26th Annual ACFE Global
FRAUD CONFERENCE

ACFE
Association of Certified Fraud Examiners

# You Completed a Fraud Risk Assessment: Now, What Do You Do with the Information?

Carol Morgan, CFE, CPA, CIA, CCEP, CISA, CGMA

# You Completed a Fraud Risk Assessment:

## Now, What Do You Do?

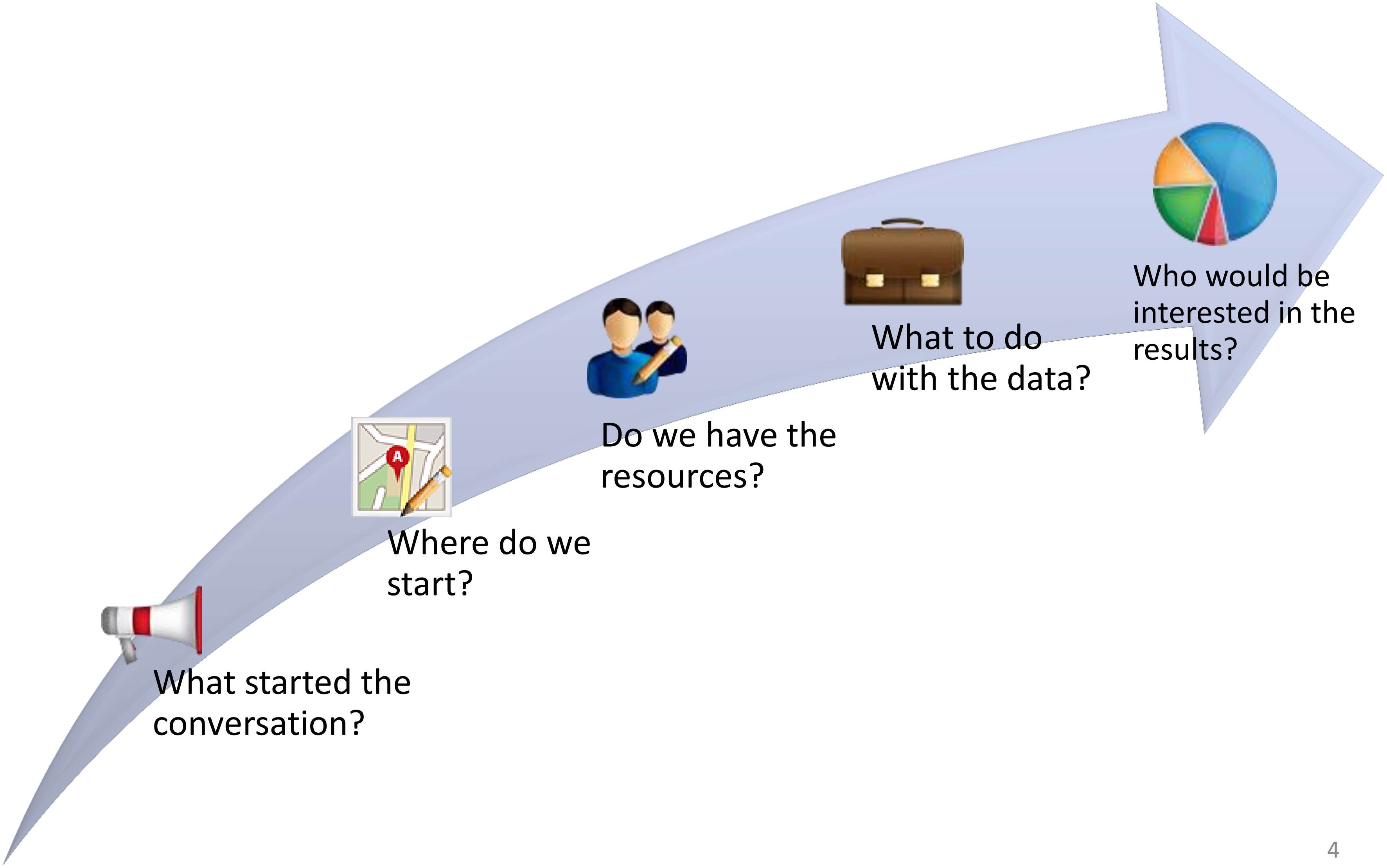
Carol A Morgan, CPA, CIA, CFE, CCEP, CISA
VP Audit & Risk Management Services
World Vision, Inc.

# Speaker Biography – Carol Morgan

As VP of Audit & Risk Management Services for World Vision, a Christian humanitarian organization dedicated to working with children, families, and their communities, I am responsible for planning and completion of operational, compliance, and financial audits conducted at all World Vision U.S. sites. In addition, my group is responsible for oversight of the compliance framework, data security, and enterprise risk management.

I began my auditing career with the Defense Contract Audit Agency (DCAA) in the Washington, DC, area. A move to Seattle, Washington, helped to develop my internal auditing skills while working for SAFECO Insurance. Returning to government auditing as Manager of Internal Audit for Todd Pacific Shipyards, I reestablished the internal audit function and was responsible for operational and government contract compliance audits. Prior to joining World Vision, I gained external auditing experience as a manager with the public accounting firm McGladrey and Pullen, LLP, where I performed financial statement audits of credit unions. I hold a BS degree from Towson University. I am a Certified Public Accountant, (CPA), Certified Fraud Examiner (CFE), Certified Internal Auditor, (CIA ), Certified Corporate Compliance & Ethics Processional (CCEP), and Certified Information Systems Auditor (CISA).

# Let’s Talk Fraud Risk Assessment



What started the conversation?

Where do we start?

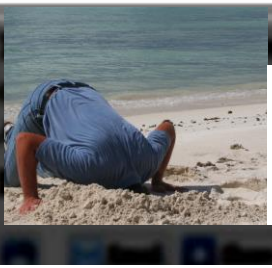
Do we have the resources?

What to do with the data?

Who would be interested in the results?

Los Angeles Times

# U.S. bans non-profit from further aid programs



"…Execs believed implementing controls slowed down business."

"…We thought systems were in place to catch wrongdoing."

"…well paid employees have no reason to steal."

"…business claims they only hire good people."

"…board acted on the belief assets were not at risk."

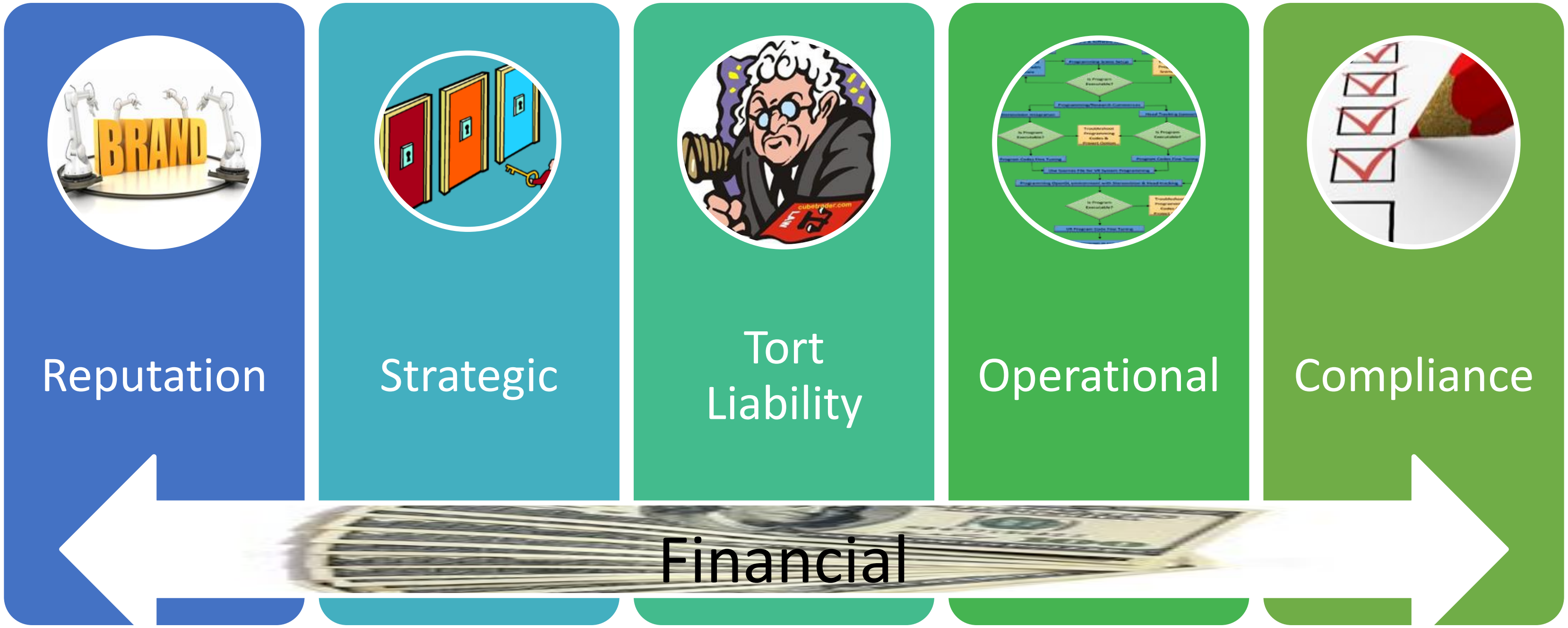
"…fraud prevention costs not worth the pound of cure."

# Can We See Behind the Doors?

Fordon som hindrar fri passage
anmäls för bortforsling
Garage
Fordon som hindrar fri passage
anmäls för bortforsling

# Why Conduct a Fraud Risk Assessment?

## Fraud is a ***business risk***
## not just a finance issue



Reputation

Strategic

Tort Liability

Operational

Compliance

Financial

# Where Do We Start?

There were just a few points to consider:

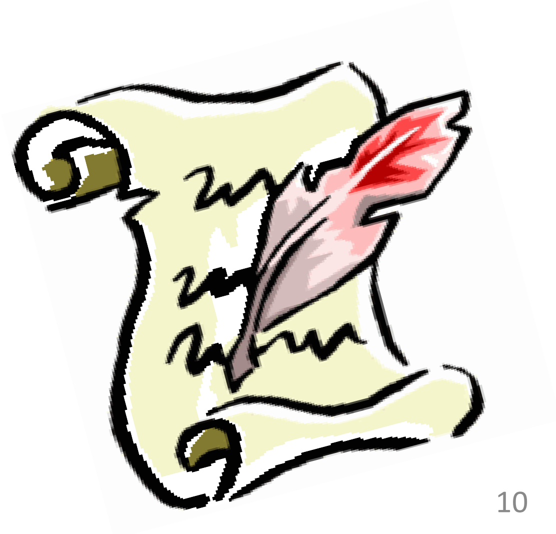
- →Fraud controls may not be a primary objective.
- →Who would own the process?
- →Do we have any experts?
- →What tool will work best?
- →What does reporting results look like?

# We Have Some Easy Answers

- Raise awareness around the code of ethics and the complementary fraud waste and abuse policy
- Tap into existing risk assessment skills
- Explore tools and guidance
- Agreement that the board and management teams should received a report of the outcomes

# Reviewed the Fraud Policy To Ensure It…

- Sets the ethical tone complimenting the Code
- Conveys the intent for risk reducing control measures to be implemented
- Provides procedures to deal with suspected events
- Communicates mechanisms for voicing concerns
- Defines accountability process
- Requires ongoing  training



# Who Has the Skill Set?

- Internal opportunities
  - Internal auditors
  - Risk managers
  - ISO-Certified resources
  - Certified Fraud Examiners
  - Loss Prevention Specialists
  - Business owners
- External consultants

Do Not Ignore

All Parts of the Organization

# Tools Are Similar, Yet Different

- Auditor information gathering assessment
- Formal facilitated sessions
- Informal roundtable discussions
- Checklists and surveys

AICPA

The Institute of Internal Auditors

ACFE Association of Certified Fraud Examiners

# Planning with the End in Mind

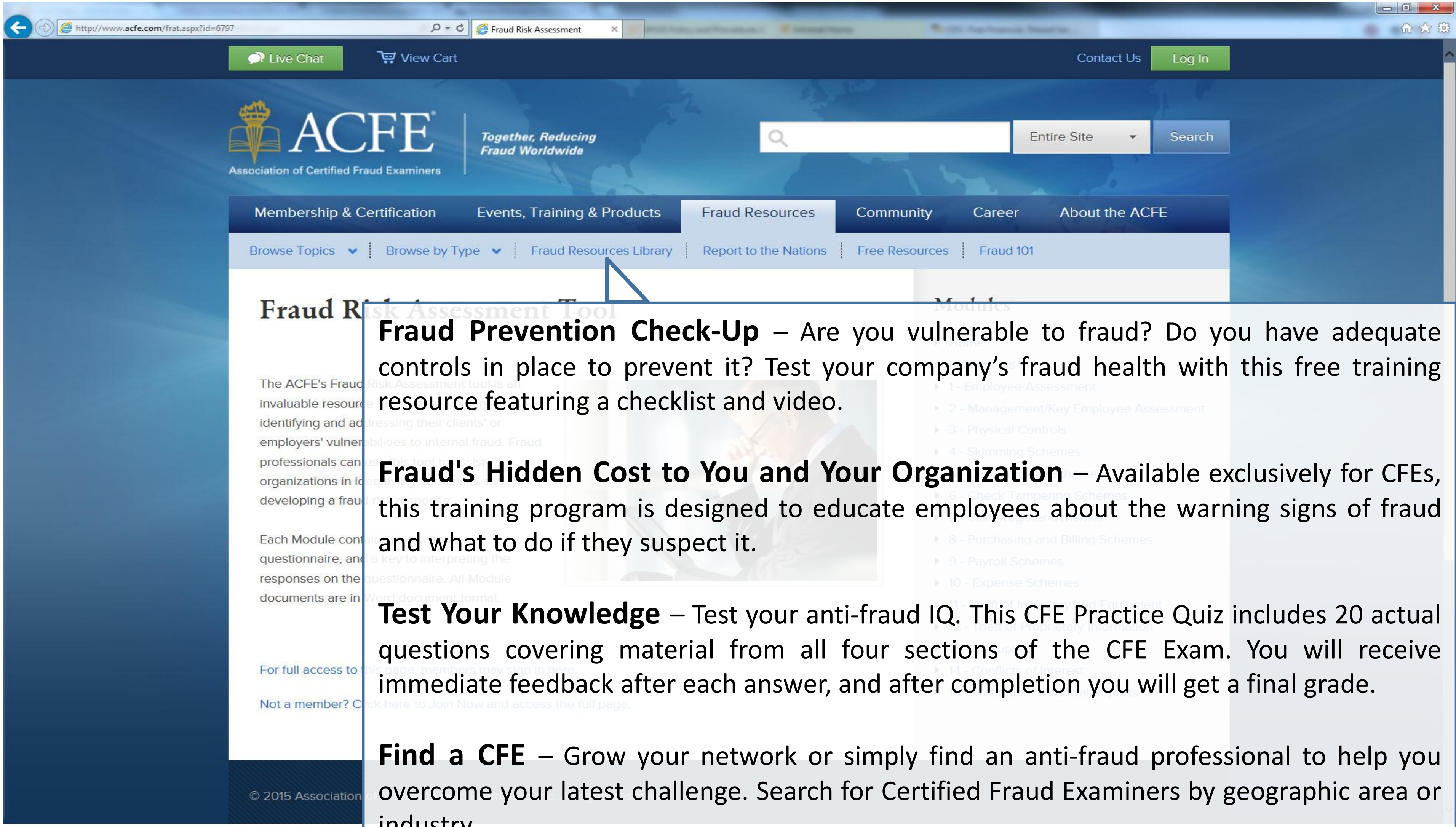
- Report to management
- Provide assurance to the board

BUT---

What will that look like??

I'll think
about that
tomorrow....
- Scarlett
O'Hara

# Why Recreate the Wheel?


http://www.acfe.com/frat.aspx?id=6797
Fraud Risk Assessment
Live Chat
View Cart
Contact Us
Log In
ACFE
Association of Certified Fraud Examiners
Together, Reducing Fraud Worldwide
Entire Site
Search
Membership & Certification
Events, Training & Products
Fraud Resources
Community
Career
About the ACFE
Browse Topics
Browse by Type
Fraud Resources Library
Report to the Nations
Free Resources
Fraud 101
Fraud Risk Assessment Tool
Modules
1 - Employee Assessment
2 - Management/Key Employee Assessment
3 - Physical Controls
4 - Skimming Schemes
6 - Check Tampering Schemes
8 - Purchasing and Billing Schemes
9 - Payroll Schemes
10 - Expense Schemes
11 - Theft of Inventory and Equipment
14 - Conflicts of Interest
© 2015 Association

The ACFE's Fraud Risk Assessment tool is an invaluable resource ... identifying and addressing their clients' or employers' vulnerabilities to internal fraud. Fraud professionals can use this tool to assist organizations in identifying ... and developing a fraud ...

Each Module contains ... questionnaire, and a key to interpreting the responses on the questionnaire. All Module documents are in Word document format.

For full access to this page, members may sign in here.

Not a member? Click here to Join Now and access the full page.

**Fraud Prevention Check-Up** – Are you vulnerable to fraud? Do you have adequate controls in place to prevent it? Test your company's fraud health with this free training resource featuring a checklist and video.

**Fraud's Hidden Cost to You and Your Organization** – Available exclusively for CFEs, this training program is designed to educate employees about the warning signs of fraud and what to do if they suspect it.

**Test Your Knowledge** – Test your anti-fraud IQ. This CFE Practice Quiz includes 20 actual questions covering material from all four sections of the CFE Exam. You will receive immediate feedback after each answer, and after completion you will get a final grade.

**Find a CFE** – Grow your network or simply find an anti-fraud professional to help you overcome your latest challenge. Search for Certified Fraud Examiners by geographic area or industry.

* Taken From ACFE Web site

# ACFE Assessment Tool

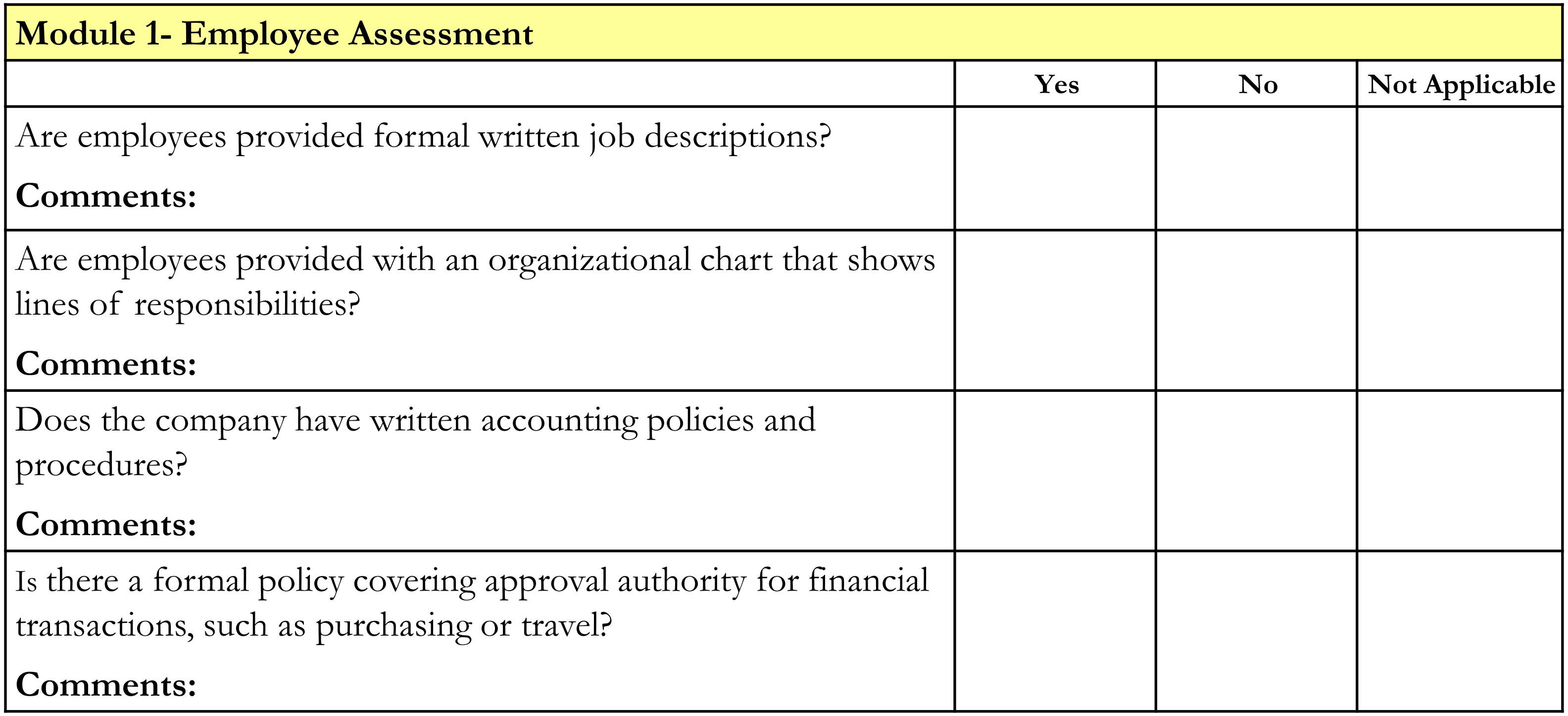
1. Employee Assessment
2. Management/Key Employee Assessment
3. Physical Controls to Deter Employee Theft and Fraud
4. Skimming Schemes
5. Cash Larceny Schemes
6. Check Tampering Schemes
7. Cash Register Schemes
8. Purchasing and Billing Schemes
9. Payroll Schemes
10. Expense Schemes
11. Theft of Inventory and Equipment
12. Theft of Proprietary Information
13. Corruption
14. Conflict of Interest
15. Fraudulent Financial Reports

* Taken from ACFE Website

# Module Assessment Tool

## Series of Internal Control Questions

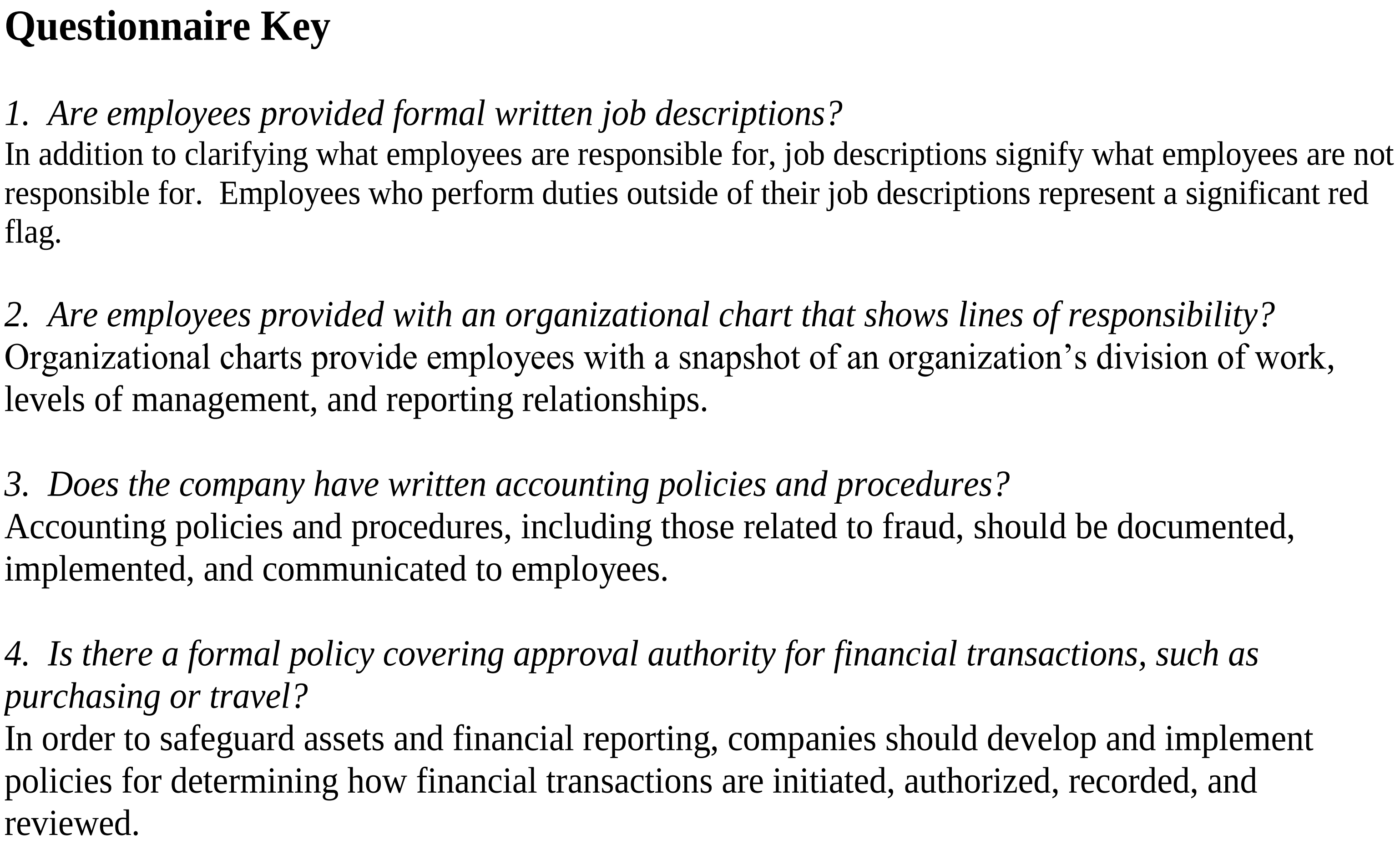
- Requires a YES, NO, or NA response
- Comprehensive – all questions may not be germane to your environment



| **Module 1- Employee Assessment** | | | |
|---|---|---|---|
| | **Yes** | **No** | **Not Applicable** |
| Are employees provided formal written job descriptions?<br>**Comments:** | | | |
| Are employees provided with an organizational chart that shows lines of responsibilities?<br>**Comments:** | | | |
| Does the company have written accounting policies and procedures?<br>**Comments:** | | | |
| Is there a formal policy covering approval authority for financial transactions, such as purchasing or travel?<br>**Comments:** | | | |

* Taken from ACFE Website

# Questionnaire Key



**Questionnaire Key**

*1.  Are employees provided formal written job descriptions?*
In addition to clarifying what employees are responsible for, job descriptions signify what employees are not responsible for.  Employees who perform duties outside of their job descriptions represent a significant red flag.

*2.  Are employees provided with an organizational chart that shows lines of responsibility?*
Organizational charts provide employees with a snapshot of an organization’s division of work, levels of management, and reporting relationships.

*3.  Does the company have written accounting policies and procedures?*
Accounting policies and procedures, including those related to fraud, should be documented, implemented, and communicated to employees.

*4.  Is there a formal policy covering approval authority for financial transactions, such as purchasing or travel?*
In order to safeguard assets and financial reporting, companies should develop and implement policies for determining how financial transactions are initiated, authorized, recorded, and reviewed.

* Taken from ACFE Website

# Tool in Action

Using each of the modules—

- Trimmed the questions to those that made sense in our environment
- Gathered information documented during the audit process and other risk assessment effort
- Reached out to stakeholders to validate known data and fill in the unknowns

# TOMORROW IS HERE!!

# TIME TO THINK ABOUT WHAT TO REPORT??

# What to Do with All the Data?

# Translate It into Clear Usable Report

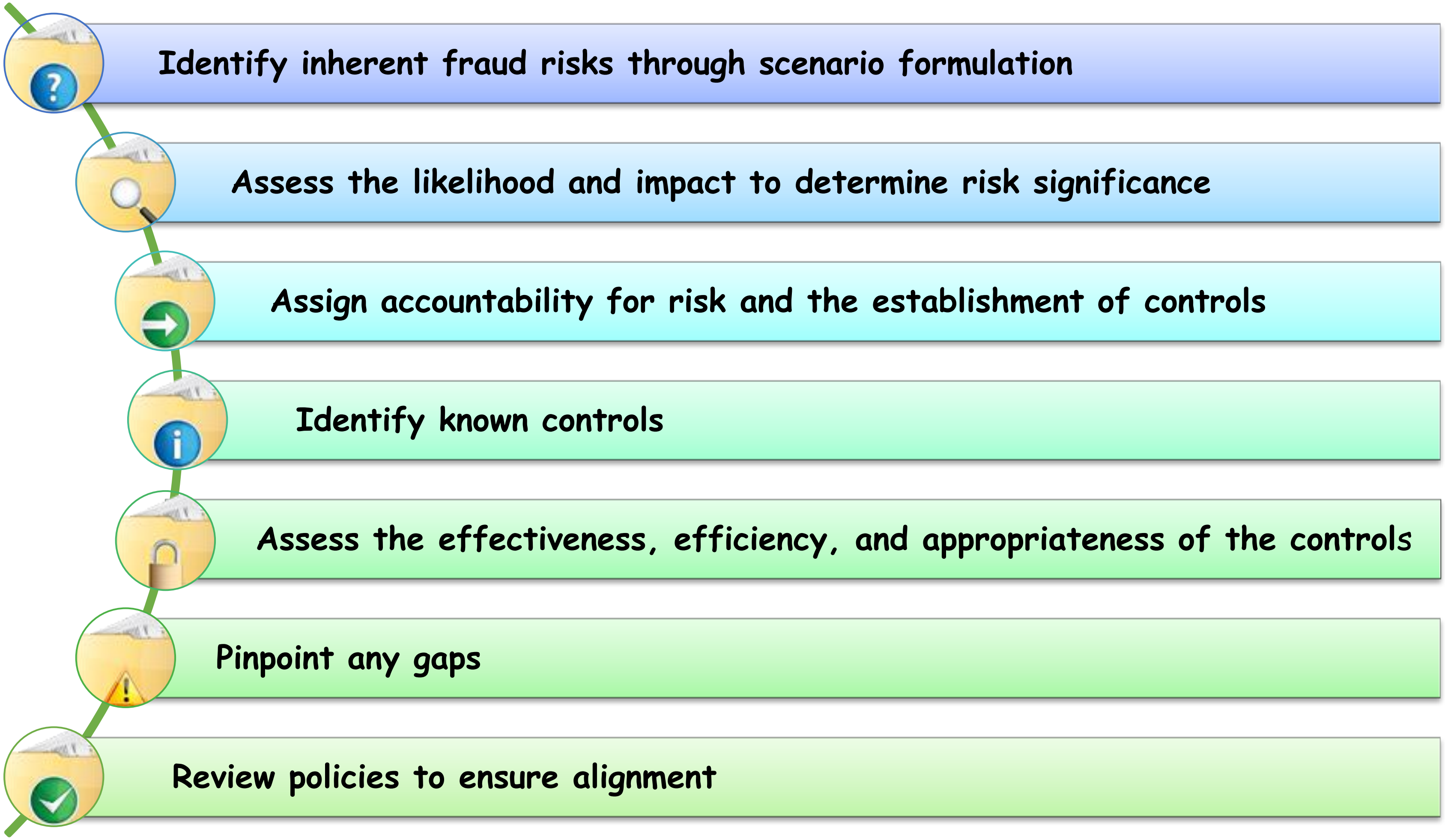
Classic Pumpkin Pie

- ☐ 9-inch Pre-baked pie shell
- ☐ 1 can (15 ounce) Libby's 100 percent pure pumpkin
- ☐ 1 1/2 cups half and half
- ☑ 3/4 cup granulated white sugar
- ☐ 1/4 cup maple syrup
- ☐ 2 large eggs, lightly beaten
- ☐ 1/4 teaspoons fine-grain sea salt
- ☑ 3 teaspoons pumpkin pie spice (see below)
- ☑ Pumpkin Pie Spice:
- ☐ 2 1/2 teaspoons cinnamon
- ☐ 1 teaspoons ginger
- ☐ 1 teaspoons nutmeg
- ☐ 1/2 teaspoons cloves

How to connect the list of controls?

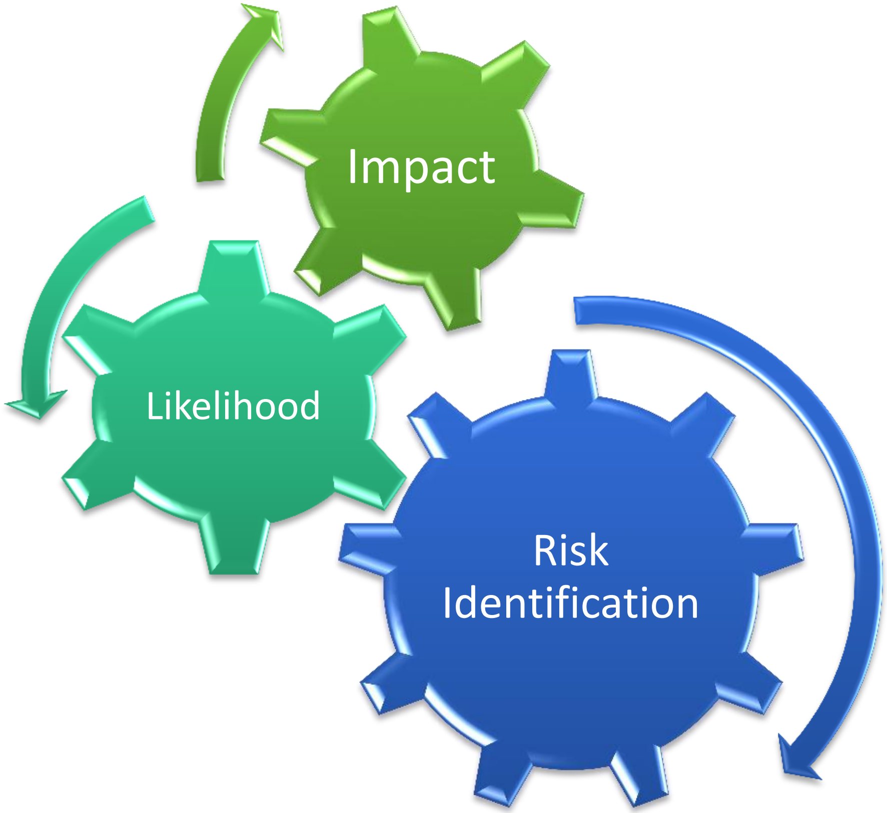
To what is important!

# Key Activities



- Identify inherent fraud risks through scenario formulation
- Assess the likelihood and impact to determine risk significance
- Assign accountability for risk and the establishment of controls
- Identify known controls
- Assess the effectiveness, efficiency, and appropriateness of the controls
- Pinpoint any gaps
- Review policies to ensure alignment

# Define the Lexicon



# Risk Identification

| | |
|---|---|
| ***Hazard risk:*** | Liability torts<br>Property damage<br>Natural catastrophe |
| ***Financial risk***: | Asset risk<br>Currency risk<br>Liquidity risk |
| ***Reputation risk***: | Brand<br>Integrity<br>Public confidence |
| ***Operational risk***: | Donor satisfaction<br>Program failure<br>Systems breakdown<br>Technology obsolescence<br>People |
| ***Compliance risk***: | Regulatory<br>Contractual requirements<br>Policy and procedures |
| ***Strategic risk***: | Competition<br>Social trend<br>Capital availability |

# Likelihood and Impact

| Level | Measurement of Likelihood | |
|---|---|---|
| 1. | ***Rare*** | Not expected to occur in the next ten years. |
| 2. | ***Unlikely*** | Could occur at sometime in the next ten years. |
| 3. | ***Possible*** | Might occur in the next five years. |
| 4. | ***Likely*** | Will probably occur at least once a year. |
| 5. | ***Almost Certain*** | Expected to occur more than once per year. |

| Level | Measurement of Impact | |
|---|---|---|
| 1. | ***Insignificant*** | Little or no impact |
| 2. | ***Minor*** | Minor loss or damage |
| 3. | ***Serious*** | Major loss or damage |
| 4. | ***Disastrous*** | Significant loss or damage |
| 5. | ***Catastrophic*** | Complete loss or devastating destruction |

Taken from University of Washington ERM

# ACFE Assessment Tool Objectives

1. Hire and grow ethical employee base
2. Employees will conduct themselves in an ethical manor
3. Only authorized employees will have access to assets
4. Cash payments will be properly accounted for
5. Cash at point of sale will be secured
6. Checking activities will be safeguarded
7. Security over acceptance of cash will be preserved
8. Purchasing & Billing activities will have oversight
9. Authentic employees will be paid at agreed to rate and for actual hours worked
10. Payments will be made for legitimate expenses
11. Inventory and assets will be protected
12. Intercultural property will be protected
13. Employees will not engage in corruptive activities
14. Conflicts of interest will be reported
15. Financial reporting will be accurate

# Scenario Creation

| |
|---|
| **Module #1** |
| **Employee Schemes** |
| 1. Employee’s information used for hiring purposes is fraudulent increasing the risk of a bad hire. |
| 2. Employees are not adequately trained to ensure acceptable behavior. |
| **Module #2** |
| **Management Override Schemes** |
| 1. Unauthorized or fictitious journal entries are made in the accounting data increasing the risk of misstament. |
| 2. Key employees have close friends or relatives reporting to them permitting the possibility of collusion. |
| 3. Preferential treatment is given to a vendor by an employee relative. |
| **Module #3** |
| **Breaches of Physical Controls** |
| 1. Unlawful physical access to financial systems occurs resulting in material unauthorized alteration of financial data. |
| 3. Unlawful physical access to financial systems resulting in loss or abuse of financial data. |
| **Module #4** |
| **Skimming Schemes** |
| 1. Cash is accepted but not recorded as a donation or other cash receipts. |
| 2. Cash is collected but under reported as a donation or other cash receipts |
| **Module #5** |
| **Cash Larceny Schemes** |
| 1. Cash is stolen while processing donations. |
| 2. Cash is stolen at fundraising events. |
| 3. Cash is stolen from cash receipts at storehouses. |

# Fraud Risk Register

| Fraud Risk Scenario | Likelihood | Impact | Accountable Department | Existing Controls | Effectiveness of Controls | Policy and Procedures |
|---|---|---|---|---|---|---|
| **Module #1** | | | | | | |
| **Employee Schemes** | | | | | | |
| 1.Employee's information used for hiring purposes is fraudulent increasing the risk of a bad hire.<br>***Risk***<br>Financial<br>Reputational<br>Operational<br>Compliance | ***Likely*** | ***Serious*** | Human Resource<br>Legal<br>Finance | 1. Dedicate professional recruiters<br>2. Existence of formal written job descriptions<br>3. Code of Ethics<br>4. Written fraud policy<br>5. Written policies and procedures<br>6. Integrity Hotline<br>7. Background check required for hire<br>8. Internal Audit Department<br>9. Automated timekeeping system to monitor vacation<br>10. Employees are adequately compensated | **Green** | C-100.10 Standards of Ethics and Business Conduct<br>C-310.25 Fraud Waste & Abuse<br>C-100.61 Integrity Hotline<br>C-240.40 Vacation |
| 1.Employees are not adequately trained to ensure acceptable behavior.<br>***Risk***<br>Reputational<br>Operational<br>Compliance | ***Likely*** | ***Serious*** | Human Resource | 1. New employee orientation<br>2. New Manager training<br>3. Education University<br>4. Awareness intranet publications<br>5. Annual Conflict of Interest disclosure<br>6. Annual formal performance evaluations | **Yellow** | C-270.25 Staff Development and Mandatory Training<br>C-270.30 Staff Orientation |

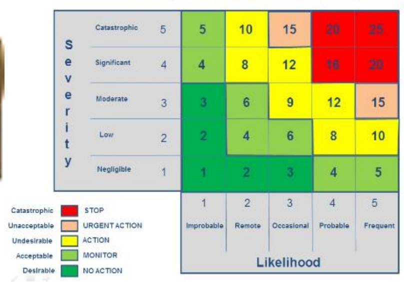
# Fraud Risk Register—GAPS

| Fraud Risk Scenario | Likelihood | Impact | Accountable Department | Existing Controls | Effectiveness of Controls | Policy & Procedures |
|---|---|---|---|---|---|---|
| | | | | | | |
| **Module #1** | | | | | | |
| **Employee Schemes** | | | | | | |
| | ***Increase*** | | | ***Control Gap***<br>Νο περιοδιχ τραινινγ ον Χοδε οφ Ετηιχσ φορ αλλ εμπλοψεεσ | **Red** | |
| | ***Increase*** | ***Increase*** | | ***Control Gap***<br>Νο ονγοινγ χριμιναλ ορ φινανχιαλ βαχκγρουνδ χηεχκσ περφορμεδ | **Red** | |
| | ***Increase*** | | | ***Control Gap***<br>Νο περιοδιχ τραινινγ ον φραυδ ωαστε ορ αβυσε φορ αλλ εμπλοψεεσ | **Red** | |

# What the Columns Mean

- **Identified Fraud Risks and Schemes**: This column should include a full list of the potential fraud risks and schemes that the organization may face.
- **Likelihood of Occurrence**: To design an efficient fraud risk management program, it is important to assess the likelihood of the identified fraud risk so that the organization can establish proper anti-fraud controls. These can be defined as rare, unlikely, possible, likely or almost certain.
- **Impact to the Organization**: Quantitative and qualitative factors should be considered when assessing the significance of fraud risk. These can be defined as Insignificant, minor serious disastrous or Catastrophic.
- **Accountable Department**: These are the individuals responsible for tailoring the controls to mitigate the risk and providing oversight for the effectiveness of the control.
- **Existing Controls**: These are the controls in place to mitigate the identified fraud risk.
- **Effectiveness of the Controls**: How well is the control working. Red yellow or green.
- **Policies and Procedures**: Formal written guidance approved and promulgated to the organization.

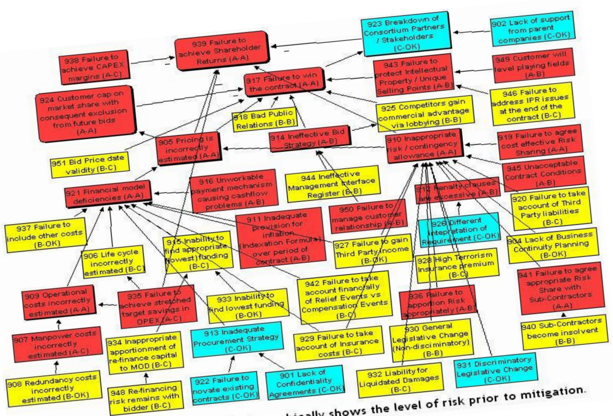
## Risk Rating = Likelihood x Severity



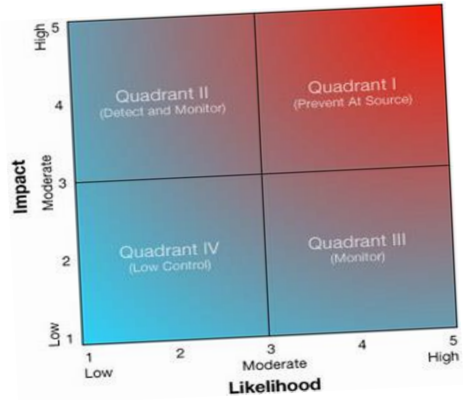
| Severity | | 1 Improbable | 2 Remote | 3 Occasional | 4 Probable | 5 Frequent |
|---|---|---|---|---|---|---|
| Catastrophic | 5 | 5 | 10 | 15 | 20 | 25 |
| Significant | 4 | 4 | 8 | 12 | 16 | 20 |
| Moderate | 3 | 3 | 6 | 9 | 12 | 15 |
| Low | 2 | 2 | 4 | 6 | 8 | 10 |
| Negligible | 1 | 1 | 2 | 3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

Likelihood

| | | |
|---|---|---|
| Catastrophic | 🟥 | STOP |
| Unacceptable | 🟧 | URGENT ACTION |
| Undesirable | 🟨 | ACTION |
| Acceptable | 🟩 | MONITOR |
| Desirable | 🟩 | NO ACTION |


939 Failure to achieve Shareholder Returns (A-A)
938 Failure to achieve CAPEX margins (A-C)
917 Failure to win the contract (A-A)
924 Customer cap on market share with consequent exclusion from future bids (A-A)
918 Bad Public Relations (B-B)
905 Pricing is incorrectly estimated (A-A)
914 Ineffective Bid Strategy (A-B)
951 Bid Price date validity (B-C)
921 Financial model deficiencies (A-A)
916 Unworkable payment mechanism causing cashflow problems (A-B)
944 Ineffective Management Interface Register (B-B)
937 Failure to include other costs (B-OK)
911 Inadequate prevision for inflation (Indexation Formula) over period of contract (A-B)
950 Failure to manage customer relationship (A-B)
906 Life cycle incorrectly estimated (B-C)
915 Inability to find appropriate (lowest) funding (B-C)
927 Failure to gain Third Party Income (B-OK)
909 Operational costs incorrectly estimated (A-A)
935 Failure to achieve stretched target savings in OPEX (A-C)
933 Inability to find lowest funding (B-OK)
942 Failure to take account financially of Relief Events vs Compensation Events (B-C)
907 Manpower costs incorrectly estimated (A-C)
934 Inappropriate apportionment of re-finance capital to MOD (B-C)
913 Inadequate Procurement Strategy (C-OK)
929 Failure to take account of Insurance costs (B-C)
908 Redundancy costs incorrectly estimated (B-OK)
948 Re-financing risk remains with bidder (B-C)
922 Failure to novate existing contracts (C-OK)
901 Lack of Confidentiality Agreements (C-OK)
923 Breakdown of Consortium Partners / Stakeholders (C-OK)
902 Lack of support from parent companies (C-OK)
943 Failure to protect Intellectual Property / Unique Selling Points (A-B)
949 Customer will level playing fields (A-B)
925 Competitors gain commercial advantage via lobbying (B-B)
946 Failure to address IPR issues at the end of the contract (B-C)
910 Inappropriate risk / contingency allowance (A-A)
919 Failure to agree cost effective Risk Sharing (A-A)
945 Unacceptable Contract Conditions (A-B)
912 Penalty clauses are excessive (A-B)
920 Failure to take account of Third Party liabilities (B-C)
926 Different intepretation of Requirement (C-OK)
904 Lack of Business Continuity Planning (B-OK)
928 High Terrorism Insurance premium (B-C)
941 Failure to agree appropriate Risk Share with Sub-Contractors (A-A)
936 Failure to apportion Risk appropriately (A-B)
930 General Legislative Change (Non-disciminatory) (B-B)
940 Sub-Contractors become insolvent (B-B)
932 Liability for Liquidated Damages (B-C)
931 Discriminatory Legislative Change (C-OK)

Example: "Current Risk Severity Map" graphically shows the level of risk prior to mitigation.



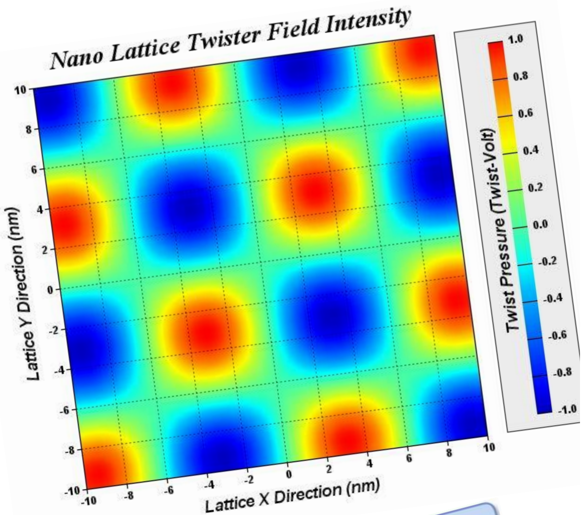
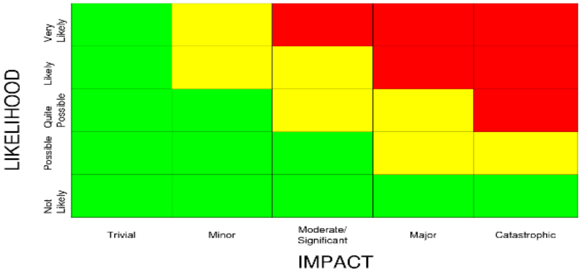
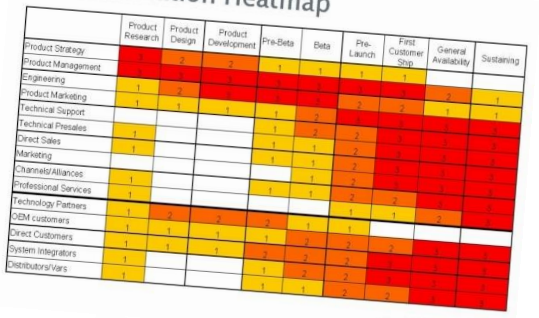


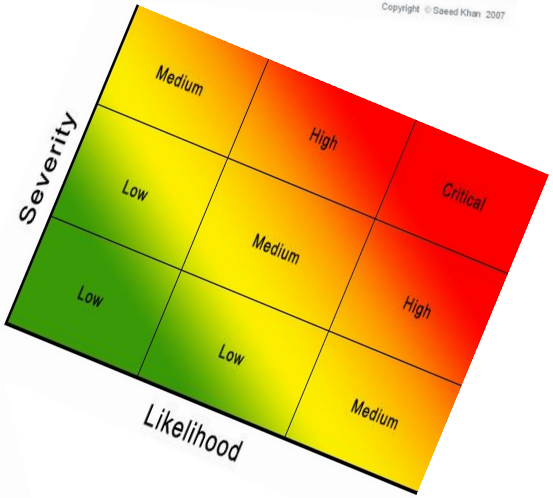
*CHART 3 – RISK MAPPING TEMPLATE*



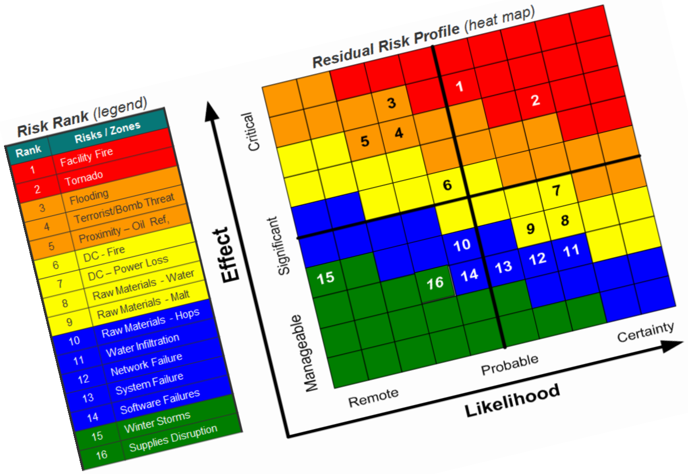
## Communication Heatmap



Copyright © Saeed Khan 2007



Reseller Sales Heat Map
Retail Mall
Retail Mall - $799,278
Fitness Toy Store
Top Sports Supply
Westside Plaza
Totes & Baskets Company
Health Sp a, Limited
Sheet Meta l Manufacturing
Closeou t Boutique
The Gear S tore
Larger Cycle Shop
Vigorous Exercise Company
Thorough Parts and Repair Services
Eastside D epartment Store
Metropo litan Bicycle Supply
Excellent Riding Supplies
Outdoor E quipment Store
Metropolit an Equipment
Modular Cycle Systems
Brakes and Gears
Corner Bicycle Supply
Latest Sports Equipment
First Bike Store
Great Bikes
Farthermost Bike Shop
Field Trip Store
Friendl y Bike Shop
Riders Company
Resale Services
Rewarding Activit ies Company
Golf an d Cycle Store
Registe red Cycle Store
Permane nt Finish Products
Reasonable Bicycl e Sales
Mail-Orde r Outlet
Mountain Bik e Center
eCommerce Bikes
Rural Cycle Empor ium
Original Bicycle Supply Company
Sturdy Toys
Bike Dealers Association
480,000
630,000
880,000
410,000
540,000
740,000



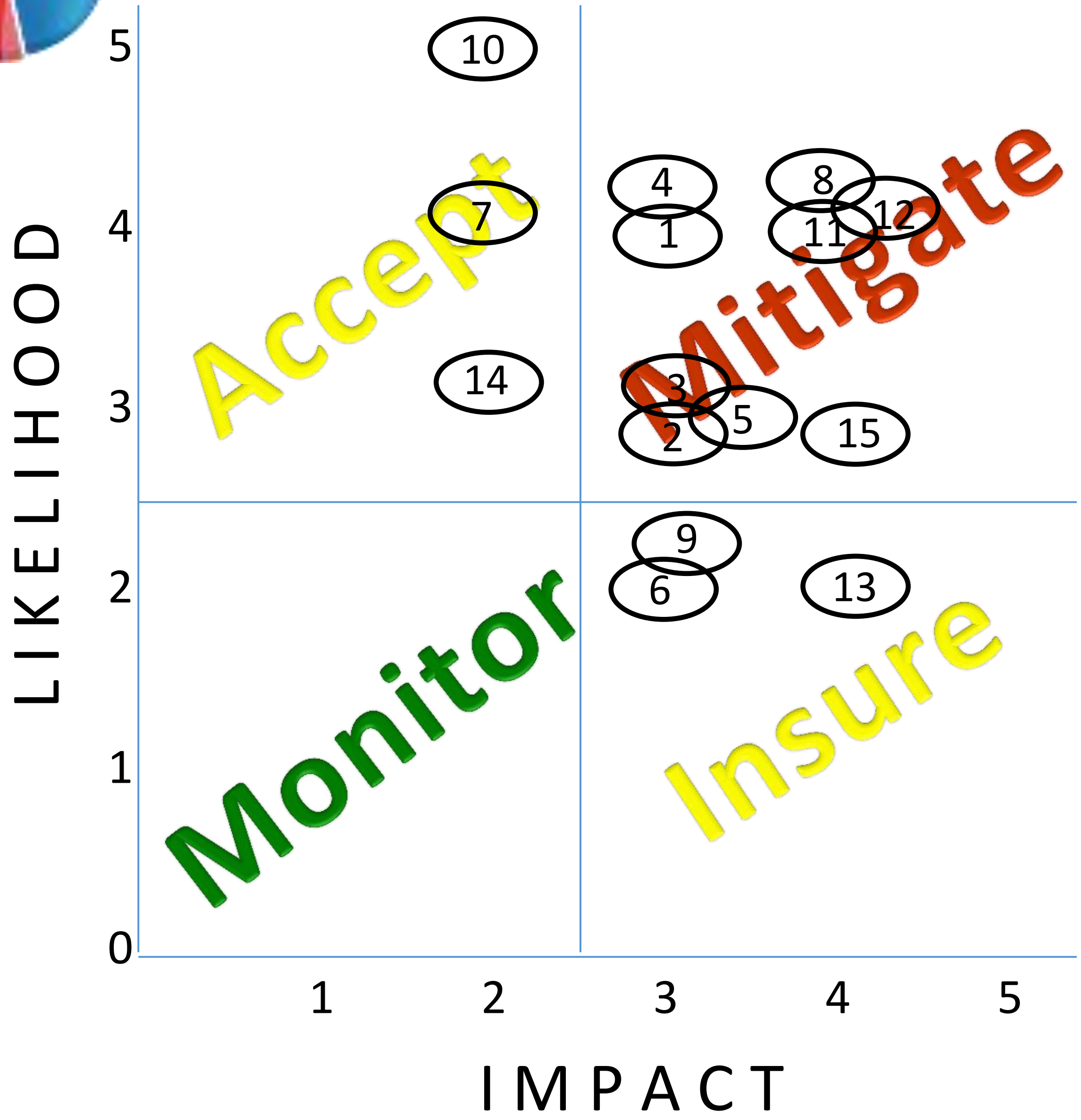
## Risk Rank (legend)

| Rank | Risks / Zones |
|---|---|
| 1 | Facility Fire |
| 2 | Tornado |
| 3 | Flooding |
| 4 | Terrorist/Bomb Threat |
| 5 | Proximity – Oil Ref. |
| 6 | DC - Fire |
| 7 | DC – Power Loss |
| 8 | Raw Materials - Water |
| 9 | Raw Materials - Malt |
| 10 | Raw Materials - Hops |
| 11 | Water Infiltration |
| 12 | Network Failure |
| 13 | System Failure |
| 14 | Software Failures |
| 15 | Winter Storms |
| 16 | Supplies Disruption |

# Heat Mapping

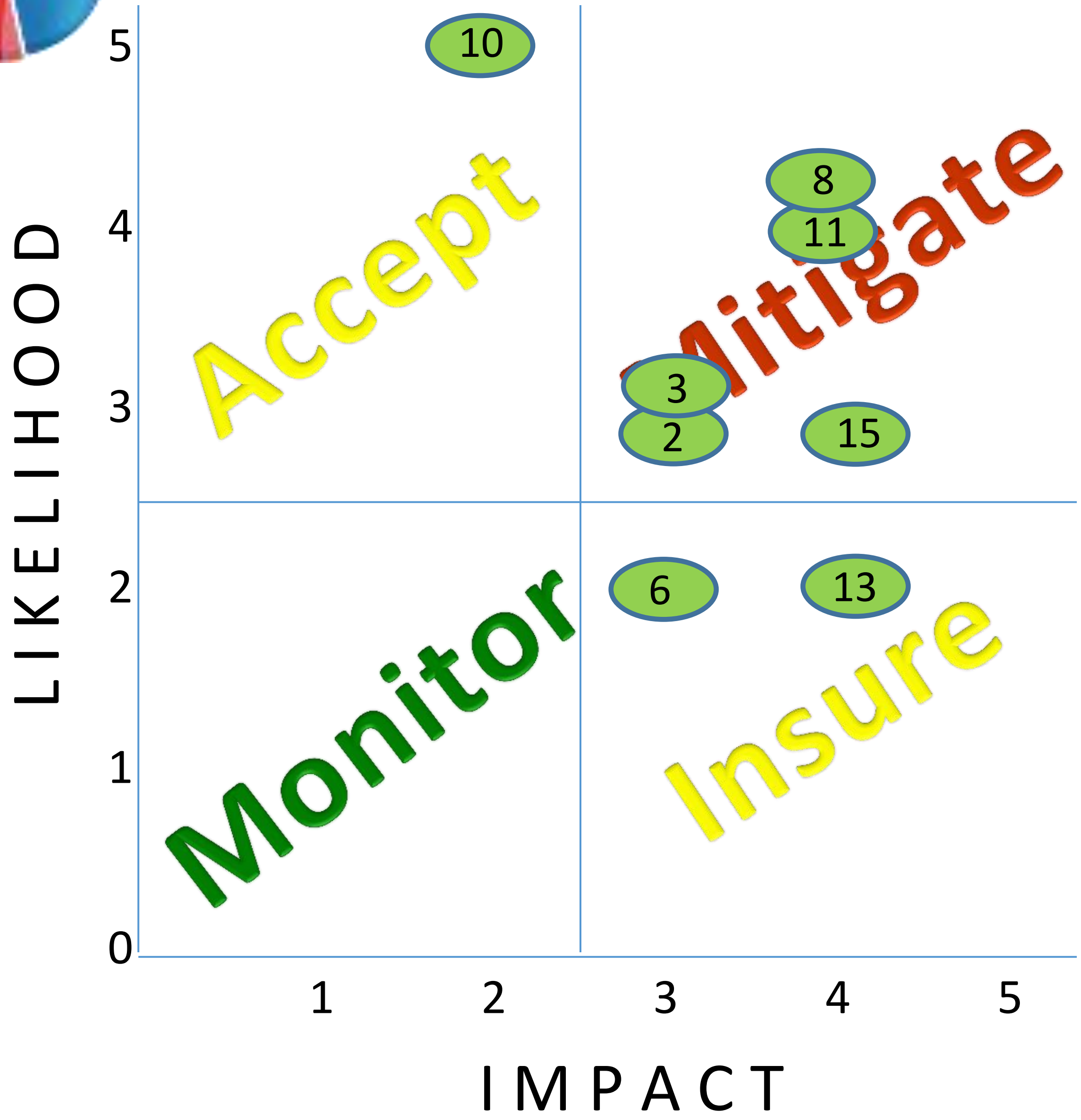
| | | | Likelihood | Impact |
|---|---|---|---|---|
| Module 1 | Employee Schemes | | | |
| | 1 | Scenario | 4 | 3 |
| | 2 | Scenario | 4 | 3 |
| | | | 4 | 3 |
| Module 2 | Management Override | | | |
| | 1 | Scenario | 2 | 3 |
| | 2 | Scenario | 3 | 3 |
| | 3 | Scenario | 3 | 2 |
| | | | 3 | 3 |
| Module 3 | Breaches of Physical Controls | | | |
| | 1 | Scenario | 2 | 2 |
| | 2 | Scenario | 3 | 3 |
| | | | 3 | 3 |
| Module 4 | Skimming | | | |
| | 1 | Scenario | 4 | 3 |
| | 2 | Scenario | 3 | 3 |
| | | | 4 | 3 |

# Fraud Risk Heat Map



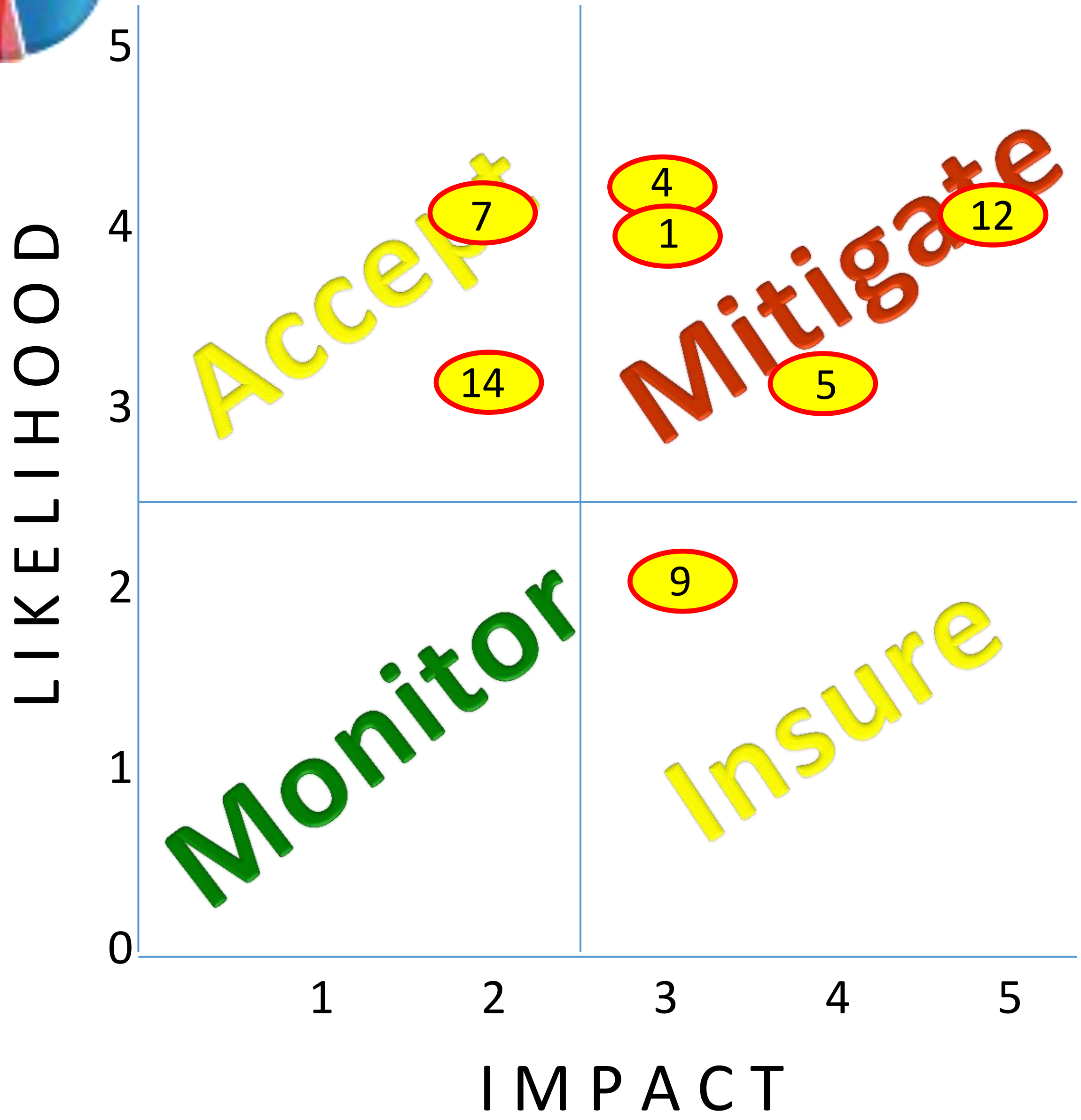
| Module | Scheme |
|---|---|
| **1** | Employee Schemes |
| **2** | Management Overrides |
| **3** | Breaches of Physical Controls |
| **4** | Skimming Schemes |
| **5** | Cash Larceny |
| **6** | Check Tampering |
| **7** | Cash Receipts |
| **8** | Purchasing Schemes |
| **9** | Payroll Schemes |
| **10** | Expense Schemes |
| **11** | Theft of Assets |
| **12** | Theft of Data |
| **13** | Corruption Schemes |
| **14** | Conflict of Interest |
| **15** | Fraudulent Financial Reporting |

# Adequately Mitigated Risk



| Module | Scheme |
|---|---|
| **2** | Management Overrides |
| **3** | Breaches of Physical Controls |
| **6** | Check Tampering |
| **8** | Purchasing Schemes |
| **10** | Expense Schemes |
| **11** | Theft of Assets |
| **13** | Corruption Schemes |
| **15** | Fraudulent Financial Reporting |

# High Residual Risk



| Module | Scheme |
|---|---|
| 1 | Employee Schemes |
| 4 | Skimming Schemes |
| 5 | Cash Larceny |
| 7 | Cash Receipts |
| 9 | Payroll Schemes |
| 12 | Theft of Data |
| 14 | Conflict of Interest |

# Gaps—Residual Risk

| Module | Scheme | Risk | GAP |
|---|---|---|---|
| ***Accept*** | | | |
| 7 | Cash Receipts | Yellow | ***Χαση ισ ινηερεντλψ ηιγη ρισκ *** |
| 14 | Conflict of Interest | Yellow | Νοτ αλλ χονφλιχτσ αρε ρεθυιρεδ το βε ρεπορτεδ |
| ***Insure*** | | | |
| 9 | Payroll Schemes | Yellow | 1. Μαναγεμεντ οϖερριδε ιν Δαψφορχε<br>2. Νο περιοδιχ ινδεπενδεντ ρεϖιεω |
| ***Mitigate*** | | | |
| 1 | Employee Schemes | Yellow | 1. Τραινινγ ον Χοδε, φραυδ ωαστε αβυσε<br>2. Χριμιναλ & Φινανχιαλ Βαχκγρουνδ χηεχκσ<br>3. Εμπλοψεεσ αρε νοτ βονδεδ |
| 3 | Breaches of Physical Controls | Green | Τραινινγ ον Χοδε |
| 4 | Skimming Schemes | Yellow | Στορεηουσε σιτεσ δο νοτ μακε δαιλψ δεποσιτσ |
| 5 | Cash Larceny | Yellow | Στορεηουσε σιτεσ δο νοτ μακε δαιλψ δεποσιτσ |
| 8 | Purchasing Schemes | Green | Περιοδιχ ρεϖιεω οφ νεω ϖενδορσ αδδεδ |
| 11 | Theft of Assets | Green | Νο προχεσσ το δετεχτ ινϖοιχε σπλιττινγ |
| 12 | Theft of Data | Yellow | 1. Τραινινγ ον δατα σεχυριτψ, χρεδιτ χαρδ δονορ ινφορματιον ετχ.<br>2. Νοτ αλλ σιγν α χονφιδεντιαλιτψ αγρεεμεντ |
| 15 | Fraudulent Financial Reporting | Green | Φιελδ ρεπορτινγ οφ ιρρεγυλαριτιεσ |

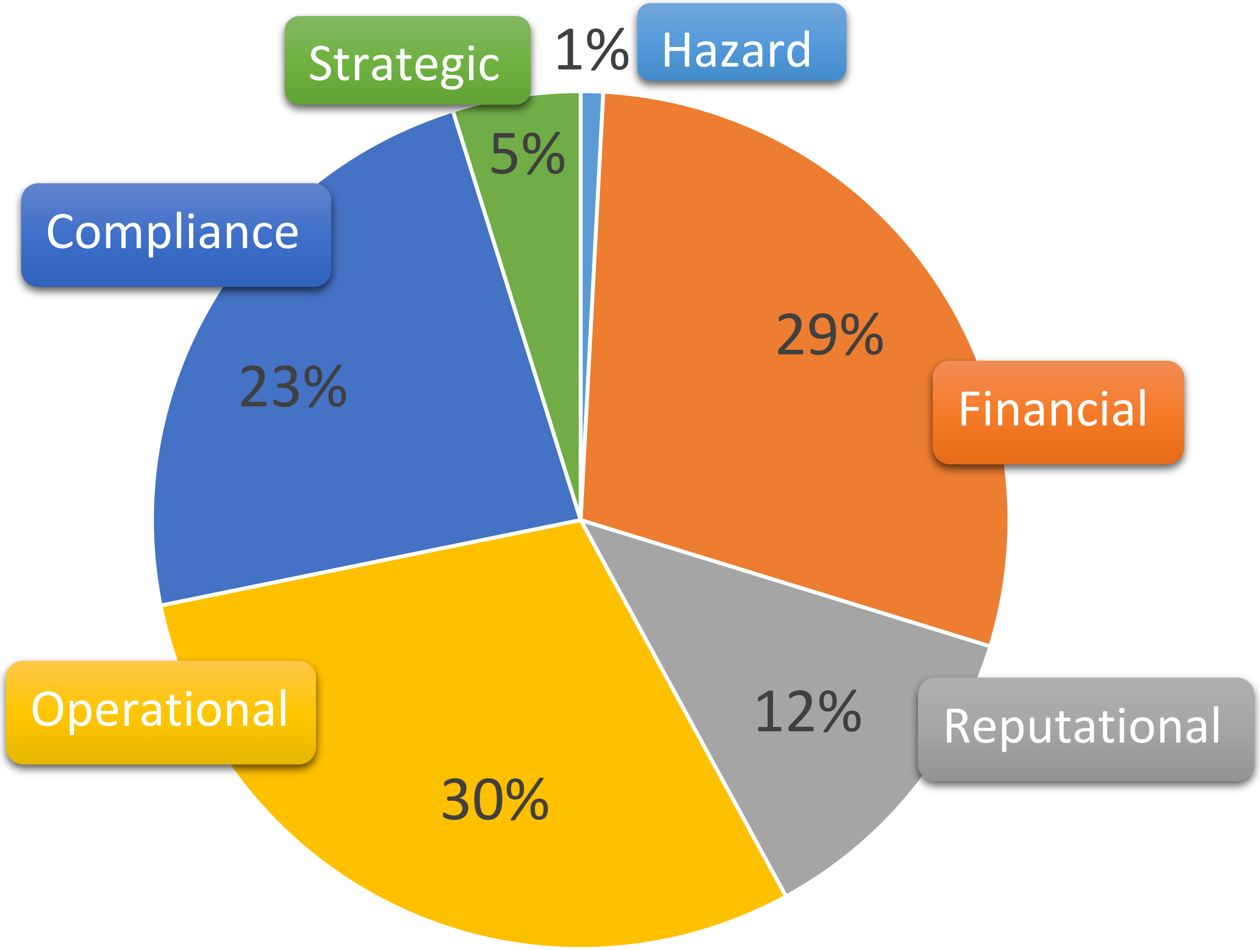
# Fraud Risk Register

| Fraud Risk Scenario | Likelihood | Impact | Accountable Department | Existing Controls | Effectiveness of Controls | Policy & Procedures |
|---|---|---|---|---|---|---|
| **Module #1** | | | | | | |
| **Employee Schemes** | | | | | | |
| 1.Employee's information used for hiring purposes is fraudulent increasing the risk of a bad hire.<br>***Risk***<br>Financial<br>Reputational<br>Operational<br>Compliance | ***Likely***<br>4 | ***Serious***<br>3 | Human Resource<br>Legal<br>Finance<br>7 | 1. Dedicate professional recruiters<br>2. Existence of formal written job descriptions<br>3. Code of Ethics<br>4. Written fraud policy<br>5. Written policies and procedures<br>6. Integrity Hotline<br>7. Background check required for hire<br>8. Internal Audit Department<br>9. Automated timekeeping system to monitor vacation<br>10. Employees are adequately compensated | **Green** | C-100.10 Standards of Ethics and Business Conduct<br>C-310.25 Fraud Waste & Abuse<br>C-100.61 Integrity Hotline<br>C-240.40 Vacation |
| 1.Employees are not adequately trained to ensure acceptable behavior.<br>***Risk***<br>Reputational<br>Operational<br>Compliance | ***Likely***<br>4 | ***Serious***<br>3 | Human Resource<br>7 | 1. New employee orientation<br>2. New Manager training<br>3. Education University<br>4. Awareness intranet publications<br>5. Annual Conflict of Interest disclosure<br>6. Annual formal performance evaluations | **Yellow** | C-270.25 Staff Development and Mandatory Training<br>C-270.30 Staff Orientation |

# What Is the Risk Profile?

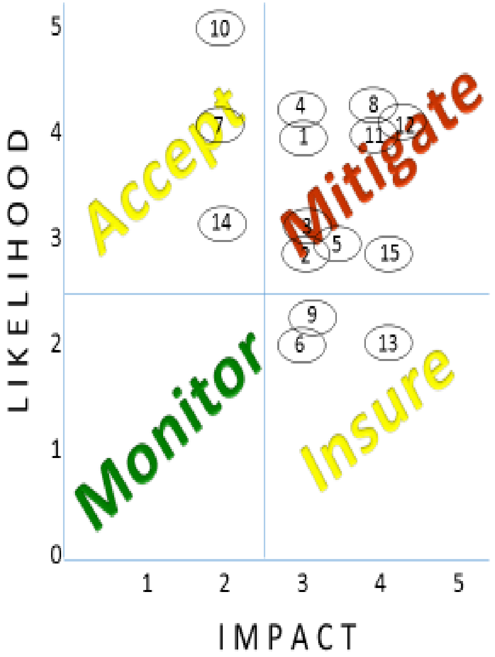
| Scenario | Hazard | Financial | Reputation | Operational | Compliance | Strategic | |
|---|---|---|---|---|---|---|---|
| 1 | | 7 | 7 | 7 | 7 | | |
| 2 | | | 7 | 7 | 7 | | |
| 3 | | 5 | | 5 | 5 | | |
| 4 | | 6 | 6 | 6 | 6 | 6 | |
| 5 | | 5 | 5 | 5 | 5 | 5 | |
| 38 | | 6 | | 6 | 6 | 6 | |
| 39 | | 5 | | 5 | 5 | 5 | |
| 40 | | 6 | | 6 | 6 | 6 | |
| | 7 | 240 | 102 | 247 | 194 | 40 | 830 |
| | 1% | 29% | 12% | 30% | 23% | 5% | 100% |

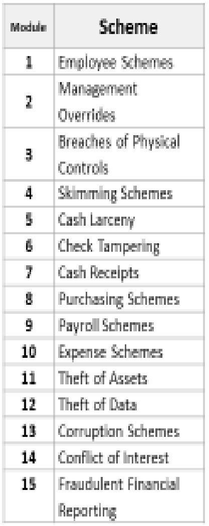
# Business Fraud Risk Profile



# What Are the Critical Controls?

## Fraud Risk Heat Map

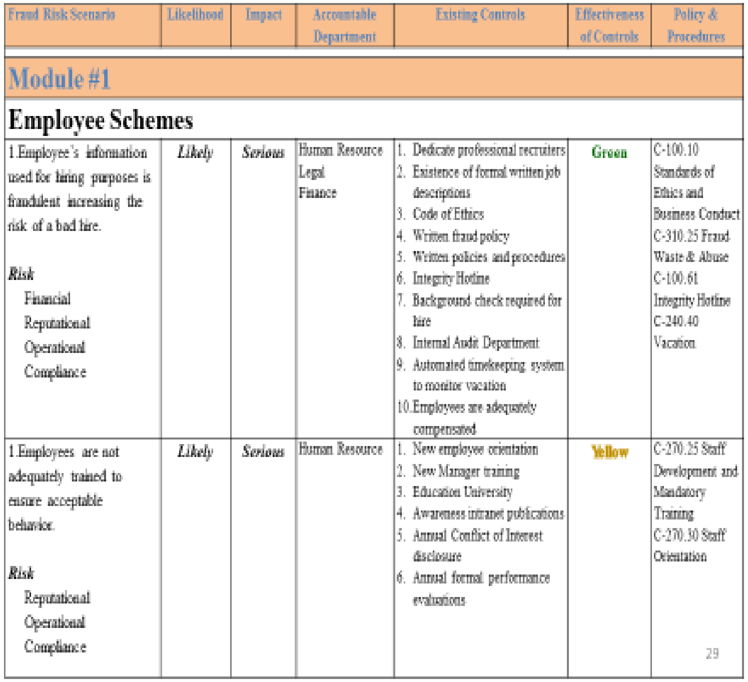




| Module | Scheme |
|---|---|
| 1 | Employee Schemes |
| 2 | Management Overrides |
| 3 | Breaches of Physical Controls |
| 4 | Skimming Schemes |
| 5 | Cash Larceny |
| 6 | Check Tampering |
| 7 | Cash Receipts |
| 8 | Purchasing Schemes |
| 9 | Payroll Schemes |
| 10 | Expense Schemes |
| 11 | Theft of Assets |
| 12 | Theft of Data |
| 13 | Corruption Schemes |
| 14 | Conflict of Interest |
| 15 | Fraudulent Financial Reporting |

34

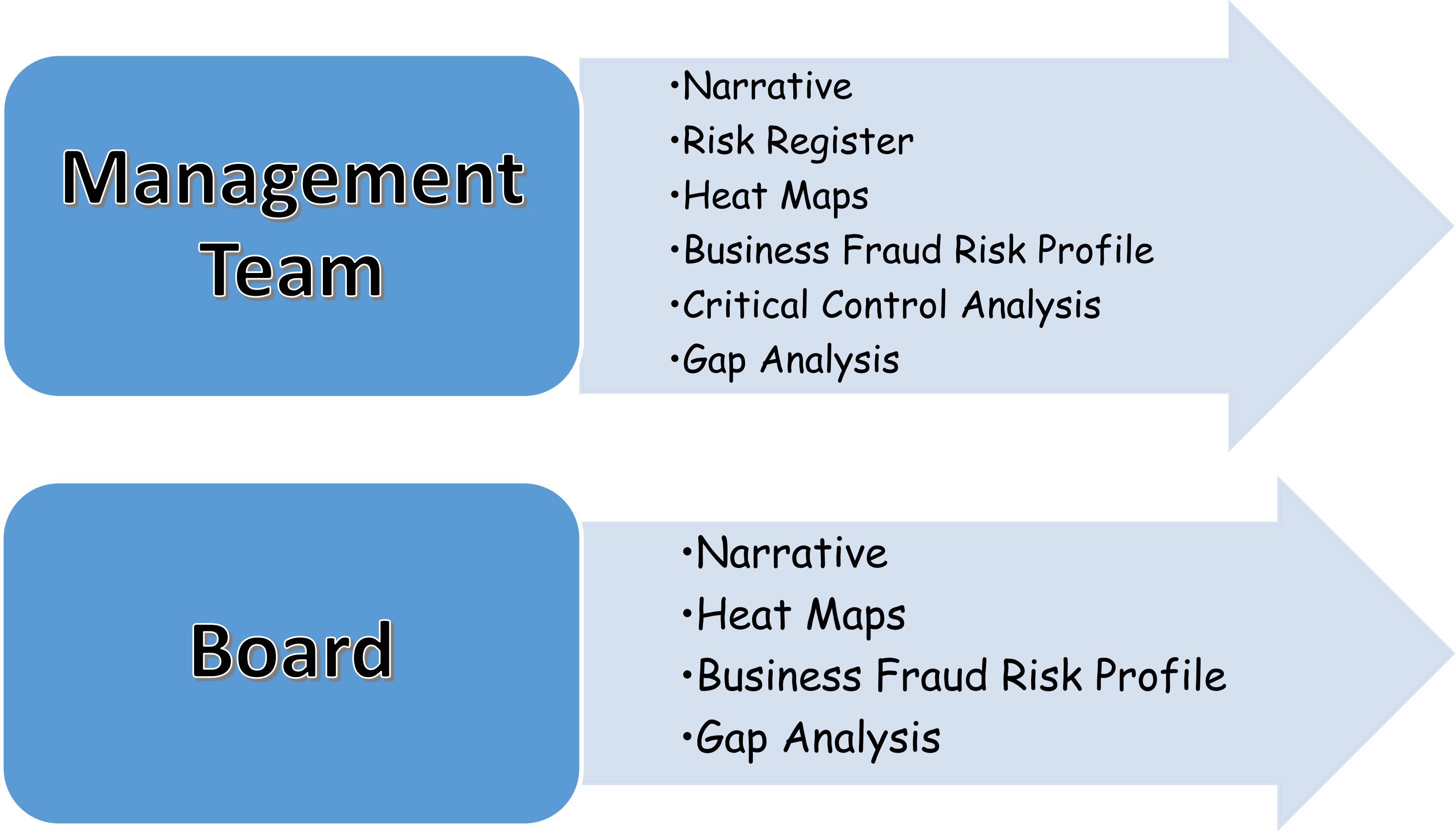
## Fraud Risk Assessment



| Fraud Risk Scenario | Likelihood | Impact | Accountable Department | Existing Controls | Effectiveness of Controls | Policy & Procedures |
|---|---|---|---|---|---|---|
| **Module #1** | | | | | | |
| **Employee Schemes** | | | | | | |
| 1.Employee's information used for hiring purposes is fraudulent increasing the risk of a bad hire.<br>*Risk*<br>Financial<br>Reputational<br>Operational<br>Compliance | *Likely* | *Serious* | Human Resource<br>Legal<br>Finance | 1. Dedicate professional recruiters<br>2. Existence of formal written job descriptions<br>3. Code of Ethics<br>4. Written fraud policy<br>5. Written policies and procedures<br>6. Integrity Hotline<br>7. Background check required for hire<br>8. Internal Audit Department<br>9. Automated timekeeping system to monitor vacation<br>10.Employees are adequately compensated | Green | C-100.10 Standards of Ethics and Business Conduct<br>C-310.25 Fraud Waste & Abuse<br>C-100.61 Integrity Hotline<br>C-240.40 Vacation |
| 1.Employees are not adequately trained to ensure acceptable behavior.<br>*Risk*<br>Reputational<br>Operational<br>Compliance | *Likely* | *Serious* | Human Resource | 1. New employee orientation<br>2. New Manager training<br>3. Education University<br>4. Awareness intranet publications<br>5. Annual Conflict of Interest disclosure<br>6. Annual formal performance evaluations | Yellow | C-270.25 Staff Development and Mandatory Training<br>C-270.30 Staff Orientation |

29

# Reporting—Who Got What



**Management Team**

- Narrative
- Risk Register
- Heat Maps
- Business Fraud Risk Profile
- Critical Control Analysis
- Gap Analysis

**Board**

- Narrative
- Heat Maps
- Business Fraud Risk Profile
- Gap Analysis

# In Summary—What We Did

- Used ACFE tools to find the boundaries of the control framework
- Created risk scenarios based on our environment
- Assessed likelihood and impact of the risk
- Aligned identified controls with relevant risk
- Assigned accountability for the control
- Considered the strengthen of the control to adequately mitigate the risk
- Identified gaps in the framework for consideration
- Communicated the results of the assessment

# How to Manage Fraud Risk Data

# You Completed a Fraud Risk Assessment: Now, What Do You Do with the Information?

Carol Morgan, CFE, CPA, CIA, CCEP, CISA, CGMA