



## Enterprise Risk Management – A Primer

Presented by  
Steven L. Blake CPA, CFE, CICA, CGMA

---

---

---

---

---

---

---

---



## Agenda

- 8:30 COSO Discussion
- 10:00 Break
- 10:10 ERM Discussion
- 11:45 Working Lunch
- 12:45 Audit Risk – Crawford Methodology
- 2:20 Break
- 2:30 Audit Risk & Class Handout and Exercise
- 4:30 Adjournment

---

---

---

---

---

---

---

---



## Thomas Jefferson

*“ . . . we might hope to see the finances of the Union as clear and intelligible as a merchant’s books, so that every member of Congress and every man of any mind in the Union should be able to comprehend them, to investigate abuses, and consequently to control them . . . ”*

---

---

---

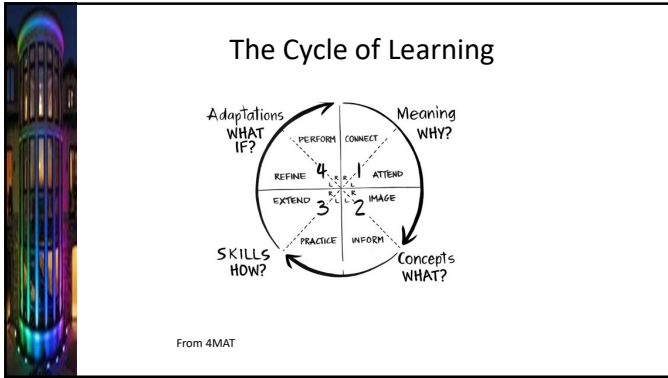
---

---

---

---

---




---

---

---

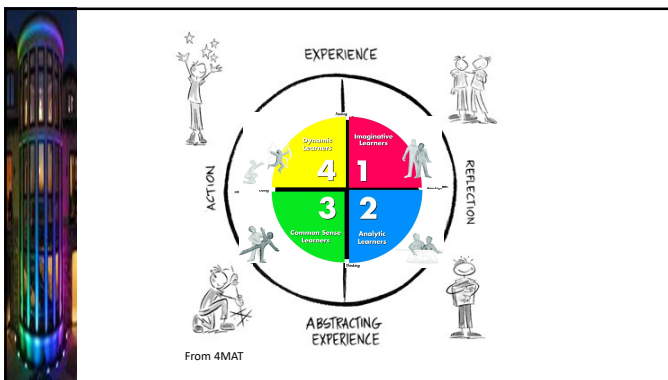
---

---

---

---

---




---

---

---

---

---

---

---

---

- ### Types of Intelligence
- Intellectual
  - Emotional
  - Physical
  - Social

---

---

---

---

---

---

---

---

### What is Risk Management?

- It is simply “living life”
- in an intentional way
- planning to accomplish
- a specific set of goals and objectives

---

---

---

---

---

---

---

---

### COSO

**COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance.**




---

---

---

---

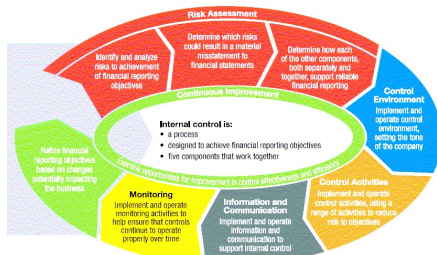
---

---

---

---

### Continuous Improvement Process




---

---

---

---

---

---

---

---

### COSO Internal Control Components

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

---

---

---

---

---

---

---

---

### Control Environment Principles

- **Integrity and Ethical Values**
- **Board of Directors**
- **Management's Philosophy and Operating Style**
- **Organizational Structure**
- **Financial Reporting Competencies**

---

---

---

---

---

---

---

---

### Control Environment Principles

- **Authority and Responsibility**
- **Human Resources**

---

---

---


---

---

---

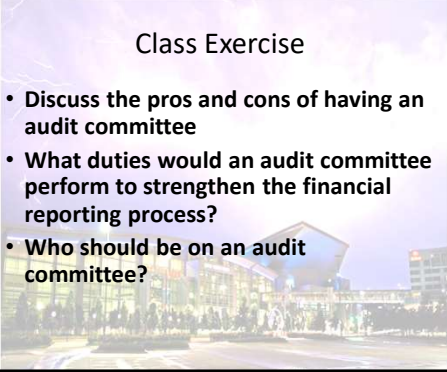
---

---



**Class Exercise**

- Discuss the pros and cons of having an audit committee
- What duties would an audit committee perform to strengthen the financial reporting process?
- Who should be on an audit committee?



---

---

---

---

---

---

---

---



**10 MINUTE BREAK**



---

---

---


---

---

---

---

---



**Risk Management Frameworks**

- COSO ERM Framework
- ACFE Fraud Risk Management
- ISO 31000 *Risk Management Principles and Guidelines*
- IT COBIT Framework

---

---

---

---

---

---

---

---

### COSO ERM Definition

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.

---

---

---

---

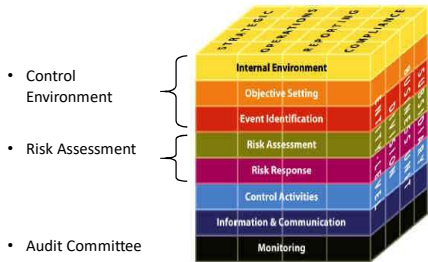
---

---

---

---

### COSO ERM Cube



---

---

---

---

---

---

---

---

### COSO ERM Risk Components

- **Financial Risk** – relating to the effectiveness of the company's financial reporting process
- **Strategic Risk** – relating to high level goals, aligned with and supporting the company's mission/vision
- **Operations Risk** – relating to the effectiveness and efficiency of the company's operations, including performance and profitability goals
- **Compliance Risk** – relating to the company's compliance with applicable laws and regulations

---

---

---

---

---

---

---

---



### Risk Management

- “Acts of God”
- Risk of Human Error = 100%
- Intentional, Planned Acts

---

---

---

---

---

---

---



### Benefits of ERM

- Avoid Surprises
- Better Governance
- Better Decision-making
- Efficiencies

---

---

---

---

---

---

---



### How Benefits Derived

- Link Goals, Growth and Risk with Resource Allocation in an Organized, Measureable Way
- Across the Entire Entity Focus [Risk Pervades Every Area, Department, Level]
- Coordinate, Define and Align Strategy(ies) with Risk, Risk Appetite and Risk Response

---

---

---

---

---

---

---



### Pressures for ERM

- GAO Comments on government being as good or better than those it regulates
- Agencies Board Members Becoming Increasingly Familiar with SOX Best-business Practices
- Response to Increasing Scrutiny and Criticism from the Stakeholders

---

---

---

---

---

---

---

---



### What ERM is not:

- It is not your risk assessment
- It is not about business continuity or business succession
- It is not about information security or employee/building insurance

---

---

---

---

---

---

---

---



### How do I Start?

**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.

---

---

---

---

---

---

---

---





### Risk Awareness

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

---

---

---

---

---

---

---

---



### Risk Appetite

- Can be Subjective
- Based on Cost Benefit
- Capability Maturity Model

---

---

---

---

---

---

---

---



### Capability Maturity Model

Capability Maturity Model – Integrated

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

---

---

---

---

---

---

---

---



### Levers of Control

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

---

---

---

---

---

---

---

---



### Belief System

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

---

---

---

---

---

---

---

---



### Boundary System

- Ethical limits beyond which behavior is prohibited

---

---

---

---

---

---

---

---



### Diagnostic System

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

---

---

---

---

---

---

---

---



### Interactive Control System

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

---

---

---

---

---

---

---

---



### ERM Risk Types

- Risks of Exposure: The Uncertainty of Future Events
- Risk as Uncertainty: For Known Events – all possible outcomes
- Risk as Opportunity: Inherent Concept in Risk/Reward

---

---

---

---

---

---

---

---



### What to do with Risk

- Identify,
- Quantify,
- Control

---

---

---

---

---

---

---

---



### What to do with Risk

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

---

---

---

---

---

---

---

---



### “Audit” Risks

- Risk of Exposure
- Risk of Incorrect Acceptance
- Risk of Incorrect Rejection
- Risk of an Incorrect Reporting Decision

---

---

---

---

---

---

---

---



### 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.
- Can be subjective and based on auditor judgment/experience/knowledge

---

---

---

---

---

---

---

---



### Control Risk

- Tests of Controls
  - Right Control for the Right Objective – Matching!
  - Attribute Based
  - “Stop and Go” Sampling [25/40/60]
- Reaction to test results ...
  - Empirical
  - Judgmental

---

---

---

---

---

---

---

---



### Detection Risk

- Test of Details Risk
  - All Substantive Procedure Based
  - Heavily Influenced by RMM Response
- Analytical and Other Procedures Risk
  - Also Substantive
  - Influenced by RRM and Test of Details

---

---

---

---

---

---

---

---




---

---

---

---

---

---

---

---

### Fraud Risk

- The risk/vulnerability an entity has to the possibility that someone in their organization is capable of overcoming the elements of the fraud diamond
- This risk differs from any other risk because by nature it is intentional misconduct designed to evade detection.

---

---

---

---

---

---

---

---

### Fraud Triangle

**EXHIBIT 2  
The Fraud Triangle**

**Pressure/Motivation**  
Pressure on employees to misappropriate cash or other organizational assets.

**Opportunity**  
Circumstances that allow an employee to carry out the misappropriation of cash or other organizational assets.

**Rationalization**  
A frame of mind or ethical character that allows employees to intentionally misappropriate cash or other organizational assets and justify their dishonest actions.

Source: Occupational Fraud Abuse, by Joseph T. Wells, CPA, CFE (Crestview Publishing Co., 1991)  
Fraud Examination, by W. Steve Albrecht (Thomson South-Western Publishing, 2005)

---

---

---

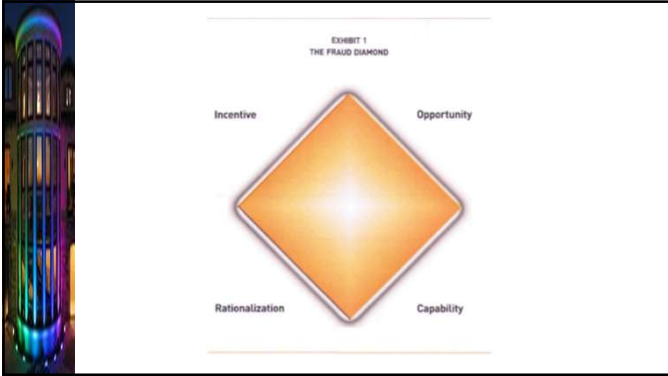
---

---

---

---

---



---

---

---

---

---

---

---



---

---

---

---

---

---

---

- 
- 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 (Consequence) and Probability values
  7. Construct the Risk Footprint

---

---


---

---

---

---

---



### 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

---

---

---


---

---

---

---

---



### 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

---

---

---


---

---

---

---

---



### 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

---

---

---

---


---

---

---

---





### 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

---

---

---

---

---


---

---

---

---

---



### 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

---

---

---

---

---


---

---

---

---

---



### Risk Ranking Characteristics

**Impact:** *Effect on achievement of goals & objectives*

- High - "showstopper"
- Medium - inefficient and extra work
- Low- no effect

**Probability:** *Likelihood of the risk happening*

- High- will happen frequently
- Medium- will happen infrequently
- Low- will seldom happen

---

---

---

---

---

---

---

---

---

---

### 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

31

---

---

---

---

---

---

---

---

### 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

32

---

---

---

---

---

---

---

---

### Levels of Control in COSO

Collaborative Assurance  
(Governance and Management Control Processes)

---

I-----I      ← Periodic Assurance →      I-----I  
(Governance Control Processes)

---

I----- On-going Assurance -----I  
(Management Control Processes)

Level 4 Controls (Internal Audit)	Level 1 Controls (Execution)	Level 2 Controls (Supervisory)	Level 3 Controls (Oversight)	Level 4 Controls (Internal Audit)
Pre-operations design review of on-going assurance	During execution of event or transaction	Immediately after execution of event or transaction	Soon after execution of event or transaction	Post-operations audit of execution of on-going assurance

---

---

---

---

---

---

---

---

## Probability Considerations

Assume only Level 1 Controls (Execution controls)

- Authorization
- Documentation
- Segregation of duties
- Budget

No Quality Controls (Level 2, Level 3 or Level 4)

---

---

---

---

---

---

---

---

---

---

## Transfer to and Sort Matrix

ACTIVITIES	1	2	3	4	5	6	7	8	9
Administration (13, 15, 18, 23)	Bad PR	Pause	Staff turnover	Lowest class action	Contractor goes bankrupt	Failure to comply with rules, regs, etc.	Ability to recruit qualified staff	Lack of performance by contractor	Operator budget overruns
Facility (5, 6, 7, 12, 19, 20, 21, 22)	Inadequate communications system	Inadequate signage	Unhealthy environment	Failure to comply with laws, regs	Poor building	Power failure	Inadequate building	Lack of sufficient storage	Death
Security & Safety (3, 4, 8, 11, 14, 16, 17)	Lack of trained security	Failure to comply with laws, regs	Fire & acts of nature	Equipment failure	Inadequate staff	Threat	Unhealthy or unhealthy environment	Injury or death	Lowest individual
Maintenance (1, 7, 9, 10)	Insecure facility	Unauthorized facility	Deferred maintenance	Equipment breakdown	Inadequate staff	Threat	Unhealthy or unhealthy environment	Injury or death	Lowest individual

---

---

---

---

---

---

---

---

---

---

## 7. Risk Footprint

ACTIVITIES	1	2	3	4	5	6	7	8	9
Administration (13, 15, 18, 23)	Bad PR	Pause	Staff turnover	Lowest class action	Contractor goes bankrupt	Failure to comply with rules, regs, etc.	Ability to recruit qualified staff	Lack of performance by contractor	Operator budget overruns
Facility (5, 6, 7, 12, 19, 20, 21, 22)	Inadequate communications system	Inadequate signage	Unhealthy environment	Failure to comply with laws, regs	Poor building	Power failure	Inadequate building	Lack of sufficient storage	Death
Security & Safety (3, 4, 8, 11, 14, 16, 17)	Lack of trained security	Failure to comply with laws, regs	Fire & acts of nature	Equipment failure	Inadequate staff	Threat	Unhealthy or unhealthy environment	Injury or death	Lowest individual
Maintenance (1, 7, 9, 10)	Insecure facility	Unauthorized facility	Deferred maintenance	Equipment breakdown	Inadequate staff	Threat	Unhealthy or unhealthy environment	Injury or death	Lowest individual

---

---

---

---

---

---

---

---

---

---



### Risk Footprint Usage

Management uses the footprint to allocate resources to managing risks that can affect the achievement of goals and objectives

Internal Audit uses the footprint to provide governance and executive management with appropriate level of assurance on all identified risks

---

---

---

---

---

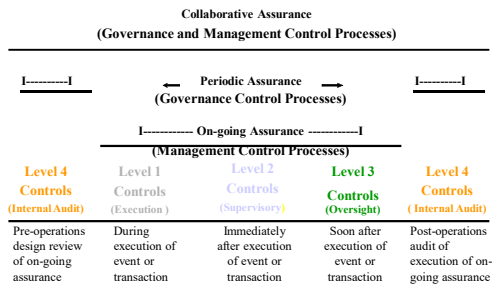
---

---

---



### Levels of Control in COSO




---

---

---

---

---

---

---

---



### 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

---

---

---

---

---

---

---

---



**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

---

---

---

---

---

---

---

---



**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

---

---

---

---

---

---

---

---



**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

---

---

---

---

---

---

---

---



### 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

---

---

---

---

---

---

---

---



### 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*

---

---

---

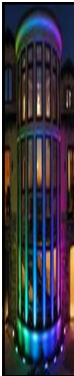
---

---

---

---

---



### 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

---

---

---

---

---

---

---

---

### Control Footprint

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

---

---

---

---

---

---

---

---

---

---

---

---

### Control Footprint Usage

Indicates

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

---

---

---

---

---

---

---

---

---

---

---

---

### Perform On-going Assessments

Indicate the evidence that would be generated for each of the color-coded controls

Monitor the color-coded controls on a random, on-going basis and record results in the appropriate columns

Monitor the other controls on an irregular basis to ensure that no employees get the feeling that their tasks will not be monitored

---

---

---

---

---

---

---

---

---

---

---

---

### Monitoring Footprint

Level	Maintenance (1, 7, 9, 10)	Personnel Quality (Un)trained, Safety	Equipment Maintenance	Equipment Condition	Availability of Staff	Availability of Resources	Priority of Work	Quality of Work	Evidence of Control	Date	Reviewer	Status
3	Mgr. Walkthrough	X	X	X	X	X	X	X				
1	Security check on staff ins & outs	X			X		X	X				
1	Preventive maintenance schedule	X	X	X	X		X	X	Preventive maintenance schedule			
2	Supervisor reviews completed maintenance	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	Last of equip. checked; Memo to file; Sign log on equip.			
1	Checklist of tasks	X					X	X				
2	Visual inspection by Supervisor	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			
3	Exception report to Mgr. About emp's not attended	X	X	X	X	X	X	X	Manager initials & dates with comments of actions taken.			

---

---

---

---

---

---

---

---

---

---

### 1. Identify Mission, Goals, & Objectives

The mission of accounts payable department is to:

Process vendor payments promptly for proper, authorized and verified purchases.

---

---

---

---

---

---

---

---

---

---

### 2. Brainstorm Activities

1		13
2		14
3		15
4		16
5		17
6		18
7		19
8		20
9		21
10		22
11		23
12		24

---

---

---

---

---

---

---

---

---

---



**3. Consolidate Activities into Processes and**  
**4. Prioritize**

CONSOLIDATED ACTIVITIES		PRIORITIZED CONSOLIDATED ACTIVITIES
	1	
	2	
	3	
	4	
	5	

---

---

---

---

---

---

---

---

**3. Consolidate Activities into Processes and**  
**4. Prioritize**

CONSOLIDATED ACTIVITIES		PRIORITIZED CONSOLIDATED ACTIVITIES
	1	
	2	
	3	
	4	
	5	

1	13
2	14
3	15
4	16
5	17
6	18
7	19
8	20
9	21
10	22
11	23
12	24

---

---

---

---

---

---

---

---

**Resources**

*Effective Compliance Systems: A Practical Guide for Educational Institutions* [Crawford, et al]  
[www.theiaa.org](http://www.theiaa.org)

[www.COSO.org](http://www.COSO.org)

---

*The Five Dysfunctions of a Team:* Patrick Lencioni

---

Email: [crawfordjd@earthlink.net](mailto:crawfordjd@earthlink.net)

---

---

---

---

---

---

---

---



### Link to you tube video

- `<div style="position:relative;height:0;padding-bottom:75.0%"><iframe src="https://www.youtube.com/embed/QgyiRWcZYS4?ecver=2" width="480" height="360" frameborder="0" style="position:absolute;width:100%;height:100%;left:0" allowfullscreen></iframe></div>`

---

---

---

---

---

---

---