- Online learning requires Attendance Verification. We use Codes to verify.
- Nestled within this presentation is a 4 Place Alphanumeric Code you will use to “confirm” your attendance. It will appear twice in each two hour section, on two different slides at two different times during this presentation.

31



UNDERSTANDING THE CURRENT RISK ENVIRONMENT


32



Review

- Being prepared ...
- Types of risk:
 - Inherent
 - Residual
 - Fraud
- Risk Response
- Risk Awareness
- Risk Appetite


33



What to do with Risk or “Risk Responses”

- Risk Avoidance,
- Risk Reduction,
- Risk Sharing,
- and Risk Acceptance


34



Risk Awareness

- Across departments
- By Type
- Embedded into existing management systems

35



Risk Appetite

- Can be Subjective, Individual and/or Corporate
- Based on Cost Benefit
- Capability Maturity Model

36

Capability Maturity Model ^α

Capability Maturity Model – Integrated

Level	Focus	Process Areas	Result
5 Optimizing	Continuous process improvement	Organizational Innovation & Deployment Causal Analysis and Resolution	Productivity & Quality
4 Quantitatively Managed	Quantitative management	Organizational Process Performance Quantitative Project Management	
3 Defined	Process standardization	Requirements Development Technical Solution Product Integration Verification Validation Organizational Process Focus Organizational Process Definition Organizational Training Integrated Project Management Risk Management Decision Analysis and Resolution	
2 Managed	Basic project management	Requirements Management Project Planning Project Monitoring & Control Supplier Agreement Management Measurement and Analysis Process & Product Quality Assurance Configuration Management	
1 Initial	Competent people and heroics		

37

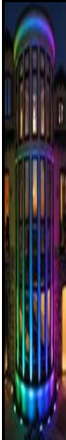
- ### Ultimate Risk Assessment
- Covid – 19; Life threatening
 - Unprecedented Public Responses:
 - Social Distancing
 - Economic Shutdowns
 - Business/Occupational Responses:
 - Work-from-home
 - “Zoom” meetings
 - Legal liabilities

38

ATTENDANCE CODE

•Z231

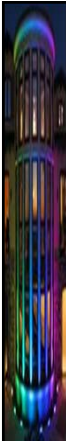
39



Ultimate Risk Assessment

- Risk Appetite
 - Getting correct information.
 - Individual’s risk responses to Covid-19
 - Age/Vulnerabilities
 - Need for a paycheck
 - Covid-19 Parties/Herd Immunity
 - “New” virus – sparse information
 - Scientific Method – time consuming


40



Ultimate Risk Assessment

- Risk Appetite
 - Business’ Responses to Covid-19:
 - Unknown Legal Environment
 - Managing employee responses
 - Managing vendor responses
 - Managing customer responses
 - Managing government responses
 - New business model to avoid bankruptcy

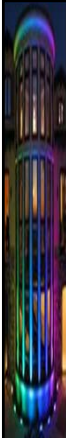
41



Ultimate Risk Assessment

- Risk Appetite
 - Governments’ Responses to Covid-19:
 - Unknown Legal Environment – Committees on new laws and limits on legal liability
 - Managing employee responses
 - Managing vendor responses
 - Managing citizen responses
 - Managing business responses – trying to maintain a tax base
 - New financing model to avoid bankruptcy

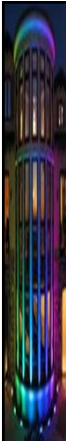
42



Ultimate Risk Assessment

- Economic Information
 - From best unemployment rates in history to worst unemployment rates in history
 - Second quarter US economic contraction – 32.9%
 - Loss of entire segments of economy:
 - Entertainment – theme parks, movies, restaurants, sports
 - Close contact businesses – grooming, non essential medical
 - Social Sacrifices – Civic and Religious gatherings


43



Human Nature ^α

- By definition:
 - the general psychological characteristics, feelings, and behavioral traits of humankind, regarded as shared by all humans. [Essentialist]
- However, this definition is biased toward the “Essentialist” school of philosophy

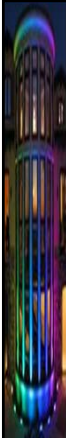
44



Philosophy

- By definition:
 - the study of the fundamental nature of knowledge, reality, and existence, especially when considered as an academic discipline.
- Synonyms: thinking, reasoning, wisdom, thought, knowledge

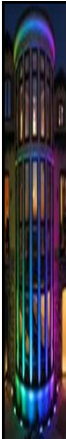
45



What is reality?^a

- Ravi Zacharias' "*Absolute Truth in Relative Terms*"
- The movie "The Matrix"
- The world of the "fraudster"


46



Self-denial vs. Self-gratification^a

- Principle of delayed gratification
- Fears for personal safety
- Need for a paycheck, selfish, uncaring thought process.
- Hopelessness

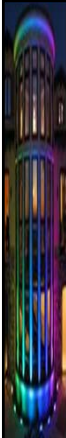
47



Main Schools of Ethics^a

- Consequentialism (including utilitarianism) the view that the right thing to do is what has the best outcomes from actions;
- Virtue Ethics (the view that some things have virtues that make actions right); and
- Duty Ethics (some actions are just duties)

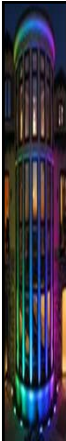
48



So What is Truth?^a

- William Backus *Telling Yourself the Truth*
- *Holy Bible*: John 17:17
- Ravi Zacharias “*Absolute Truth in Relative Terms*”
- Quran: "God is the Truth (the Real)"
- Google: ...


49



Distorted Thought Processes^a

- The following “Cognitive Distortions” are from the Neal Nedley *Depression and Anxiety Recovery Program*:
 - All or Nothing Thinking
 - Mental Filter
 - Mind Reading
 - Fortune Teller Error
 - Emotional Reasoning

50



Why is this even important?^a

- From the first video we learned that during the first pandemic [Spanish Flu – 1918] the social fabric disintegrated.
- Social moral values and Creationist origins have been removed from most public education in recent generations. So where do people learn their “ethics”? What are people putting their hope in?

51

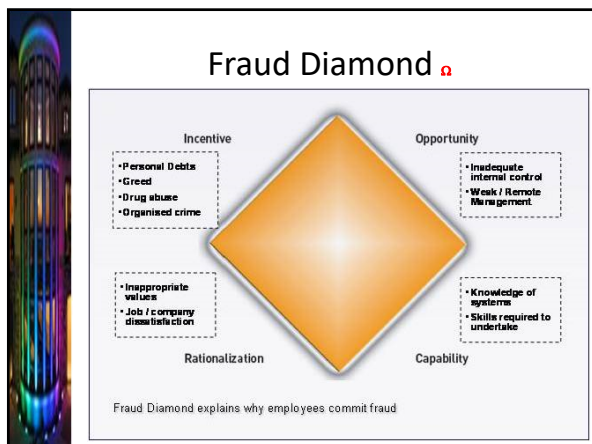
Pew Charitable Trust Studies ^α

- 2014 Studies on the influence of religion on and in people's lives


52



53




54



ATTENDANCE CODE

•Z231

55



Incentives to Commit Fraud

- Individual Financial Pressures
 - Unexpected Financial Need e.g. Sudden Medical Bills
 - Keeping Up with the Jones'
 - Poor Credit
- Individual Vices – Gambling, Drugs etc.
- Work Related Pressures
 - Get Even for lack of recognition/promotion/pay.


56



Incentives to Commit Fraud

- Corporate Financial Pressures
 - Poor Financial Position
 - Uncollectible Receivables
 - Eroding Market Share
- Corporate Vices – Uncompetitive
 - Poor S.W.O.T. or E.R.M.
- Work Related Pressures
 - Obsolescence


57



Opportunity Ω

- Poor Internal Controls or Management Override
- Poor Information Systems – either nonintegrated or lack of audit trail
- Poor Corporate Culture
 - Lack of training/knowledge of job performance
 - Management ignorance or apathy
 - Failure to communicate integrity


58



Rationalization Ω

- People are moral, rational human beings, or not!
- Books by Joseph T. Wells
 - *Fraud Fighter, my Fables and Foibles*
 - *Franksteins of Fraud: the 20th Century's Top 10 White-collar Criminals*
- The amazing ability to lie to oneself.
- Integrity

59



Capability

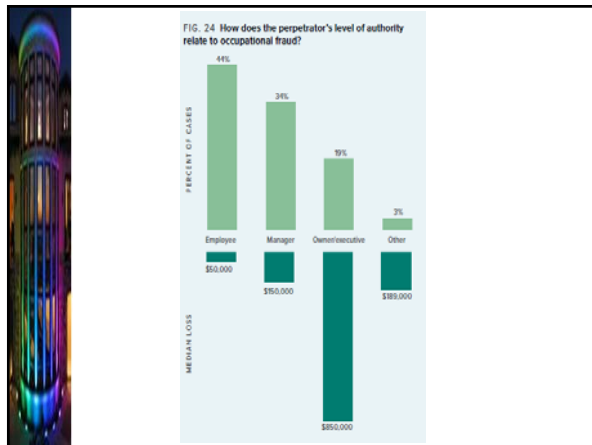
- Has a knowledge of the systems, processes or the lack thereof
- Cooperates in the 'need' to override or perpetrates the override
- Has the position or skill set to accomplish the task. In the world of corporate espionage, this could be the janitor!

60

The Typical Embezzler ^α

- Trusted, generally long-term employee
- Generally in a management-like role
- Dedicated, works long hours
- Rarely takes vacation, dislikes the policy of mandatory vacations. Makes excuses why they cannot go on vacation.
- Resents and will not cooperate with cross-training.
- Seen as likable and generous

61

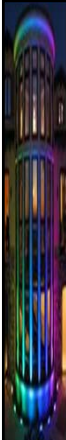


62

Biblical Pressures Discussion

Romans 5: ³ ... we also glory in tribulations [pressures], knowing that tribulation produces ⁴ perseverance; and perseverance, ⁵ character; and character, hope. ⁶ Now hope does not disappoint, [NKJV]

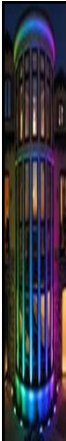
63



Does Character Get Noticed?


- Daniel 6:3³ Daniel proved himself to be a better supervisor than any of the others. He did this by his good character and great ability. The king was so impressed with Daniel that he planned to make him ruler over the whole kingdom. [ERV]

64



How do you recognize when an organization or individual is getting into trouble?


65



Warning Signs

- Organizational/Individual culture of arrogance and/or entitlement; failure to listen
- Accounting policies that rely too heavily on management's judgment
- Departure of key senior management
- Overly centralized control of financial reporting, especially in large organizations with a qualified finance staff


66



Warning Signs ⚠

- Failure to pay bills on time or as timely as in prior years
- Accounting policies seem overly aggressive, especially when given the qualifications of the accounting staff
- Periods of prolonged success even during periods when the industry is down
- Transactions lacking economic purpose


67



One Last Item of Note ⚠


- Which warning signs have increased during the Covid responses?
 - Are things being done timely?
 - Does management have to “override” normal controls due to the unusual circumstances?
 - Do citizens/vendors all have “sob” stories related to their current circumstances?
- If it is too good to be true ...
- You don’t get something for nothing ...

68



SPECIFIC RISK RESPONSE TECHNIQUES AND HOW TO ADAPT THEM TO THE CURRENT RISK ENVIRONMENT

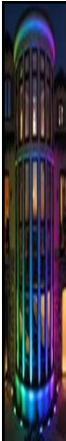
69



Risk Assessment in the Covid-19 Environment

Presented by
Steven L. Blake CPA, CFE, CICA, CGMA
 SLBCPA@CHARTER.NET 864-680-6191


70



Agenda

- THERE WILL BE 4 2-HOUR SESSIONS
- First 2 Hour Session: Learning about the current risk environment.
- Second 2 Hour Session: Understanding the current risk environment
- Third 2 Hour Session: Specific risk assessment techniques and how to adapt them to the current risk environment.
- Fourth 2 Hour Session: Continuance of Third Session.
- Live Questions/Comments Period – Must Attend


71



Learning Objectives

- Understand what risk is in this environment
- Increase awareness, assessment and responses to risk.
- Provide tools to both early detect and potentially deter fraud.
- Discuss security risk management techniques to monitor on an on-going basis.


72



Learning Objectives α

- Online learning requires Attendance Verification. We use Codes to verify.
- Nestled within this presentation is a 4 Place Alphanumeric Code you will use to “confirm” your attendance. It will appear twice in each two hour section, on two different slides at two different times during this presentation.


73



Scheme Categories

- Asset Misappropriation
- Bribery and Corruption
- Fraudulent Statements

74



Scheme Subcategories α

- Employee Fraud
- Management Fraud
- Investment Schemes
- Vendor Fraud
- Customer Fraud
- Other - Miscellaneous

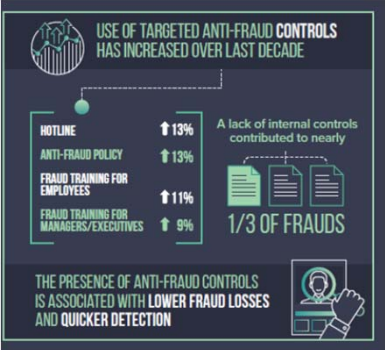
75

Asset Misappropriation

- Cash
- Inventory
- Office Supplies
- Expense Reports
- Company Vehicles, Cell Phones
- Accounts Receivables, Revenues
- Falsifying Hours on a Timesheet

76

ACFE 2020 Report to the Nation



USE OF TARGETED ANTI-FRAUD CONTROLS HAS INCREASED OVER LAST DECADE


HOTLINE	↑ 13%
ANTI-FRAUD POLICY	↑ 13%
FRAUD TRAINING FOR EMPLOYEES	↑ 11%
FRAUD TRAINING FOR MANAGERS/EXECUTIVES	↑ 9%

A lack of internal controls contributed to nearly 1/3 OF FRAUDS

THE PRESENCE OF ANTI-FRAUD CONTROLS IS ASSOCIATED WITH LOWER FRAUD LOSSES AND QUICKER DETECTION

77

ACFE 2020 Report to the Nation



42% OF OCCUPATIONAL FRAUDSTERS WERE LIVING BEYOND THEIR MEANS

26% OF OCCUPATIONAL FRAUDSTERS WERE EXPERIENCING FINANCIAL DIFFICULTIES

78

Bribery and Corruption α

- By far the most common in government officials
- Common in procurement also
- Generally begins by an ethics issue related to a conflict of interest [individual interest takes precedent over organizational interest]
- Breach of Fiduciary Duty [Criminal]

79

Fraudulent Financial Reporting α

- Manipulation, falsification or alteration of accounting records or supporting documentation;
- Misrepresentations or intentional omissions; and/or
- Intentional misapplication of accounting principles

80

Fraud Types

Type of Fraud	Victim	Perpetrator	Explanation
<i>Employee fraud</i>	<i>Employer</i>	<i>Employees</i>	<i>Employees directly or indirectly steal from their employers.</i>
<i>Management fraud</i>	<i>Stockholders, lenders, and others who rely on the financial statements</i>	<i>Management</i>	<i>Top management "cooks the books."</i>
<i>Investment scams</i>	<i>Investor</i>	<i>Individuals</i>	<i>Individuals trick investors into putting money into fraudulent investments.</i>
<i>Vendor fraud</i>	<i>Purchaser</i>	<i>Vendors</i>	<i>Vendors overcharge for goods or services or nonshipment of goods.</i>
<i>Customer fraud</i>	<i>Seller</i>	<i>Customers</i>	<i>Customers deceive sellers into giving customer something they should not have or charging them less than they should.</i>

From *Advanced Fraud Techniques* by Madray & Girolami

81

Employee Frauds ^α

- AKA "Occupational" Fraud
- ACFE *REPORT TO THE NATIONS* – a global study on occupational fraud and abuse
- Methodologies:
 - Direct – Embezzlement
 - Indirect – Bribes, Kickbacks [Corruption]

82

ACFE Fraud Tree

- At the top are the major Fraud Categories
- Then come the Major Schemes
- And then the Sub-schemes/Methodologies

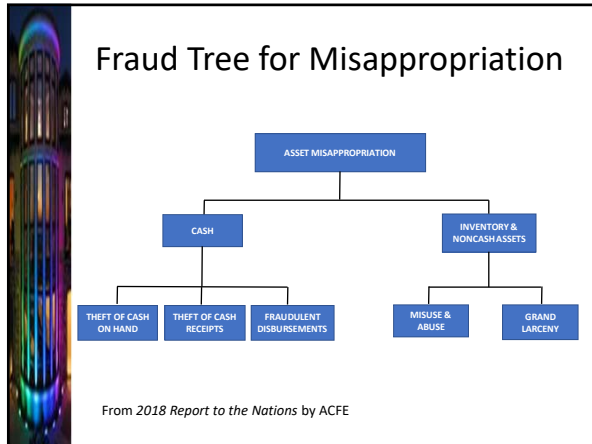
83

Fraud Tree for Corruption

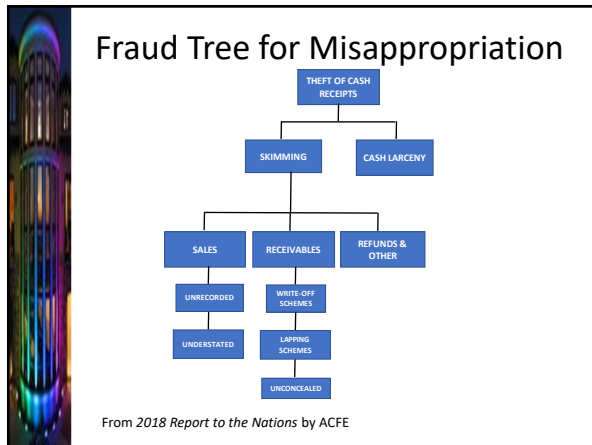
```
graph TD; CORRUPTION --> COI[CONFLICTS OF INTEREST]; CORRUPTION --> BRIBERY; CORRUPTION --> ILLEGAL[ILLEGAL GRATUITIES]; CORRUPTION --> ECONOMIC[ECONOMIC EXTORTION]; COI --> PURCHASING[PURCHASING SCHEMES]; COI --> SALES[SALES SCHEMES]; BRIBERY --> INVOICE[INVOICE KICKBACKS]; BRIBERY --> BID[BID RIGGING];
```

From 2018 Report to the Nations by ACFE

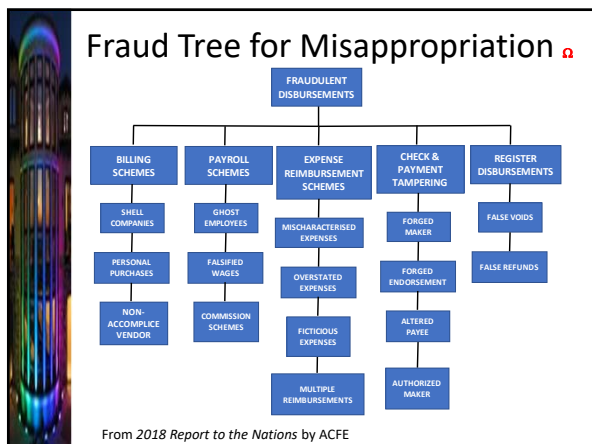
84



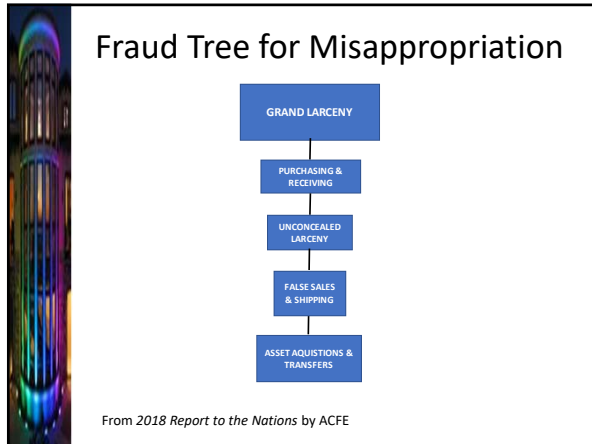
85



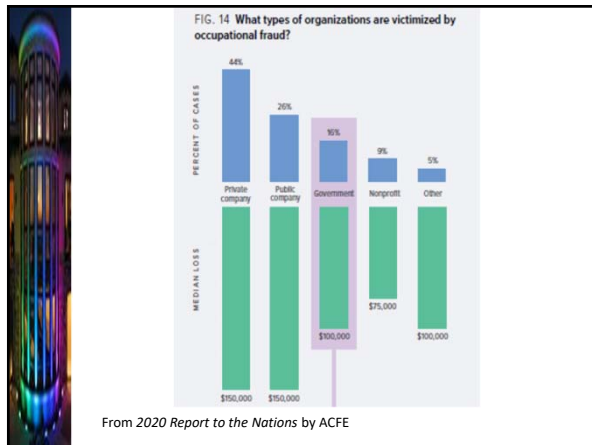
86



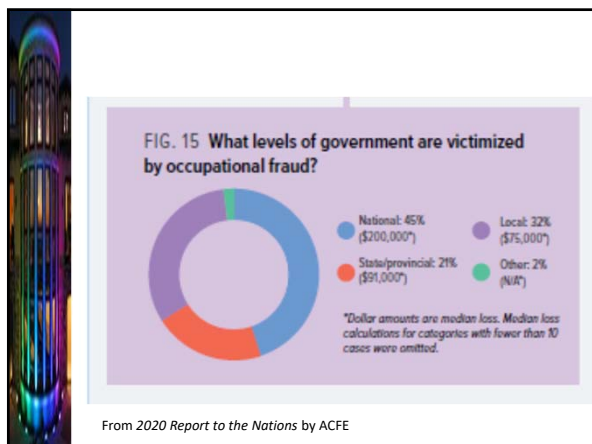
87



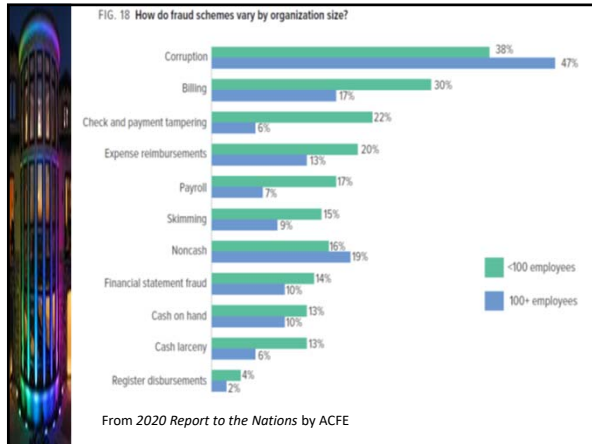
88



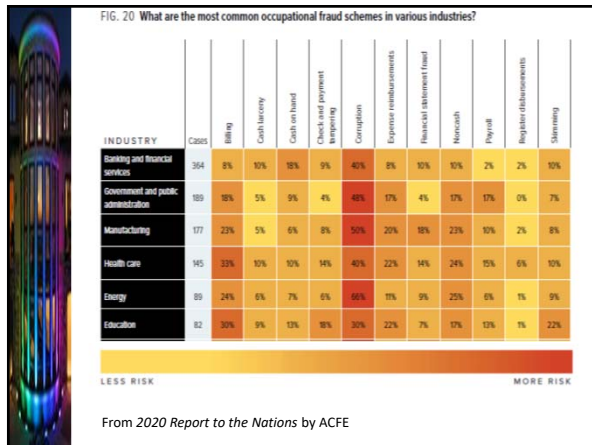
89



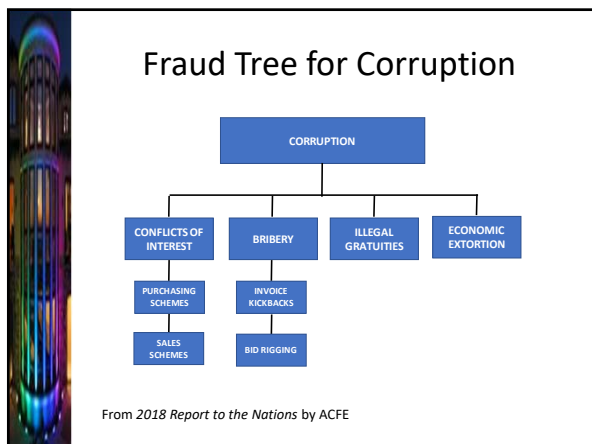
90



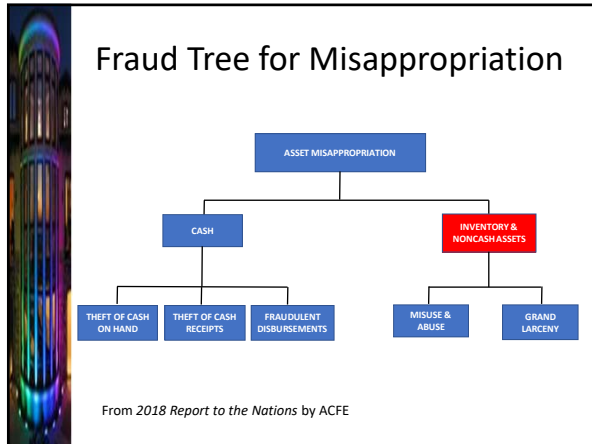
91



92



93



94

RESPONSES

- DETECTION AND DETERRENCE

95

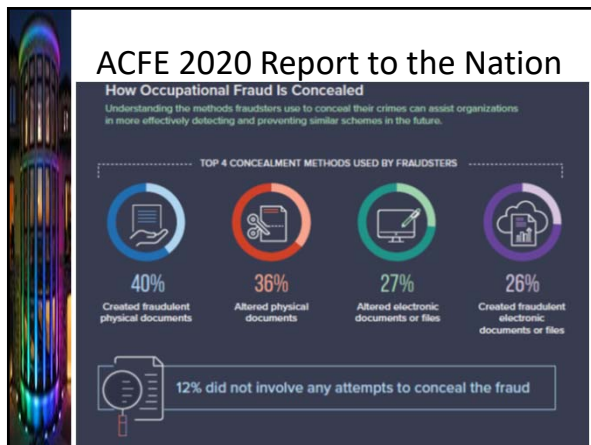
Behavioral Red Flags

- In 85% of cases, Fraudsters displayed at least one of the following behaviors:
 - Living Beyond Their Means
 - Financial Difficulties
 - Unusually Close Association with Vendor/Customer
 - Control Issues; Unwilling to Vacation or Share Duties
 - Divorce, Family Problems
 - “Wheeler-Dealer” Attitude
 - Source: 2018 ACFE Report to the Nations.

96



97



98

-
- Initial Detection Methods**
1. Tips [40%] [43]
 2. Internal Audit Only [15%] [15]
 3. Management Review [13%] [12]
- Source: 2018/2020 ACFE Report to the Nations

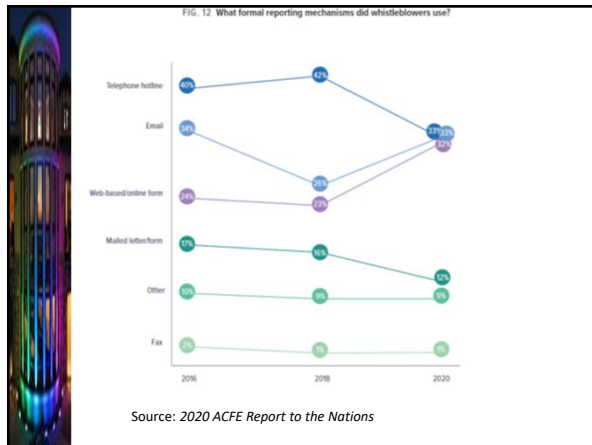
99

Initial Detection Methods ▢

- Who provides the tips?
 - Employees [53%] [50]
 - Customers [21%] [22]
 - Anonymous [14%] [15]
 - Vendors [8%] [11]
 - Other [5%] [6]
 - Competition [3%] [2]
 - Shareholder/Owner [2%] [2]

• Source: 2018/2020 ACFE Report to the Nations.

100



101

Detection Method vs Duration & Loss

- IT Controls [1% of Cases] (Capability Maturity Level 4+) – within 5 months with average loss of \$39,000
- Surveillance/monitoring [3%] – within 6 months and \$50,000
- Account Reconciliation [5%] – within 11 months and \$52,000
- Internal Audit [15%] – within 12 months and \$108,000
- 2018

102

Detection Method vs Duration & Loss

- IT Controls (Capability Maturity Level 4+) – within 6 months with average loss of \$80,000
- Surveillance/monitoring – within 7 months and \$44,000
- Account Reconciliation – within 7 months and \$81,000
- Internal Audit – within 12 months and \$100,000
- 2020

103

Impact of Controls

Control	Percent of cases	Control in place	Control not in place	Percent reduction
Code of conduct	80%	\$ 10,000	\$250,000	96%
Proactive data monitoring/analysis	37%	\$ 80,000	\$ 165,000	52%
Surprise audits	37%	\$ 75,000	\$ 152,000	51%
External audit of internal controls over financial reporting	67%	\$100,000	\$200,000	50%
Management review	66%	\$100,000	\$200,000	50%
Hotline	63%	\$100,000	\$200,000	50%
Anti-fraud policy	54%	\$100,000	\$ 180,000	47%
Internal audit department	73%	\$108,000	\$200,000	46%
Management certification of financial statements	72%	\$109,000	\$ 192,000	43%
Fraud training for employees	53%	\$100,000	\$ 189,000	41%
Formal fraud risk assessments	4%	\$100,000	\$ 162,000	38%
Employee support programs	54%	\$100,000	\$ 160,000	38%
Fraud training for managers/executives	52%	\$100,000	\$ 153,000	35%
Dedicated fraud department, function, or team	4%	\$100,000	\$ 150,000	33%
External audit of financial statements	80%	\$120,000	\$ 170,000	29%
Job rotation/mandatory vacation	19%	\$100,000	\$ 130,000	23%
Independent audit committee	6%	\$120,000	\$ 150,000	20%
Rewards for whistleblowers	12%	\$ 110,000	\$ 125,000	12%

104

Control Factors

- An effective control system is the single, most important step to guard against fraud.
 - The Control Environment
 - The Accounting System [IT, Communication]
 - Control Procedures

105

Internal Control Definition

- 1992 Framework gives us a definition - **a process**, effected by an entity's board of directors, management and other personnel, designed to provide **reasonable assurance** regarding the achievement of **objectives**. [effective/efficient]
- assumes objectives exist

106

Internal Control Definition

- COSO Components**
 - Control Environment
 - Control Activities
 - Information & Communication
 - Monitoring
 - Risk Assessment

107

Internal Control Definition

Another View at the Refresh 2013

The Framework has become the **most widely adopted control framework worldwide**.

108

Internal Control Definition

- **Control Environment Principles**
 - Integrity and Ethical Values
 - Board of Directors
 - Management's Philosophy and Operating Style
 - Organizational Structure
 - Financial Reporting Competencies
 - Authority and Responsibility
 - Human Resources

109

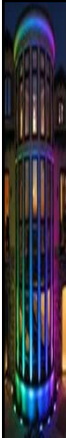
Control Environment

- Tone at the Top
- Code of Conduct is the most effective way to implement measures to reduce wrongdoing
- Culture of honesty
- Ethical Environment
- Positive Workplace Environment

110

RESPONDING TO THE CURRENT RISK ENVIRONMENT

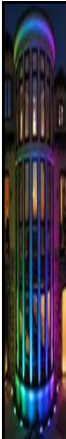
111



Creating a Culture of Honesty

- Create a positive work environment
- Hire honest people and train them about fraud awareness
- Disseminating a well-understood and respected Code of Conduct
- Provide an Employee Assistance Prog.


112



Enemies of a Positive Work Environment

- Uncaring management attitude
- Negative feedback or lack of recognition by management
- Low loyalty or feelings of ownership
- Unreasonable expectations
- Poor training and promotion opportunities
- Less-than-competitive compensation
- Lack of clear responsibilities

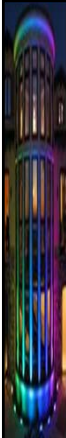
113



Discipline – Sending a Message

- Expectations about the consequences of committing fraud MUST be clearly communicated
- Actions taken in response to alleged fraud should be:
 - Thorough investigation conducted
 - Appropriate and consistent action against perps
 - Relevant controls assessed and improved
 - Communication and training to reinforce entity values, code of conduct and expectations

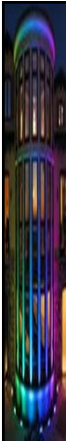
114



Management's Behavior

- Buy-in to Code of Conduct based on management's actions and examples
- Management's consistent treatment of violators of Code of Conduct
- Management's encouragement and openness regarding reporting violations
- Management's actions ARE corporate culture
- Employee Assistance Programs


115



Proactive Data Monitoring/analysis

- Zero tolerance for missing documents, stale items on recons, document alterations
- Prenumbered documents used in sequence
- Unexplained, unusual or unsupported JE's
- Subsidiary ledger and other reconciliations
- Budget comparison, analytical review
- Benford's Law
- Surprise audits

116



Evaluating Processes & Risk Assessment

117

Comparing Frameworks

Risk Assessment in ICIF is Expanded into Three Components:
1) Event Identification 2) Risk Assessment and 3) Risk Response

118

Comparing Frameworks

Linking Organization Essentials

Who is responsible for each of these important elements?
Who determines the first four elements?
Are these part of internal control?

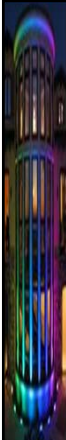
119

How do I Start? α

Build Risk Awareness...

A sustainable ERM initiative must realize the importance of increasing management and employees' general awareness of business risks. As such, a key objective of an ERM initiative is to identify and develop senior management's agreed-upon view and approach to risk management – the Company's risk philosophy – and to identify any gaps between the *existing* understanding of risk and management's *desired (appetite)* risk philosophy.

120

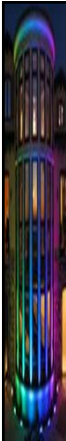


COSO ERM Definition ^α

Enterprise Risk Management (ERM) is a process affected by an entity's board of directors, management and other personnel, applied in a strategic setting and across the enterprise.

ERM is designed to identify potential events or situations that may affect the entity, manage risks to be within the company's risk appetite, and provide reasonable assurance regarding the achievement of entity objectives.

121




Another Definition

- Enterprise Risk Management (ERM) is a process-driven tool that enables senior management to visualize, assess and manage significant risks that may adversely impact the attainment of key organizational objectives

(source: University System of Georgia, Board of Regents ERM program)

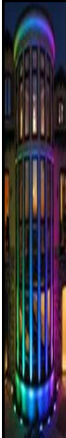
122



Risk Assessment in the Covid-19 Environment

Presented by
Steven L. Blake CPA, CFE, CICA, CGMA
SLBCPA@CHARTER.NET 864-680-6191

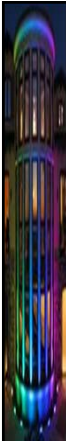
123



Agenda

- THERE WILL BE 4 2-HOUR SESSIONS
- First 2 Hour Session: Learning about the current risk environment.
- Second 2 Hour Session: Understanding the current risk environment
- Third 2 Hour Session: Specific risk assessment techniques and how to adapt them to the current risk environment.
- Fourth 2 Hour Session: Continuance of Third Session.
- Live Questions/Comments Period – Must Attend


124



Creating a Culture of Honesty

- Create a positive work environment
- Hire honest people and train them about fraud awareness
- Disseminating a well-understood and respected Code of Conduct
- Provide an Employee Assistance Prog.


125



Levers of Control α

- Belief System
- Boundary System
- Diagnostic System
- Interactive Control System


126



Belief System

- The entity's core values used to INSPIRE and DIRECT actions


127



Boundary System

- Ethical limits beyond which behavior is prohibited

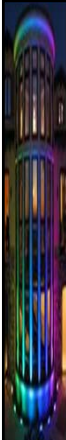
128



Diagnostic System

- The entity's system(s) that ensure the effective and efficient achievement of goals; i.e. budgets

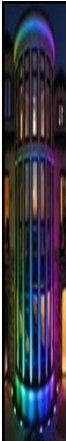
129



Interactive Control System

- The entity's top level development of strategy, risk assessment and monitoring of competitive conditions and technology changes

130




ERM Sustainability


- A popular definition of sustainability is to meet present needs without compromising the ability of future generations to meet their needs.

(Source: United Nations, 1987 Conference)

131




Risk Procedures Integration



```
graph LR; A[Fraud Detection] --> B[Fraud Deterrence]; B --> C[Fraud Prevention];
```


132



Traditional Outlooks

- External audits provide assurance
- People are for the most part honest
- These are good economic times


133



Specific Process Interventions

- TIMELY Reconciliations
- Segregation of Duties
- Cross-training
- Mandatory vacations where others perform your duties and answer your phone calls
- Analytical procedures
- "Turn the Light on" decisions


134



Audit Committee

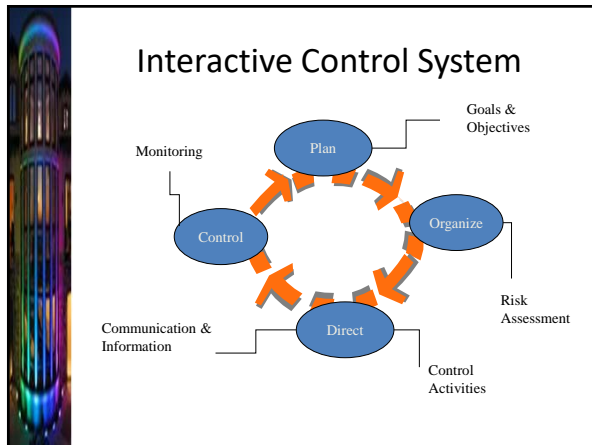
- Evaluate management's identification of fraud risks
- Active oversight to reinforce management's commitment to creating positive corporate culture
- Setting tone at the top
- Serve to deter senior management from fraudulent activity by encouraging measures like Hotlines, analytical review etc.
- Has a financial expert serving

135




**RISK ASSESSMENT – CRAWFORD
METHODOLOGY**

136



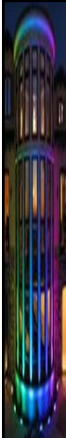
137



**ERM Will Change Your Organizational
Culture**

- Ownership of risk and controls
- Questioning before acting
- Two-way communication
- Bad as well as good news
- Rapid response to changes
- Rapid response to failures in risk management

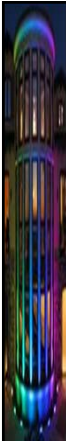
138



Primary ERM Process Activities

- Know the boundaries and obstacles that will have a critical effect on the achievement of objectives
- Optimize the set of strategies to minimize the effect of boundary violations and obstacle occurrences
- Perform on-going assessments of the design and application of mitigation strategies

139




Assurance Continuum ERM Model

- **Standard risk assessment methodology**
- **Common risk language**
- **Standard tools and techniques**
- **Standard outputs**

140

140



Risk Self Assessment Techniques

- **Facilitated Workshop**
 - Management Directed
 - External Facilitator Directed
- **Interviews**
- **Questionnaires**

141

141




Common Risk Language Examples

- Business risk
- Impact
- Probability/likelihood
- Monitoring plan
- On-going assurance
- Periodic assurance
- Goals and objectives
- Level 1 Controls
- Level 2 Controls
- Level 3 Controls
- Level 4 Controls
- Process
- Mitigation strategy
- Assurance Continuum
- Certification
- Self-assessment workshop
- Control footprint
- Risk Footprint

142

142




Standard Tools and Techniques

- Brainstorming
- Excel Workbook (powered by Visual Basic Macros)
- Standard Outputs
 - Risk Footprint
 - Control Footprint
 - The Levels of Control in COSO
 - Monitoring Footprint

143

143



Know the Boundaries and Obstacles

(Risk Assessment)

- Know the desired objectives
- Inventory activities performed to achieve objectives
- Inventory risks (boundary and obstacle) associated with each activity
- Value each risk as to impact on achievement of objectives and probability of occurrence without mitigation strategies
- Produce a risk footprint

144

144

Risk Mgmt. Process

Create A Risk Footprint

1. Identify mission, goals, and objectives
2. Brainstorm Activities
3. Consolidate into Processes
4. Prioritize processes
5. Brainstorm risks for each process
6. Assign Impact and Probability values
7. Construct the Risk Footprint

145

Risk Mgmt. Process

1. Identify Mission, Goals, & Objectives

The mission of the juvenile justice agency education facilities is to:

Provide adequate space and equipment to educate clients in a secure environment

146

Risk Mgmt. Process

2. Brainstorm Activities

1 Provide utilities	13 Budget
2 Access controls	14 Lockdown capability
3 Staff	15 Food service
4 Surveillance cameras	16 Transportation
5 Facility	17 Fire extinguishers
6 Furnishings	18 Medical services
7 Equipment	19 Parking
8 Alarms	20 Landscaping
9 Maintenance	21 Clients
10 Janitorial	22 Storage
11 Emergency plan	23 ADA
12 Communications system	24

26

147

Risk Mgmt. Process

3. Consolidate Activities into Processes and

4. Prioritize

CONSOLIDATED ACTIVITIES	PRIORITIZED CONSOLIDATED ACTIVITIES
Maintenance (1,7,9,10)	1 Security & Safety(2, 3, 4, 8, 11, 14, 16, 17)
Security & Safety(2, 3, 4, 8, 11, 14, 16, 17)	2 Facility (5, 6, 7, 12, 19, 20, 21, 22)
Facility (5, 6, 7, 12, 19, 20, 21, 22)	3 Administration (13, 15, 18, 23)
Administration (13, 15, 18, 23)	4 Maintenance (1, 7, 9, 10)

1 Provide utilities	13 Budget
2 Access controls	14 Lockdown capability
3 Staff	15 Food service
4 Surveillance cameras	16 Transportation
5 Facility	17 Fire extinguishers
6 Furnishings	18 Medical services
7 Equipment	19 Parking
8 Alarms	20 Landscaping
9 Maintenance	21 Clients
10 Janitorial	22 Storage
11 Emergency plan	23 ADA
12 Communications system	24

6

148

Risk Mgmt. Process

5. Brainstorm Risks for Each Process

Maintenance (1, 7, 9, 10)	IMPACT	PROB.	RANKING
Insecure facility			n/a
Unlicensed facility			n/a
Deferred maintenance			n/a
Equipment breakdown			n/a
Inadequate staff			n/a
Theft			n/a
Unsanitary or unhealthy environment			n/a
Injury or death			n/a
Lawsuit - individual			n/a

149

Risk Mgmt. Process

6. Assign Impact & Probability to Each Risk

Maintenance (1, 7, 9, 10)	IMPACT	PROB.	RANKING
Insecure facility	h	m	HM
Unlicensed facility	h	m	HM
Deferred maintenance	m	h	MH
Equipment breakdown	m	m	MM
Inadequate staff	m	m	MM
Theft	m	m	MM
Unsanitary or unhealthy environment	m	m	MM
Injury or death	m	l	ML
Lawsuit - individual	l	m	LM

150

Risk Ranking Characteristics

Impact: Effect on achievement of goals & objectives

- [H] High - "showstopper"
- [M] Medium - inefficient and extra work
- [L] Low - no effect

Probability: Likelihood of the risk happening

- [H] High - will happen frequently
- [M] Medium - will happen infrequently
- [L] Low - will seldom happen

151

151

How to Value Impact

- Develop a list of consequences to the organization if a risk were to become a reality (Every organization has a finite number of potential consequences)
- Value the effect on the organization for each consequence (high, medium, or low)
- The Impact value of an identified risk is the value of its highest potential consequence

152

152

Example: Impact Valuation

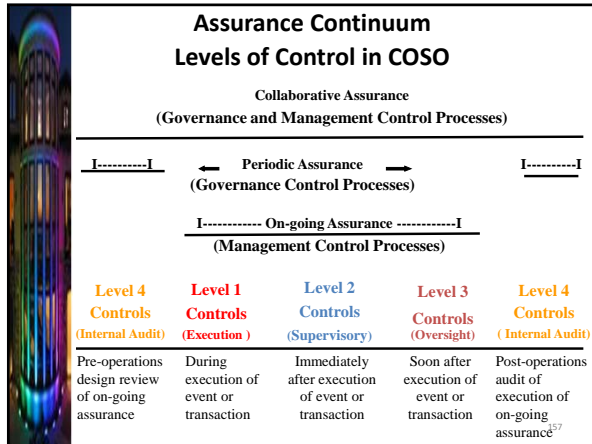
- Activity: Own an Automobile
 - Consequence with Value to Owner

• Loss of asset	Medium
• Death/Major Injury	High
• Minor Injury	Low
• Criminal penalty	High
 - Risk with associated consequence & value

• Fender Bender	<i>Minor Injury</i>	L
• DWI	<i>Criminal penalty or D/I</i>	H
• No PM	<i>Loss of asset</i>	M

153

153



157

Optimize the Portfolio of Mitigation Strategies (Control Optimization)

- Inventory mitigation strategies used to manage each activity row on the risk footprint
- Assign appropriate Level of Control to each mitigation strategy
- Assign inventoried strategies to identified risks
- Identify under-controlled and over-controlled risks
- Identify excess or unproductive mitigation strategies
- Optimize the mitigation strategy portfolio

158


158

Risk Mgmt. Process

Level 1 Controls (Execution Controls)

- Embedded in day-to-day operations
 - Policies and procedures
 - Segregation of Duties
 - Reconciliations/Comparisons
- Performed on every event/transaction
- Performed by the generators of the event/transaction
- Performed in ‘real time’, as the event/transaction is executed

159




Risk Mgmt.
Process

Level 2 Controls (Supervisory Controls)

- Re-application of operating controls
 - Supervisory Review; Quality Assurance; Self Assessment
- Performed very soon after the generation of the event/transaction
- Performed by line management or staff positions who do not originate the event/transaction
- Performed on a sample of the total number of events/transactions

160




Risk Mgmt.
Process

Level 3 Controls (Oversight Controls)

- Exception reports, status reports, analytical reviews, variance analysis
- Performed by representatives of executive management
- Performed on information provided by supervisory management
- Performed within a short period (weeks/months) after the event/transaction is originated

161



Risk Mgmt.
Process

Level 4 Controls (Internal Audit Controls)

- Audit of the design of controls not the operation of controls
- Performed either before the event/transaction is originated or long after
- Performed by staff with no involvement in the operations
- Performed on individual events/transactions for discovery only

162

Risk Mgmt. Process **Create Control Footprints (1/3)**

- Construct a control footprint matrix for each activity on the risk footprint
 - Risk Axis (horizontal axis) contains the prioritized risks taken electronically from the risk footprint
 - Control Axis (vertical axis) contains all the control steps in the process and are entered manually by YOU (See next slide for description of how to create the Control Axis)
 - Place an “X” in each cell where a control step operates to mitigate a risk

163

Risk Mgmt. Process **Create Control Footprints (2/3)**

- Create the Vertical Axis (Control Steps) in the following manner:
 - List a control step from documented procedures or brainstorming
 - Identify the Level of Control for that step
 - List associated control steps and their Level of Control
 - Repeat the process for the next control step from brainstorming or documented procedures
 - Example:
 - First listed step: Review Bank Reconciliation *Level 2*
 - Associated steps: Prepare Bank Reconciliation *Level 1*
Review Summary of Adjustments *Level 3*
 - Next listed step: Issue cash receipt *Level 1*
 - Associated step: Compare total receipts to total of cash *Level 3*
 - New listed step: Acknowledgement for transfer of cash from one employee to another *Level 1*

164

Risk Mgmt. Process **Create Control Footprints (3/3)**

- Identify sets of associated controls (levels 1 and 2 or levels 1, 2, and 3) that provide the most assurance concerning mitigation of both Red and Yellow risk and all risks
- Color code those controls to indicate subjects for on-going monitoring

165

Risk Mgmt. Process

Control Footprint Usage

Indicates

- most important controls for ensuring risks are being controlled as planned
- under or over control
- Optimal control mixture

166

Risk Mgmt. Process

Control Footprint

Level	Maintenance (1, 7, 9, 10)	Insecure facility	Unlicensed facility	Deferred maintenance	Epileptic break down	Inadequate staff	Unsanitary or unhealthy environment	Theft	Injury or death	Lawsuit - Individual
3	Mgr. Walkthrough	x	x							
1	Security check on staff ins. & outs	x					x		x	
1	Preventive maintenance schedule	x	x	x	x			x	x	x
2	Supervisor reviews completed maintenance	x	x	x	x			x	x	x
3	Spot check of equipment by Mgr.	x	x	x	x			x	x	x
1	Checklist of tasks		x					x	x	x
2	Visual inspection by Supervisor		x					x	x	x
1	Training of employees	x	x		x	x	x	x	x	x
2	Comparison of training log to list of employees	x	x		x	x	x	x	x	x
3	Exception report to Mgr. About temps not attended	x	x		x	x	x	x	x	x

167

Perform On-going Assessments

- Determine the mitigation strategies that provide the most assurance that critical risks are being managed
- Develop a monitoring plan for assessment of the proper application of planned mitigation strategies
- Perform continuous monitoring using the plan to ensure acceptable performance and desired results

168

56

Monitoring Footprint

Level		Access Facility	Uncompensated Facility	Deferred maintenance	Equipment breakdown	Workload management	Training or development	Injury or death	Loss of individual	Evidence of Control	Date	Review	Status
3	Mgr. Walkthrough	X	X	X	X	X	X	X	X				
3	Security check on staff ins & outs	X					X	X					
1	Preventive maintenance schedule	X	X	X	X		X	X	X	Preventive maintenance schedule			
1	Supervisor reviews completed maintenance	X	X	X	X		X	X	X	Supr. Signs & dates report with notes			
2	Spot check of equipment by Mgr.	X	X	X	X		X	X	X	List of equip. checked; Memo to file; Sign log on equip.			
1	Checklist of tasks	X					X	X	X				
2	Visual inspection by Supervisor	X					X	X	X				
1	Training of employees	X	X		X	X	X	X	X	Training roster, certificates, curriculum			
2	Comparison of training log to list of employees	X	X		X	X	X	X	X	Report of exceptions signed & dated Manager initials & dates with comments of actions taken.			
3	Exception report to Mgr. About emps not attended	X	X		X	X	X	X	X				

169

Resources

Effective Compliance Systems: A Practical Guide for Educational Institutions
[Crawford,et al] www.theiia.org

www.COSO.org

www.csa-pdk.com


Email: crawfordjd@earthlink.net

170

FIRST RISK ASSESSMENT ASSIGNMENT

- Work-from-home security
 - Access Controls
 - Home Network
 - Passwords
 - “I am not a robot” button
 - Two-factor Authentication


171



Access Controls

- Initial control is Password Control for a specific user
- Then access control over specific user. Users only have access to the needed systems/processes they are using
- At this point password security IS CRUCIAL. Especially in the 'work-from-home' environment.


172



Secure Access

- How do you access your system(s) from home?
 - ISP provided access [cable, T1, wireless]
 - Wireless – what protocols, what security?
 - Firewalls?
 - VPN?

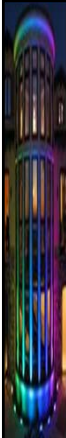
173



ISP Provided

- Does your ISP provide any security?
 - Firewalls
 - VPN
 - Encryption

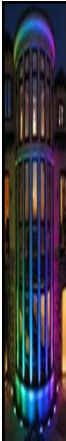
174



Wireless

- **Wireless Protocols**
 - Speed
 - Legacy 802.11 – 2.4GHz, 2Mbps
 - 802.11b – 2.4GHz, 11Mbps
 - 802.11a – 5GHz, 54Mbps
 - 802.11g – 2.4GHz, 54Mbps
 - Security
 - WEP, WPA, WPA2 WPA3


175



Wireless Security

- **WEP = Wired Equivalent Privacy**
 - 1999-2004 Standard; Easy to break, hard to configure – abandoned. BUT some may still have it at home
 - WPA – Wi-Fi Protected Access
 - Temporary enhancement to WEP. Also easy to break
 - WPA2
 - Uses AES [Advance Encryption Standard]; Top secret government security clearance. Good security unless you have WPS.

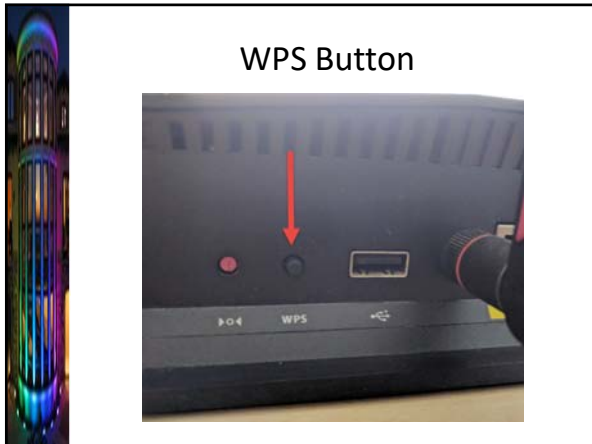
176



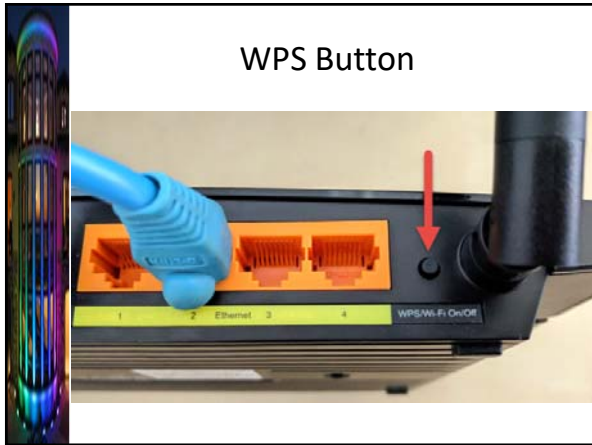
Wireless Security

- **WPS – WiFi Protected Setup**
 - This is an additional protocol on your home network wireless router. How physically secure?
 - It is designed to be used only on home networks that require a password [so far so good] and is a **BUTTON** on the router usually.
 - As stated, it is used in the setup process to streamline setup. It sends the password out to devices it “discovers” automatically so you don’t have to know the password. Physical access to your router is all you need!!

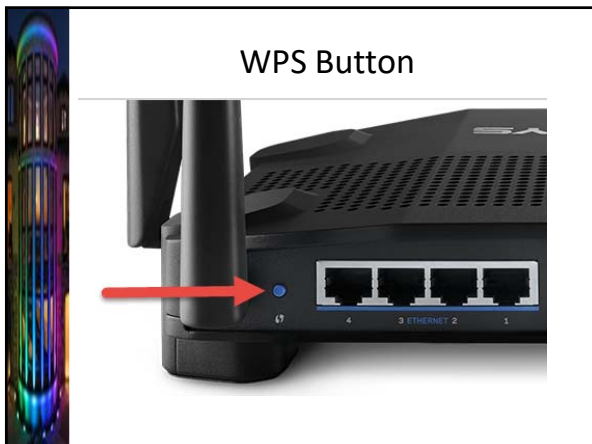
177



178



179



180

WPS Button

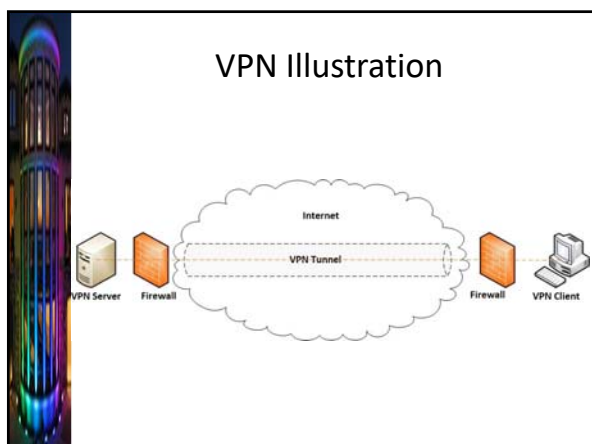
- WPA3
 - The Internet of Things [IoT] protocol
 - Stops KRACK vulnerability [encrypted connections]
 - Stops decrypting older data, only current, hacked data
 - WiFi Easy Connect for devices [printers et. al.]
 - Public WiFi Opportunistic Wireless Encryption

181

Wireless Security

- WEP = Wired Equivalent Privacy
 - 1999-2004 Standard; Easy to break, hard to configure – abandoned. BUT some may still have it at home
 - WPA – Wi-Fi Protected Access
 - Temporary enhancement to WEP. Also easy to break
 - WPA2
 - Uses AES [Advance Encryption Standard]; Top secret government security clearance. Good security unless you have WPS.

182



183
