SCHNEIDER DOWNS

2018 CENTRAL OHIO AGA - REGIONAL PROFESSIONAL DEVELOPMENT TRAINING

# Internal Controls: Complacency is Not an Option

Presenter: Donald R. Owens
October 30, 2018

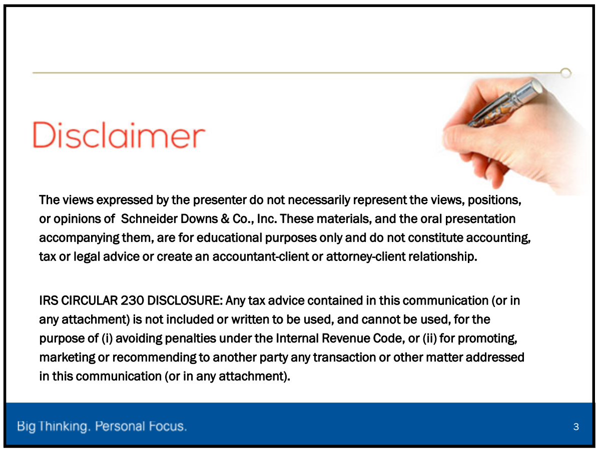
Big Thinking. Personal Focus.

## Presenter

Donald R. Owens
Shareholder
Risk Advisory Services
CPA, CITP, CFF, CIA, CFSA, CRMA, CBA

Schneider Downs & Co., Inc.
65 E. State Street, Suite 2000
Columbus, OH 43215
dowens@schneiderdowns.com
Work Phone: (614) 586-7257
Cell Phone: (614) 271-8551

Big Thinking. Personal Focus. 2

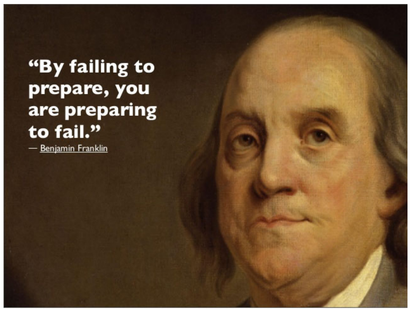


## Disclaimer

The views expressed by the presenter do not necessarily represent the views, positions, or opinions of Schneider Downs & Co., Inc. These materials, and the oral presentation accompanying them, are for educational purposes only and do not constitute accounting, tax or legal advice or create an accountant-client or attorney-client relationship.

IRS CIRCULAR 230 DISCLOSURE: Any tax advice contained in this communication (or in any attachment) is not included or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code, or (ii) for promoting, marketing or recommending to another party any transaction or other matter addressed in this communication (or in any attachment).

Big Thinking. Personal Focus. 3



“By failing to prepare, you are preparing to fail.”
— Benjamin Franklin

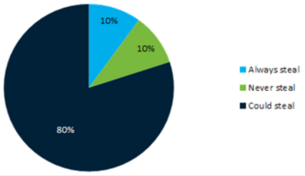
Friday, 31 October 14

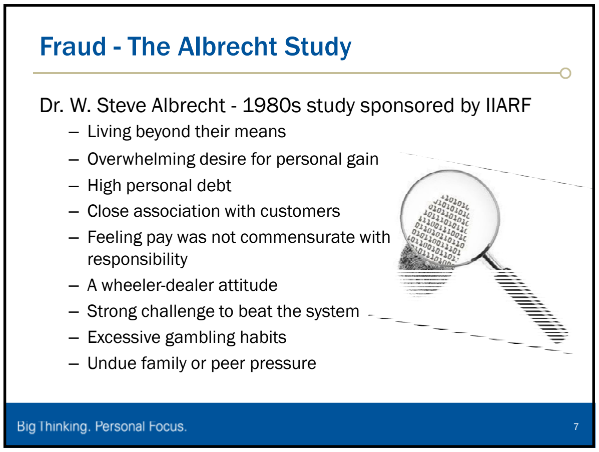
Safety Assurance

Don't worry, it'll be fine.
Trust me

## Human Nature is THE RISK

When thinking through risk and internal controls, consider the 10-10-80 Rule. This rule is based on the assumption that 10 percent of the people are ethical all the time, 10 percent are unethical all the time, and 80 percent *could behave unethically depending* on the situation.

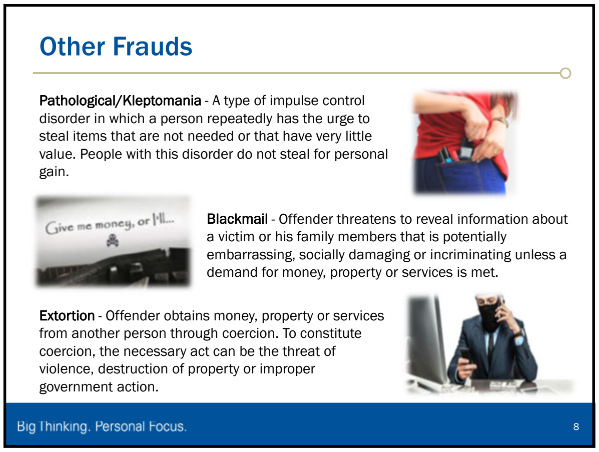




## Fraud - The Albrecht Study

Dr. W. Steve Albrecht - 1980s study sponsored by IIARF

- Living beyond their means
- Overwhelming desire for personal gain
- High personal debt
- Close association with customers
- Feeling pay was not commensurate with responsibility
- A wheeler-dealer attitude
- Strong challenge to beat the system
- Excessive gambling habits
- Undue family or peer pressure



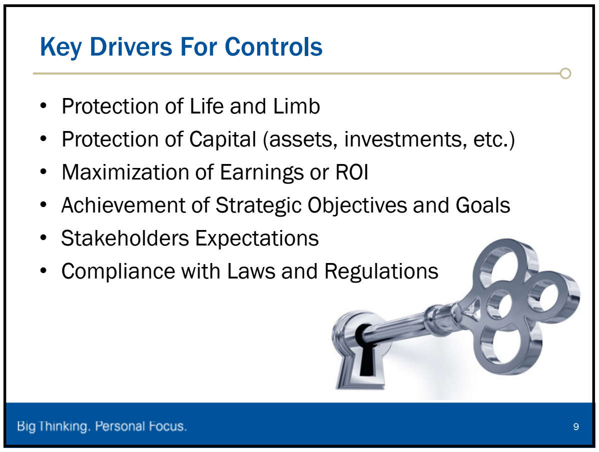
## Other Frauds

**Pathological/Kleptomania** - A type of impulse control disorder in which a person repeatedly has the urge to steal items that are not needed or that have very little value. People with this disorder do not steal for personal gain.

Give me money, or I'll...

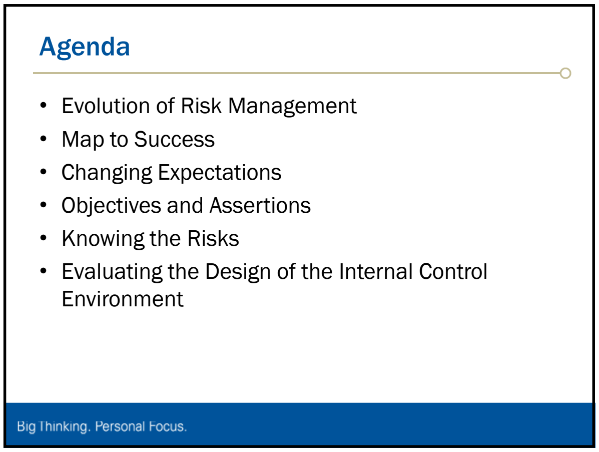
**Blackmail** - Offender threatens to reveal information about a victim or his family members that is potentially embarrassing, socially damaging or incriminating unless a demand for money, property or services is met.

**Extortion** - Offender obtains money, property or services from another person through coercion. To constitute coercion, the necessary act can be the threat of violence, destruction of property or improper government action.



## Key Drivers For Controls

- Protection of Life and Limb
- Protection of Capital (assets, investments, etc.)
- Maximization of Earnings or ROI
- Achievement of Strategic Objectives and Goals
- Stakeholders Expectations
- Compliance with Laws and Regulations



## Agenda

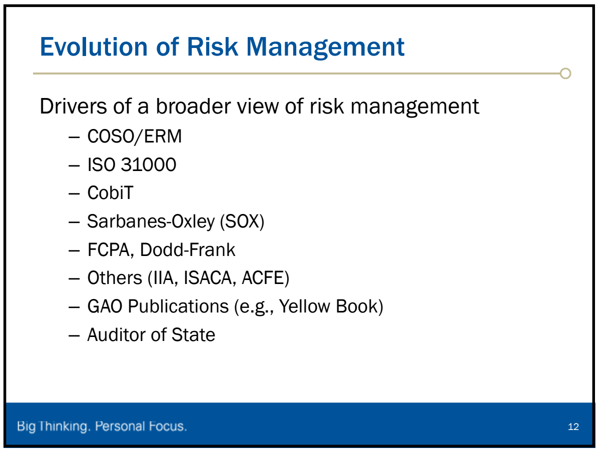
- Evolution of Risk Management
- Map to Success
- Changing Expectations
- Objectives and Assertions
- Knowing the Risks
- Evaluating the Design of the Internal Control Environment

Big Thinking. Personal Focus.

## Evolution of Risk Management

- Historical look - silo approach
  - External Audit - Financial
  - Internal Audit - Operational and Policy Compliance
  - Compliance - Regulatory
- Stagnant Rotating Control Assessments/Internal Audit Plans
  - Need to touch all functions
  - High emphasis on adherence with P & Ps
- No true aggregation of risks

Big Thinking. Personal Focus. 11



## Evolution of Risk Management

Drivers of a broader view of risk management

- COSO/ERM
- ISO 31000
- CobiT
- Sarbanes-Oxley (SOX)
- FCPA, Dodd-Frank
- Others (IIA, ISACA, ACFE)
- GAO Publications (e.g., Yellow Book)
- Auditor of State

Big Thinking. Personal Focus. 12

## Evolution of Risk Management

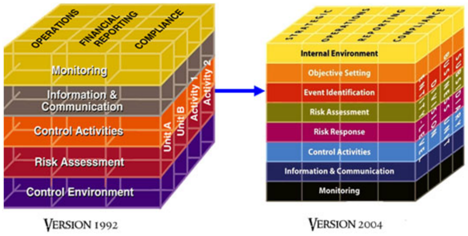
Inherent and residual risk measurements (establish measurements at the company level)

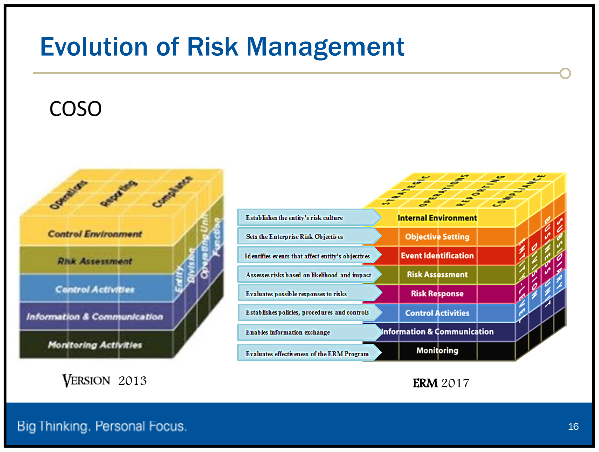
- Risk Acceptance (risks in the normal course of business)
- Risk Appetite (determined based on strategy/long-term business plan)
- Risk Tolerance (point at which potential impairment occurs, entering crisis mode)

## What is Your Risk Mitigation Plan?

## Evolution of Risk Management

COSO



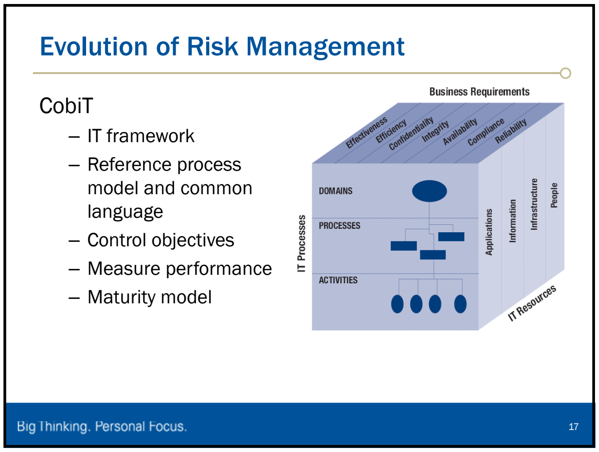


## Evolution of Risk Management

COSO

Operations
Reporting
Compliance
Control Environment
Risk Assessment
Control Activities
Information & Communication
Monitoring Activities
Entity
Division
Operating Unit
Function
VERSION 2013
STRATEGIC
OPERATIONS
REPORTING
COMPLIANCE
Establishes the entity's risk culture
Internal Environment
Sets the Enterprise Risk Objectives
Objective Setting
Identifies events that affect entity's objectives
Event Identification
Assesses risks based on likelihood and impact
Risk Assessment
Evaluates possible responses to risks
Risk Response
Establishes policies, procedures and controls
Control Activities
Enables information exchange
Information & Communication
Evaluates effectiveness of the ERM Program
Monitoring
ENTITY-LEVEL
DIVISION
BUSINESS UNIT
SUBSIDIARY
ERM 2017

Big Thinking. Personal Focus. 16

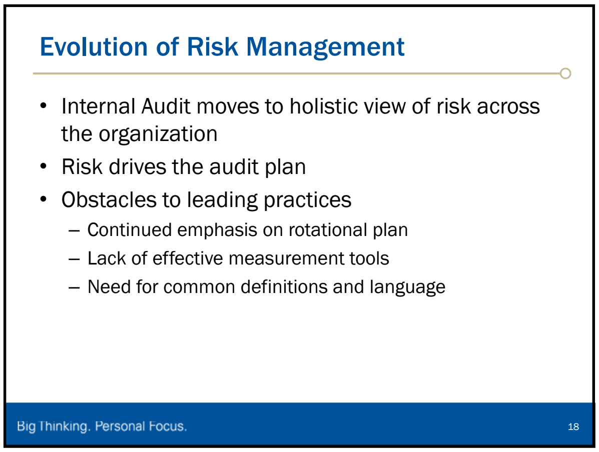


## Evolution of Risk Management

CobiT

- IT framework
- Reference process model and common language
- Control objectives
- Measure performance
- Maturity model

Big Thinking. Personal Focus. 17



## Evolution of Risk Management

- Internal Audit moves to holistic view of risk across the organization
- Risk drives the audit plan
- Obstacles to leading practices
  - Continued emphasis on rotational plan
  - Lack of effective measurement tools
  - Need for common definitions and language

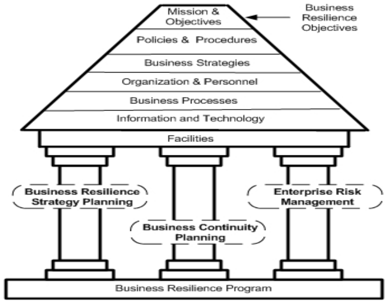
Big Thinking. Personal Focus. 18

## Evolution of Risk Management

Current Leading Practices

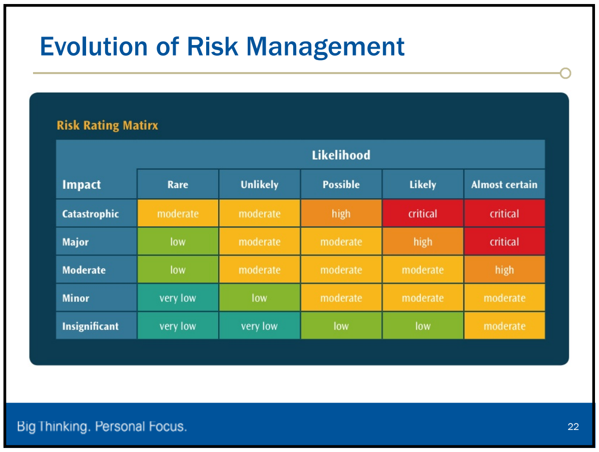
- Integration of risk management into the business functions
- Fully engaged executive management
- Risk ownership by key management
- Transparency
- Integration of risk with strategic planning
- Intelligence gathering (benchmarking, trend analysis)
- Continuous monitoring (data analytics)
- Scenario analysis (stress testing, disaster recovery)
- Advanced audit tools

## Evolution of Risk Management


Mission & Objectives
Business Resilience Objectives
Policies & Procedures
Business Strategies
Organization & Personnel
Business Processes
Information and Technology
Facilities
Business Resilience Strategy Planning
Enterprise Risk Management
Business Continuity Planning
Business Resilience Program

## Evolution of Risk Management

| SEVERITY | | |
|---|---|---|
| High | *Medium Risk*<br>***Share*** | *High Risk*<br>***Mitigate & Control*** |
| Low | *Low Risk*<br>***Accept*** | *Medium Risk*<br>***Control*** |
| | **PROBABILITY** | High |

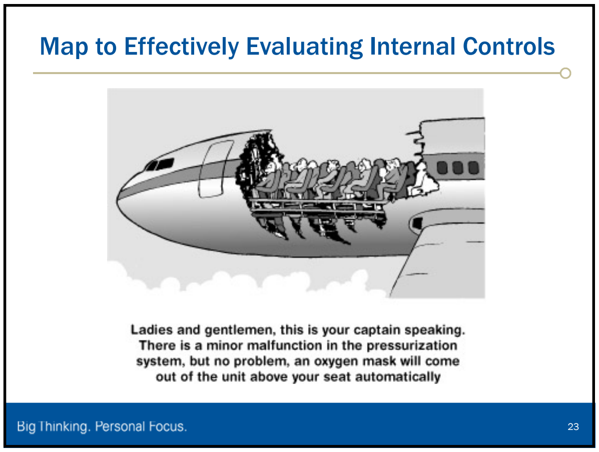


## Evolution of Risk Management

Risk Rating Matirx

| | Likelihood | | | | |
|---|---|---|---|---|---|
| Impact | Rare | Unlikely | Possible | Likely | Almost certain |
| Catastrophic | moderate | moderate | high | critical | critical |
| Major | low | moderate | moderate | high | critical |
| Moderate | low | moderate | moderate | moderate | high |
| Minor | very low | low | moderate | moderate | moderate |
| Insignificant | very low | very low | low | low | moderate |

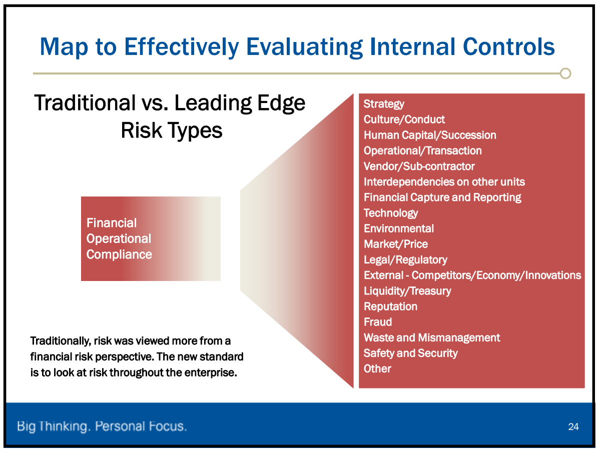
Big Thinking. Personal Focus. 22



## Map to Effectively Evaluating Internal Controls

Ladies and gentlemen, this is your captain speaking.
There is a minor malfunction in the pressurization
system, but no problem, an oxygen mask will come
out of the unit above your seat automatically

Big Thinking. Personal Focus. 23



## Map to Effectively Evaluating Internal Controls

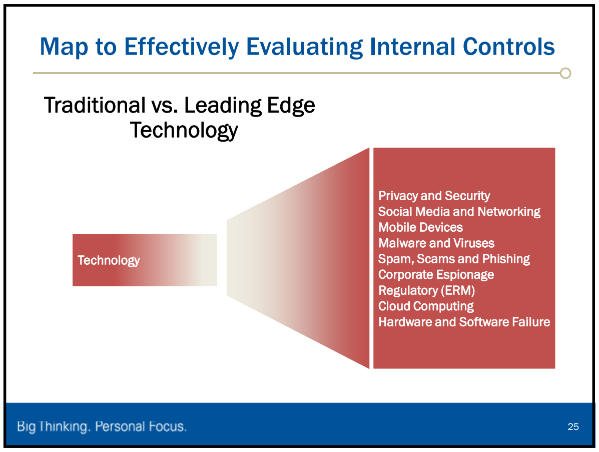
Traditional vs. Leading Edge Risk Types

Financial
Operational
Compliance

Strategy
Culture/Conduct
Human Capital/Succession
Operational/Transaction
Vendor/Sub-contractor
Interdependencies on other units
Financial Capture and Reporting
Technology
Environmental
Market/Price
Legal/Regulatory
External - Competitors/Economy/Innovations
Liquidity/Treasury
Reputation
Fraud
Waste and Mismanagement
Safety and Security
Other

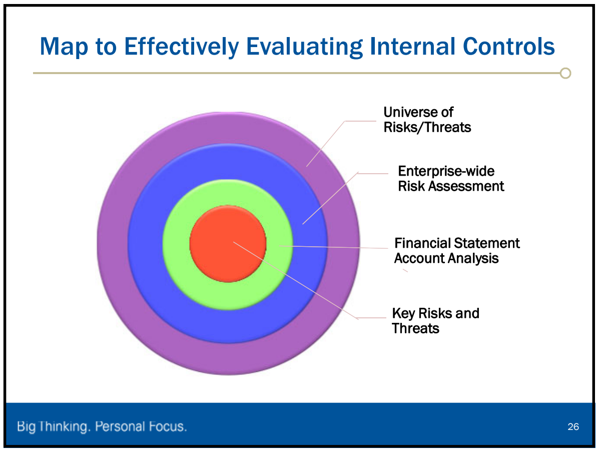
Traditionally, risk was viewed more from a financial risk perspective. The new standard is to look at risk throughout the enterprise.

Big Thinking. Personal Focus. 24



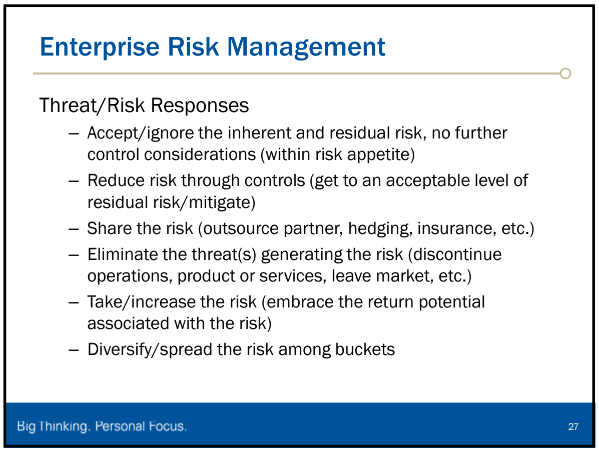
## Map to Effectively Evaluating Internal Controls

Traditional vs. Leading Edge Technology



## Map to Effectively Evaluating Internal Controls

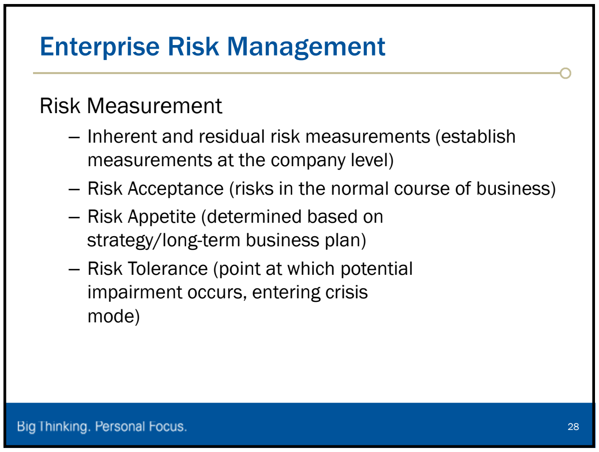
Universe of Risks/Threats
Enterprise-wide Risk Assessment
Financial Statement Account Analysis
Key Risks and Threats



## Enterprise Risk Management

Threat/Risk Responses

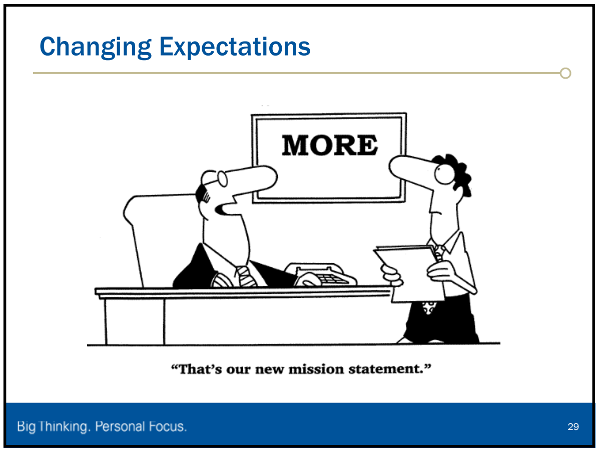
- Accept/ignore the inherent and residual risk, no further control considerations (within risk appetite)
- Reduce risk through controls (get to an acceptable level of residual risk/mitigate)
- Share the risk (outsource partner, hedging, insurance, etc.)
- Eliminate the threat(s) generating the risk (discontinue operations, product or services, leave market, etc.)
- Take/increase the risk (embrace the return potential associated with the risk)
- Diversify/spread the risk among buckets



## Enterprise Risk Management

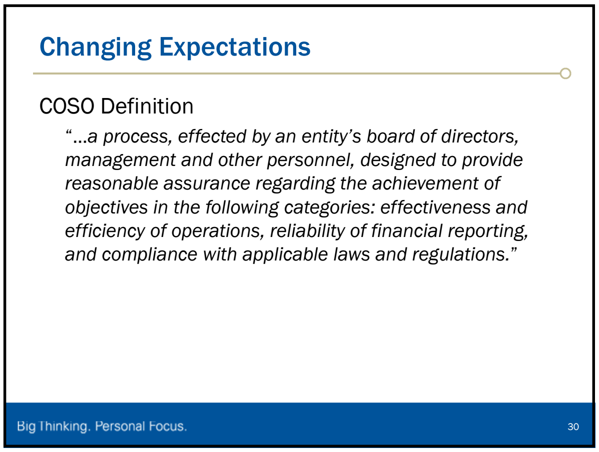
Risk Measurement

- Inherent and residual risk measurements (establish measurements at the company level)
- Risk Acceptance (risks in the normal course of business)
- Risk Appetite (determined based on strategy/long-term business plan)
- Risk Tolerance (point at which potential impairment occurs, entering crisis mode)



## Changing Expectations

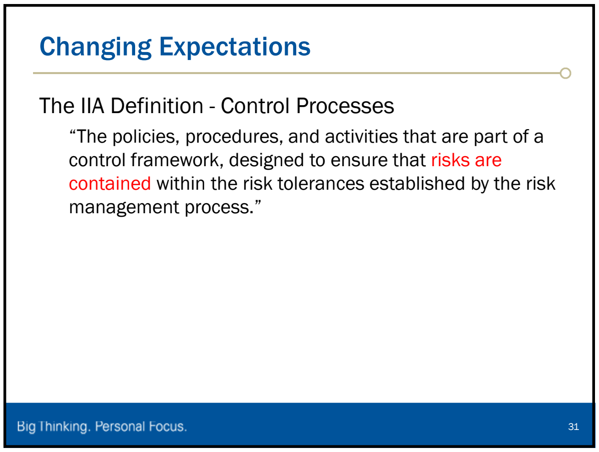
"That's our new mission statement."



## Changing Expectations

COSO 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 in the following categories: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations."*

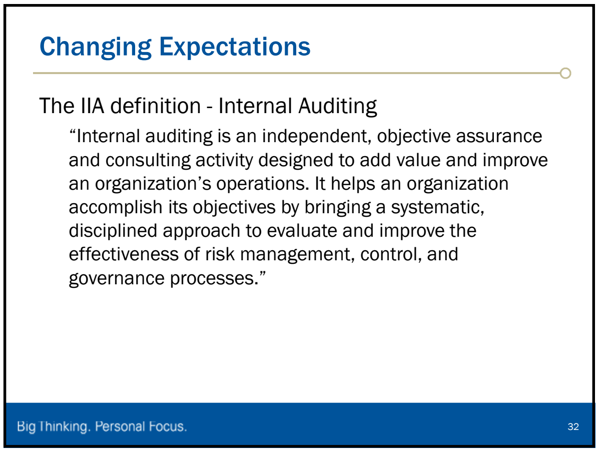


## Changing Expectations

The IIA Definition - Control Processes

> "The policies, procedures, and activities that are part of a control framework, designed to ensure that risks are contained within the risk tolerances established by the risk management process."

Big Thinking. Personal Focus. 31

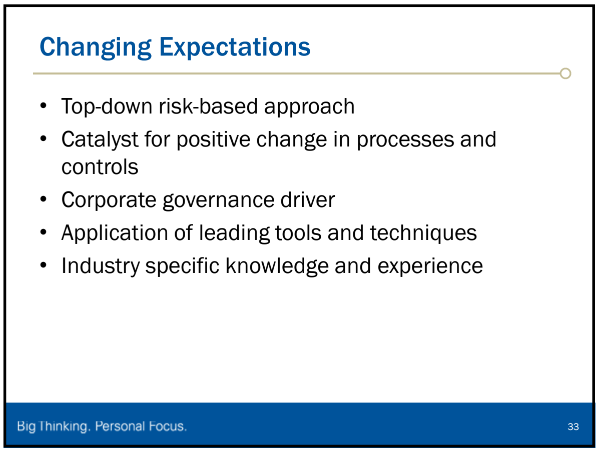


## Changing Expectations

The IIA definition - Internal Auditing

> "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."

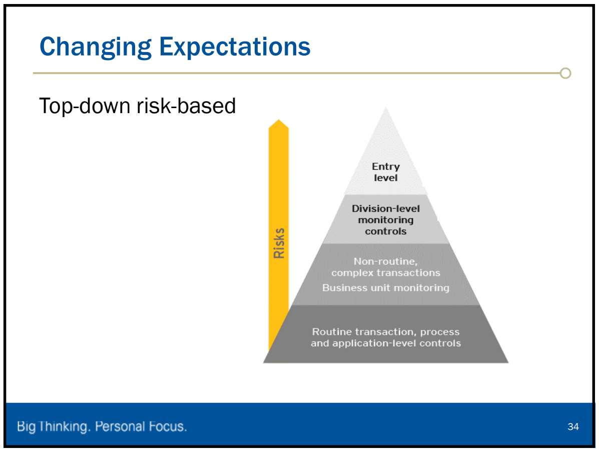
Big Thinking. Personal Focus. 32



## Changing Expectations

- Top-down risk-based approach
- Catalyst for positive change in processes and controls
- Corporate governance driver
- Application of leading tools and techniques
- Industry specific knowledge and experience

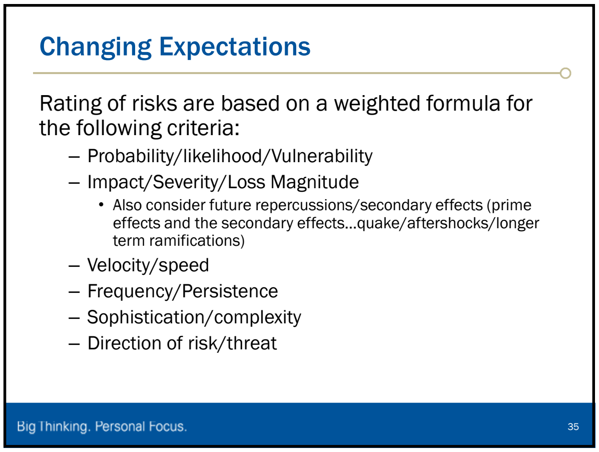
Big Thinking. Personal Focus. 33



## Changing Expectations

Top-down risk-based

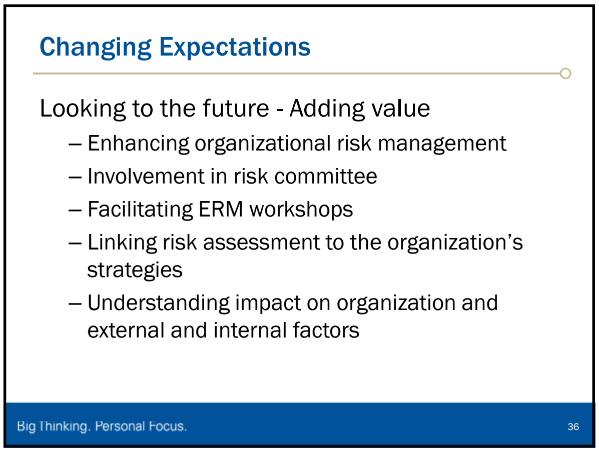
Risks
Entry level
Division-level monitoring controls
Non-routine, complex transactions
Business unit monitoring
Routine transaction, process and application-level controls



## Changing Expectations

Rating of risks are based on a weighted formula for the following criteria:

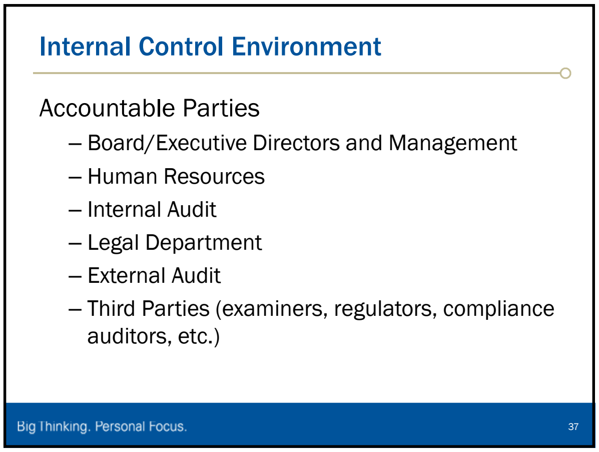
- Probability/likelihood/Vulnerability
- Impact/Severity/Loss Magnitude
  - Also consider future repercussions/secondary effects (prime effects and the secondary effects…quake/aftershocks/longer term ramifications)
- Velocity/speed
- Frequency/Persistence
- Sophistication/complexity
- Direction of risk/threat



## Changing Expectations

Looking to the future - Adding value

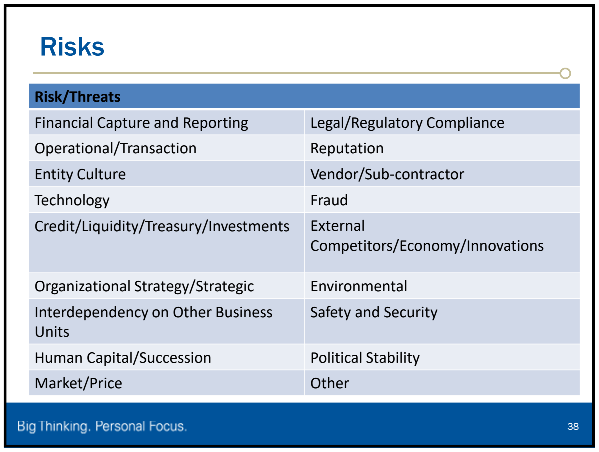
- Enhancing organizational risk management
- Involvement in risk committee
- Facilitating ERM workshops
- Linking risk assessment to the organization’s strategies
- Understanding impact on organization and external and internal factors



## Internal Control Environment

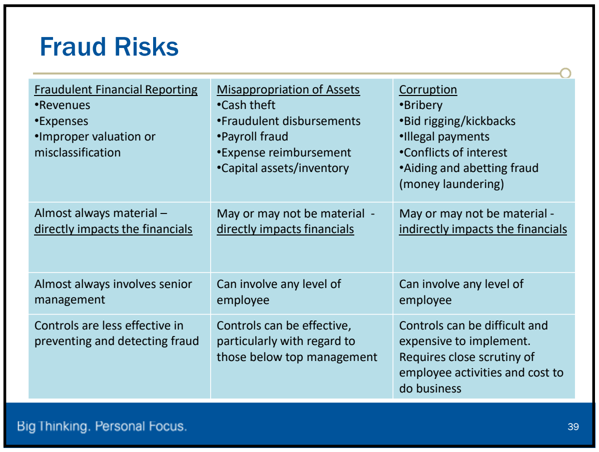
Accountable Parties

- Board/Executive Directors and Management
- Human Resources
- Internal Audit
- Legal Department
- External Audit
- Third Parties (examiners, regulators, compliance auditors, etc.)



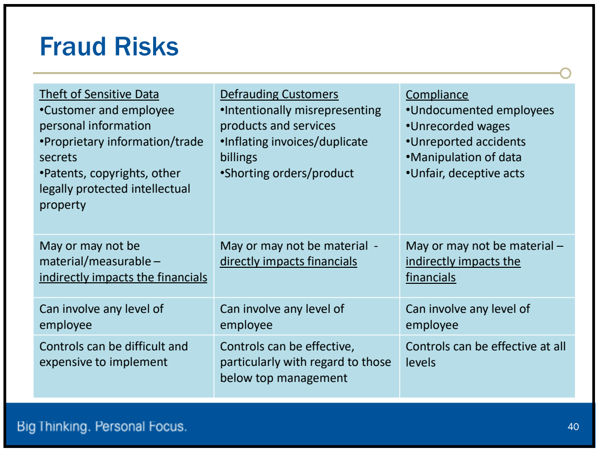
## Risks

| Risk/Threats | |
|---|---|
| Financial Capture and Reporting | Legal/Regulatory Compliance |
| Operational/Transaction | Reputation |
| Entity Culture | Vendor/Sub-contractor |
| Technology | Fraud |
| Credit/Liquidity/Treasury/Investments | External Competitors/Economy/Innovations |
| Organizational Strategy/Strategic | Environmental |
| Interdependency on Other Business Units | Safety and Security |
| Human Capital/Succession | Political Stability |
| Market/Price | Other |



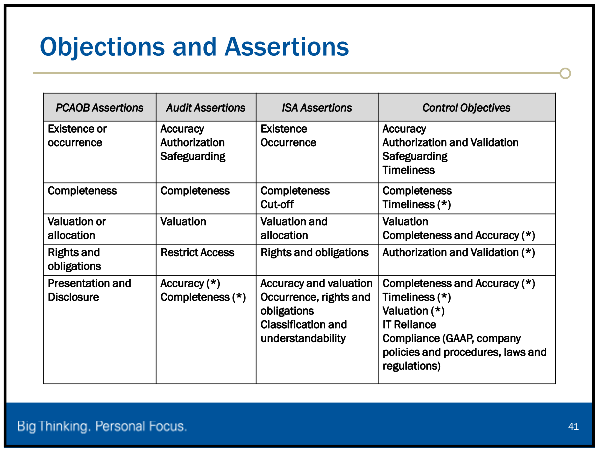
## Fraud Risks

| | | |
|---|---|---|
| Fraudulent Financial Reporting<br>•Revenues<br>•Expenses<br>•Improper valuation or misclassification | Misappropriation of Assets<br>•Cash theft<br>•Fraudulent disbursements<br>•Payroll fraud<br>•Expense reimbursement<br>•Capital assets/inventory | Corruption<br>•Bribery<br>•Bid rigging/kickbacks<br>•Illegal payments<br>•Conflicts of interest<br>•Aiding and abetting fraud (money laundering) |
| Almost always material – directly impacts the financials | May or may not be material - directly impacts financials | May or may not be material - indirectly impacts the financials |
| Almost always involves senior management | Can involve any level of employee | Can involve any level of employee |
| Controls are less effective in preventing and detecting fraud | Controls can be effective, particularly with regard to those below top management | Controls can be difficult and expensive to implement. Requires close scrutiny of employee activities and cost to do business |



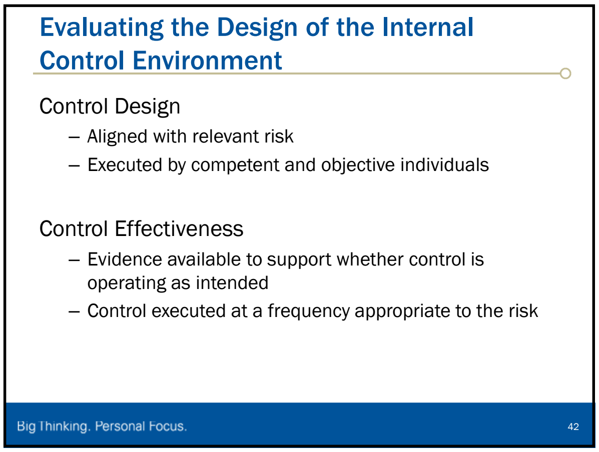
## Fraud Risks

| | | |
|---|---|---|
| Theft of Sensitive Data<br>•Customer and employee personal information<br>•Proprietary information/trade secrets<br>•Patents, copyrights, other legally protected intellectual property | Defrauding Customers<br>•Intentionally misrepresenting products and services<br>•Inflating invoices/duplicate billings<br>•Shorting orders/product | Compliance<br>•Undocumented employees<br>•Unrecorded wages<br>•Unreported accidents<br>•Manipulation of data<br>•Unfair, deceptive acts |
| May or may not be material/measurable – indirectly impacts the financials | May or may not be material - directly impacts financials | May or may not be material – indirectly impacts the financials |
| Can involve any level of employee | Can involve any level of employee | Can involve any level of employee |
| Controls can be difficult and expensive to implement | Controls can be effective, particularly with regard to those below top management | Controls can be effective at all levels |



## Objections and Assertions

| *PCAOB Assertions* | *Audit Assertions* | *ISA Assertions* | *Control Objectives* |
|---|---|---|---|
| Existence or occurrence | Accuracy<br>Authorization<br>Safeguarding | Existence<br>Occurrence | Accuracy<br>Authorization and Validation<br>Safeguarding<br>Timeliness |
| Completeness | Completeness | Completeness<br>Cut-off | Completeness<br>Timeliness (*) |
| Valuation or allocation | Valuation | Valuation and allocation | Valuation<br>Completeness and Accuracy (*) |
| Rights and obligations | Restrict Access | Rights and obligations | Authorization and Validation (*) |
| Presentation and Disclosure | Accuracy (*)<br>Completeness (*) | Accuracy and valuation<br>Occurrence, rights and obligations<br>Classification and understandability | Completeness and Accuracy (*)<br>Timeliness (*)<br>Valuation (*)<br>IT Reliance<br>Compliance (GAAP, company policies and procedures, laws and regulations) |



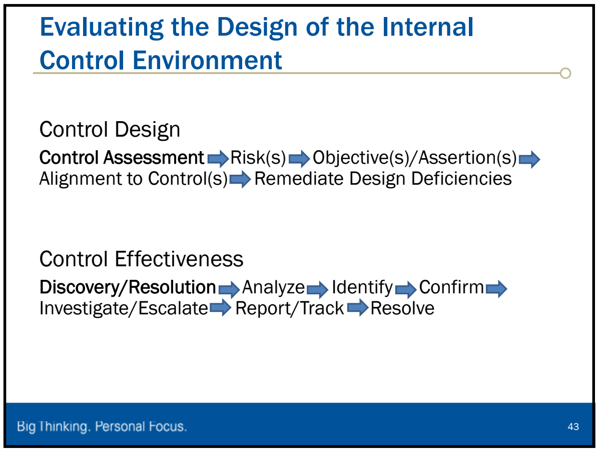
## Evaluating the Design of the Internal Control Environment

Control Design

- Aligned with relevant risk
- Executed by competent and objective individuals

Control Effectiveness

- Evidence available to support whether control is operating as intended
- Control executed at a frequency appropriate to the risk



## Evaluating the Design of the Internal Control Environment

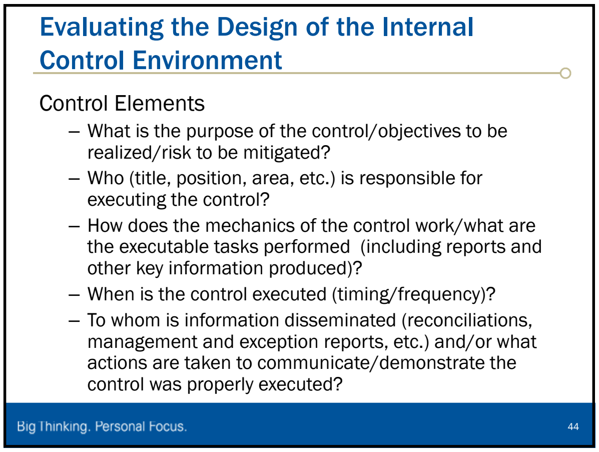
Control Design

**Control Assessment** → Risk(s) → Objective(s)/Assertion(s) → Alignment to Control(s) → Remediate Design Deficiencies

Control Effectiveness

**Discovery/Resolution** → Analyze → Identify → Confirm → Investigate/Escalate → Report/Track → Resolve

Big Thinking. Personal Focus. 43

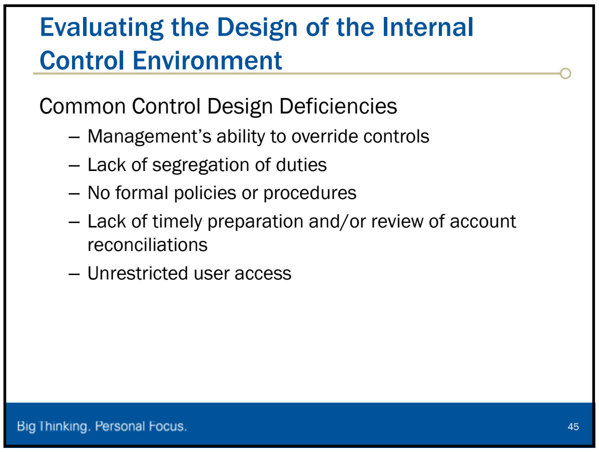


## Evaluating the Design of the Internal Control Environment

Control Elements

- What is the purpose of the control/objectives to be realized/risk to be mitigated?
- Who (title, position, area, etc.) is responsible for executing the control?
- How does the mechanics of the control work/what are the executable tasks performed  (including reports and other key information produced)?
- When is the control executed (timing/frequency)?
- To whom is information disseminated (reconciliations, management and exception reports, etc.) and/or what actions are taken to communicate/demonstrate the control was properly executed?

Big Thinking. Personal Focus. 44

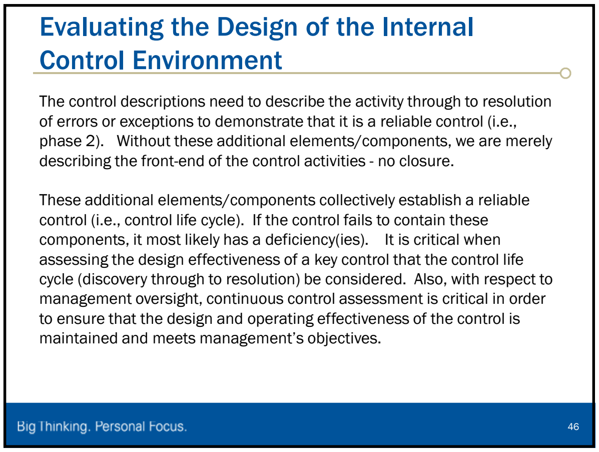


## Evaluating the Design of the Internal Control Environment

Common Control Design Deficiencies

- Management's ability to override controls
- Lack of segregation of duties
- No formal policies or procedures
- Lack of timely preparation and/or review of account reconciliations
- Unrestricted user access

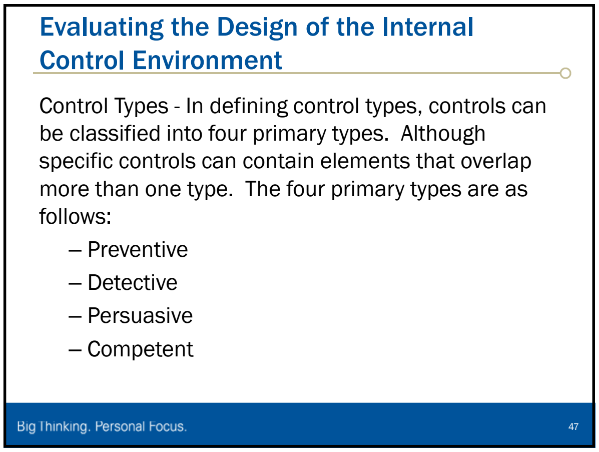
Big Thinking. Personal Focus. 45



## Evaluating the Design of the Internal Control Environment

The control descriptions need to describe the activity through to resolution of errors or exceptions to demonstrate that it is a reliable control (i.e., phase 2). Without these additional elements/components, we are merely describing the front-end of the control activities - no closure.

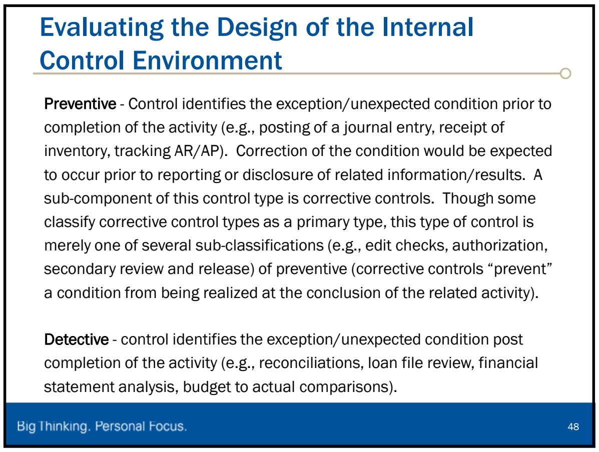
These additional elements/components collectively establish a reliable control (i.e., control life cycle). If the control fails to contain these components, it most likely has a deficiency(ies). It is critical when assessing the design effectiveness of a key control that the control life cycle (discovery through to resolution) be considered. Also, with respect to management oversight, continuous control assessment is critical in order to ensure that the design and operating effectiveness of the control is maintained and meets management's objectives.



## Evaluating the Design of the Internal Control Environment

Control Types - In defining control types, controls can be classified into four primary types. Although specific controls can contain elements that overlap more than one type. The four primary types are as follows:

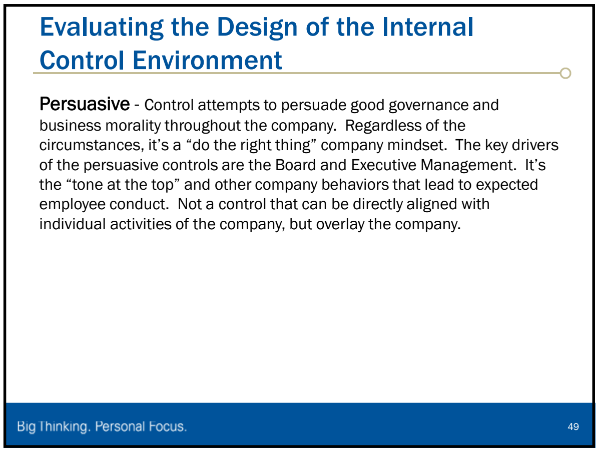
- Preventive
- Detective
- Persuasive
- Competent



## Evaluating the Design of the Internal Control Environment

**Preventive** - Control identifies the exception/unexpected condition prior to completion of the activity (e.g., posting of a journal entry, receipt of inventory, tracking AR/AP). Correction of the condition would be expected to occur prior to reporting or disclosure of related information/results. A sub-component of this control type is corrective controls. Though some classify corrective control types as a primary type, this type of control is merely one of several sub-classifications (e.g., edit checks, authorization, secondary review and release) of preventive (corrective controls "prevent" a condition from being realized at the conclusion of the related activity).

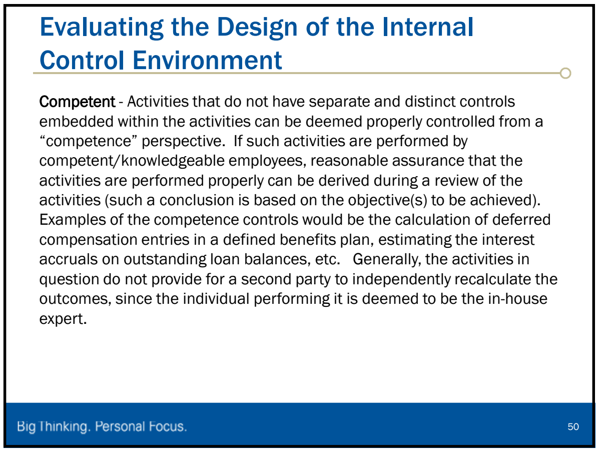
**Detective** - control identifies the exception/unexpected condition post completion of the activity (e.g., reconciliations, loan file review, financial statement analysis, budget to actual comparisons).



## Evaluating the Design of the Internal Control Environment

**Persuasive** - Control attempts to persuade good governance and business morality throughout the company. Regardless of the circumstances, it's a "do the right thing" company mindset. The key drivers of the persuasive controls are the Board and Executive Management. It's the "tone at the top" and other company behaviors that lead to expected employee conduct. Not a control that can be directly aligned with individual activities of the company, but overlay the company.

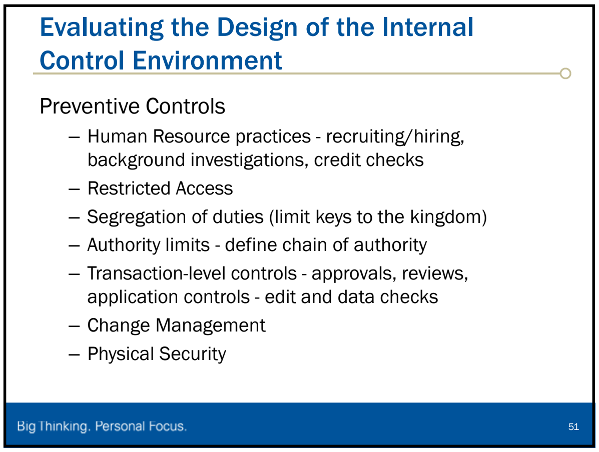
Big Thinking. Personal Focus. 49



## Evaluating the Design of the Internal Control Environment

**Competent** - Activities that do not have separate and distinct controls embedded within the activities can be deemed properly controlled from a "competence" perspective. If such activities are performed by competent/knowledgeable employees, reasonable assurance that the activities are performed properly can be derived during a review of the activities (such a conclusion is based on the objective(s) to be achieved). Examples of the competence controls would be the calculation of deferred compensation entries in a defined benefits plan, estimating the interest accruals on outstanding loan balances, etc. Generally, the activities in question do not provide for a second party to independently recalculate the outcomes, since the individual performing it is deemed to be the in-house expert.

Big Thinking. Personal Focus. 50

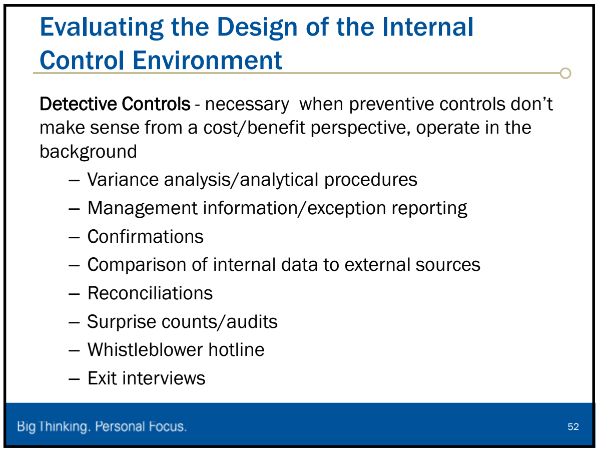


## Evaluating the Design of the Internal Control Environment

Preventive Controls

- Human Resource practices - recruiting/hiring, background investigations, credit checks
- Restricted Access
- Segregation of duties (limit keys to the kingdom)
- Authority limits - define chain of authority
- Transaction-level controls - approvals, reviews, application controls - edit and data checks
- Change Management
- Physical Security

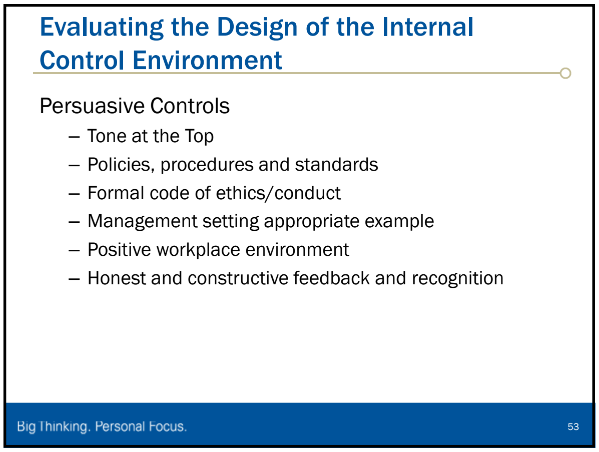
Big Thinking. Personal Focus. 51



## Evaluating the Design of the Internal Control Environment

**Detective Controls** - necessary  when preventive controls don't make sense from a cost/benefit perspective, operate in the background

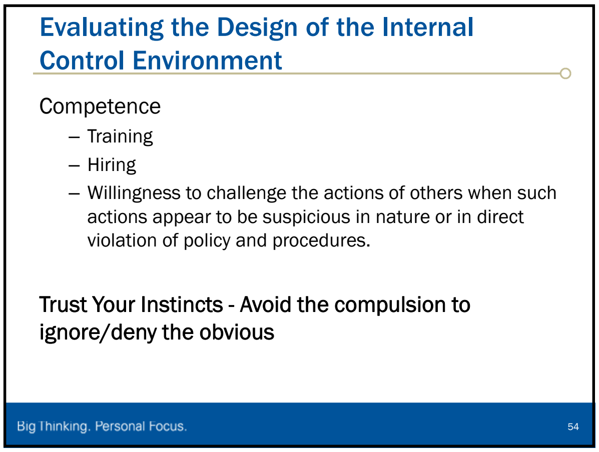
- Variance analysis/analytical procedures
- Management information/exception reporting
- Confirmations
- Comparison of internal data to external sources
- Reconciliations
- Surprise counts/audits
- Whistleblower hotline
- Exit interviews



## Evaluating the Design of the Internal Control Environment

Persuasive Controls

- Tone at the Top
- Policies, procedures and standards
- Formal code of ethics/conduct
- Management setting appropriate example
- Positive workplace environment
- Honest and constructive feedback and recognition

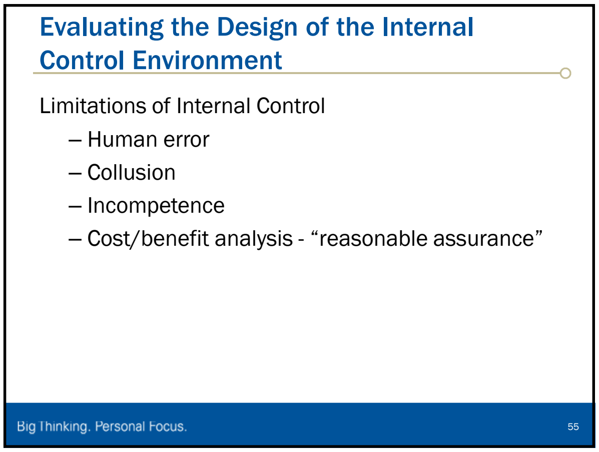


## Evaluating the Design of the Internal Control Environment

Competence

- Training
- Hiring
- Willingness to challenge the actions of others when such actions appear to be suspicious in nature or in direct violation of policy and procedures.

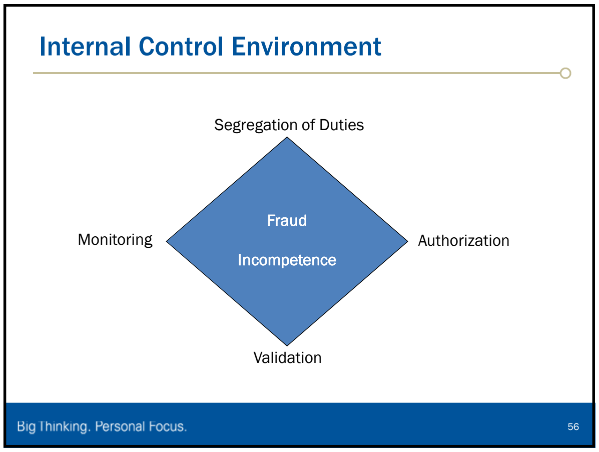
Trust Your Instincts - Avoid the compulsion to ignore/deny the obvious



## Evaluating the Design of the Internal Control Environment

Limitations of Internal Control

- Human error
- Collusion
- Incompetence
- Cost/benefit analysis - “reasonable assurance”



## Internal Control Environment

Segregation of Duties

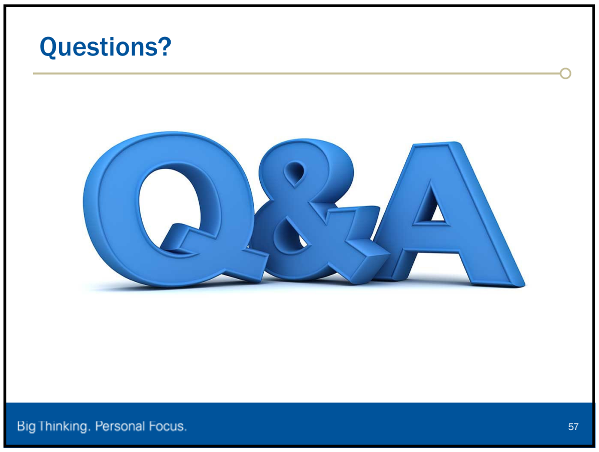
Monitoring

Fraud

Incompetence

Authorization

Validation



## Questions?

## Thank you!

**As one of the largest certified public accounting and business advisory firms in the region,** Schneider Downs serves clients throughout the country and around the world. By integrating high-quality resources, systems and personnel, Schneider Downs has built a reputation of delivering individualized services built on insight, innovation, and experience to meet each client's specific needs.

For more information, visit us at www.schneiderdowns.com

Big Thinking. Personal Focus.

Schneider Downs

Big Thinking. Personal Focus. 58