"Double, Double Boil & Trouble" – Internal Control & Fraud

Photo: Billy Morehead – Dakar, Senegal, West Africa, 2001

PRESENTER

Billy Morehead, Ph.D., CPA, CGFM, CGMA
Professor of Accountancy,
Director of Graduate Accounting Programs
Director of THE CENTER for Faith, Service, and Ethics
School of Business
Mississippi College

Today's Agenda

<1> COSO Framework

<2> Anatomy of Fraud

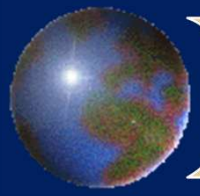
<3> Common Internal Control Weaknesses

<4> Role of Auditor vs Management

<5> Self Assessment

<6> Real World Examples

1. COSO Framework



Song of the Witches (from Macbeth) by William Shakespeare

Double, double toil and trouble;
Fire burn and caldron bubble.
Fillet of a fenny snake,
In the caldron boil and bake;
Eye of newt and toe of frog,
Wool of bat and tongue of dog,
Adder's fork and blind-worm's sting,
Lizard's leg and howlet's wing,
For a charm of powerful trouble,
Like a hell-broth boil and bubble.

Double, double toil and trouble;
Fire burn and caldron bubble.
Cool it with a baboon's blood,
Then the charm is firm and good.

Internal control is a process – effected by those charged with governance, management, and other personnel – designed to provide reasonable assurance about the achievement of entity's objectives with regard to:

- **Reliability of financial reporting**
- **Effectiveness and efficiency of operations, and**
- **Compliance with applicable laws and regulations**

Source: COSO

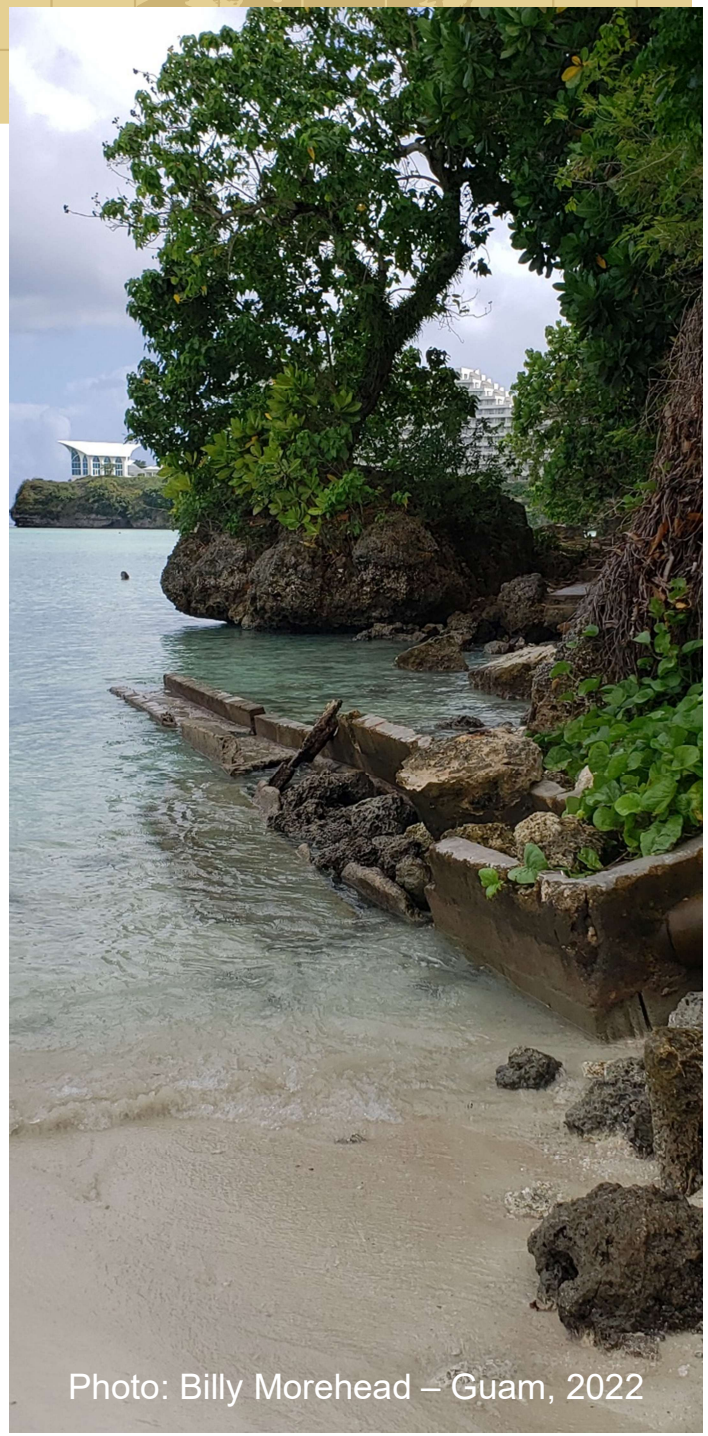
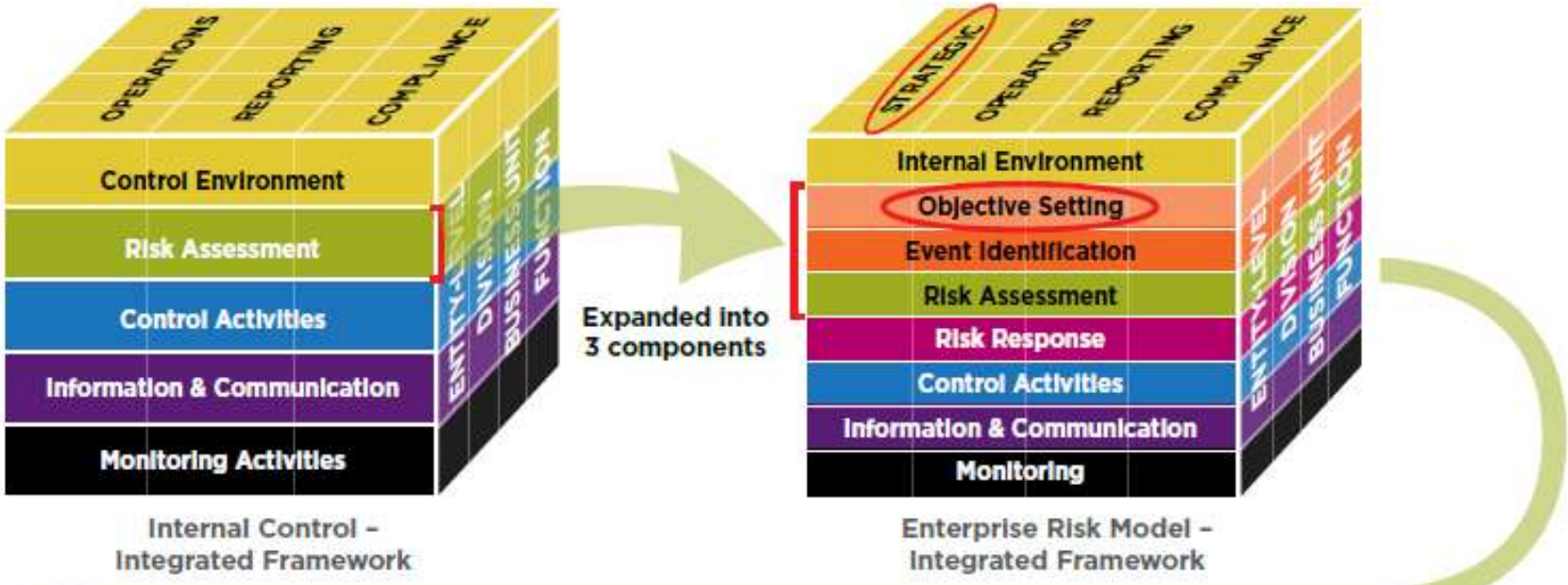


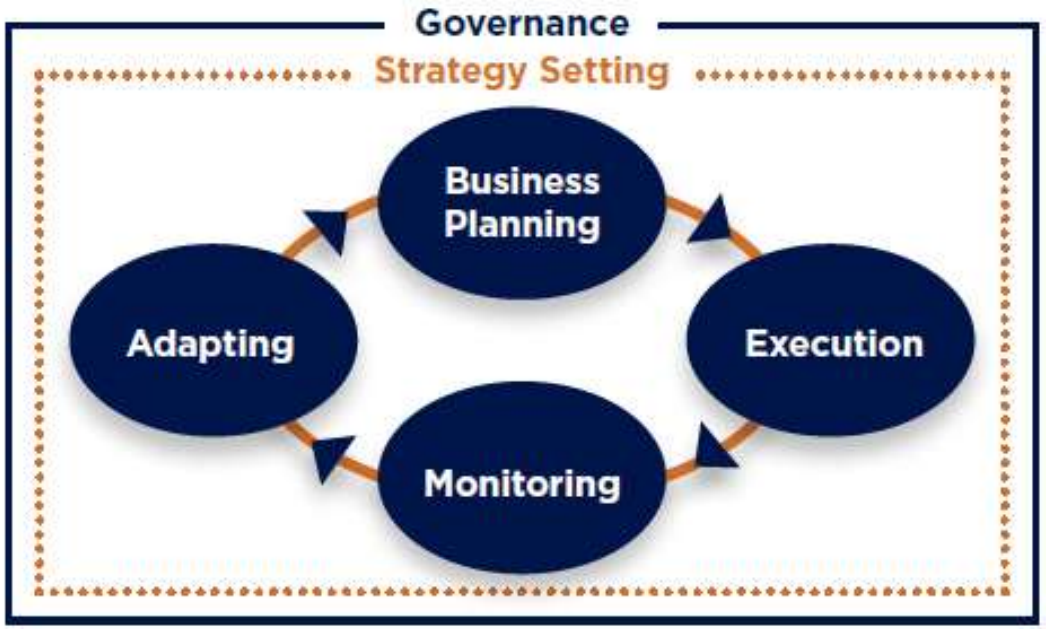
Photo: Billy Morehead – Guam, 2022

The Relationships Between the ICIF, ERMIF and Contextual Business Model



Internal Control – Integrated Framework

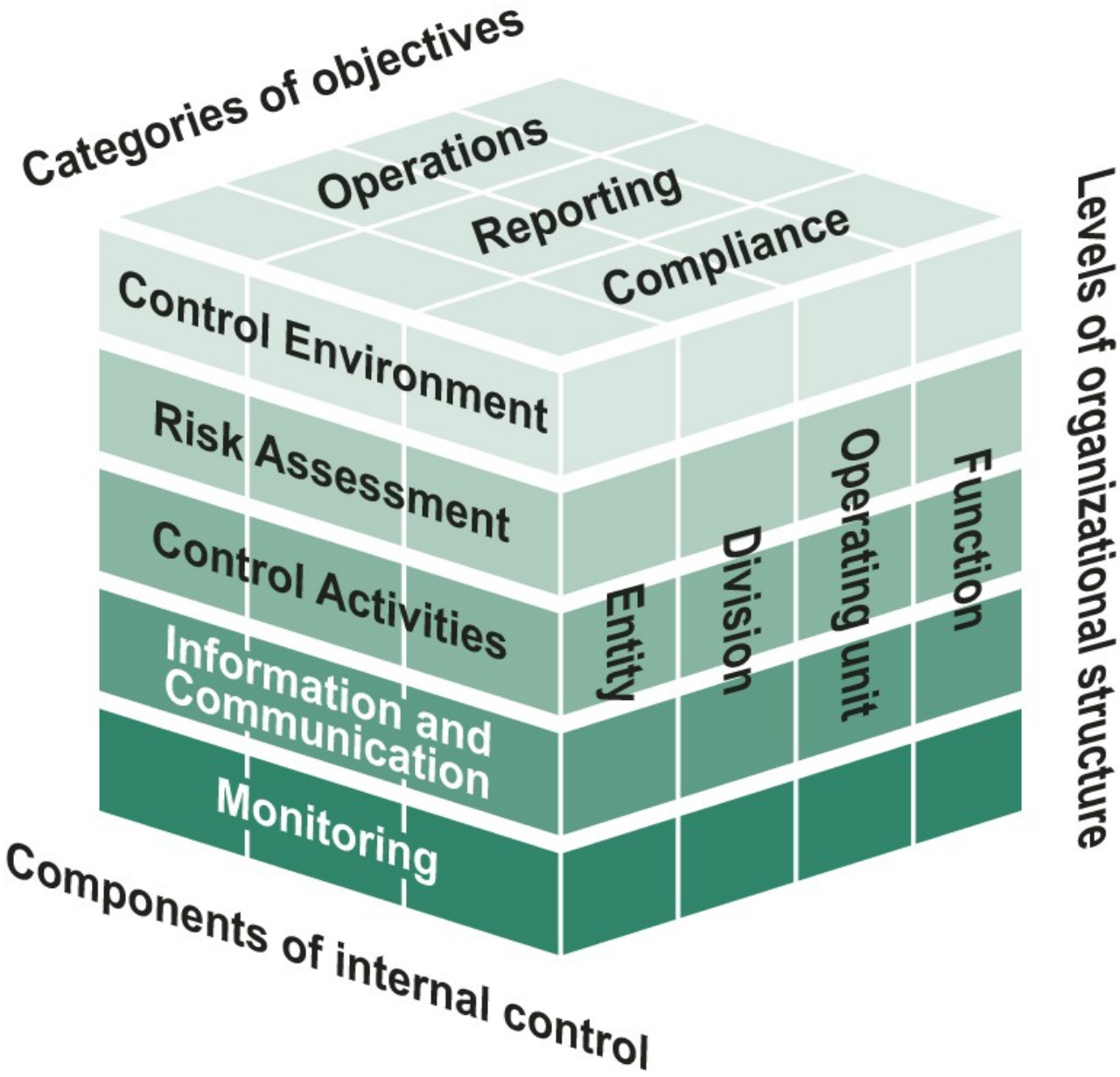
Enterprise Risk Model – Integrated Framework



Contextual Business Model

Source: COSO, Protiviti, & IMA (DeLoach & Thomson) – Improving Organizational Performance & Governance

2014 (2025) COSO CUBE



Achieving IC Objectives

Figure 2: Achieving Objectives through Internal Control

Source: GAO. | GAO-24-106889

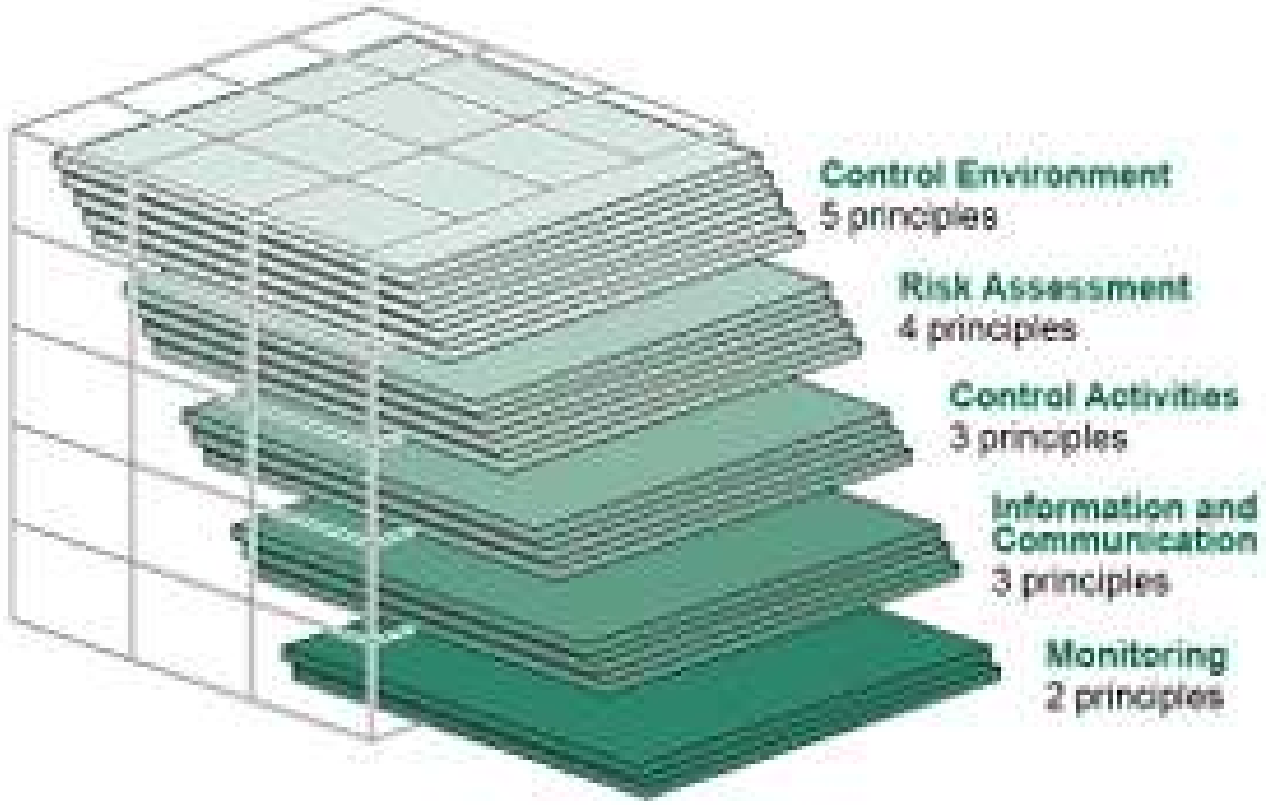
Oversight Body

2.09 The oversight body oversees management's design, implementation, and operation of the entity's internal control system. The oversight body's responsibilities for the entity's internal control system include the following:

- **Control Environment** - Establish integrity and ethical values, establish oversight structure, develop expectations of competence, and maintain accountability to all members of the oversight body and key stakeholders.
- **Risk Assessment** - Oversee management's assessment of risks to the achievement of objectives, including risks related to fraud, improper payments, information security, identified and potential changes, and management override of internal control.
- **Control Activities** - Provide oversight to management in the development and performance of control activities.
- **Information and Communication** - Analyze and discuss information relating to the entity's achievement of objectives.
- **Monitoring** - Scrutinize the nature and scope of management's monitoring activities as well as its evaluation and remediation of identified deficiencies.

Components & Principles of IC

Figure 5: The 17 Principles Supporting the Five Components of Internal Control



Source: GAO. | GAO-24-106699

Components & Principles of IC

Figure 3: The Five Components and 17 Principles of Internal Control

Control Environment

1. The oversight body and management should demonstrate a commitment to integrity and ethical values.

2. The oversight body should oversee the entity's internal control system.

3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.

4. Management should demonstrate a commitment to recruit, develop, and retain competent individuals.

5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.

Risk Assessment

6. Management should define objectives clearly to enable the identification of risks and define risk tolerances.

7. Management should identify, analyze, and respond to risks related to achieving the defined objectives.

8. Management should consider the potential for fraud, improper payments, and information security risk when identifying, analyzing, and responding to risks.

9. Management should identify, analyze, and respond to significant changes that could impact the internal control system.

Control Activities

10. Management should design control activities to mitigate risks to achieving the entity's objectives to acceptable levels.

11. Management should design general control activities over information technology to mitigate risks to achieving the entity's objectives to acceptable levels.

12. Management should implement control activities through policies and procedures.

Information and Communication

13. Management should obtain or generate, and use relevant, quality information to support the functioning of the internal control system.

14. Management should internally communicate relevant and quality information, including objectives and responsibilities for internal control, necessary to support the functioning of the internal control system.

15. Management should communicate relevant and quality information with appropriate external parties regarding matters impacting the functioning of the internal control system.

Monitoring

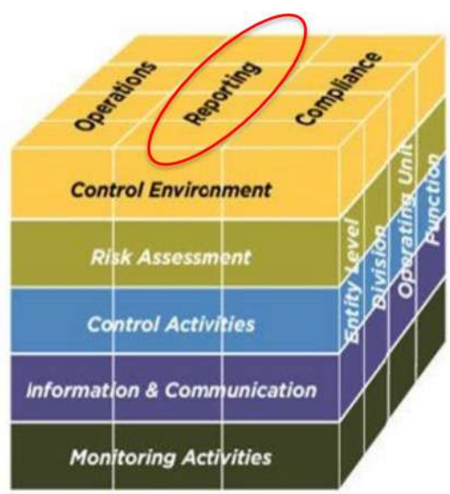
16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.

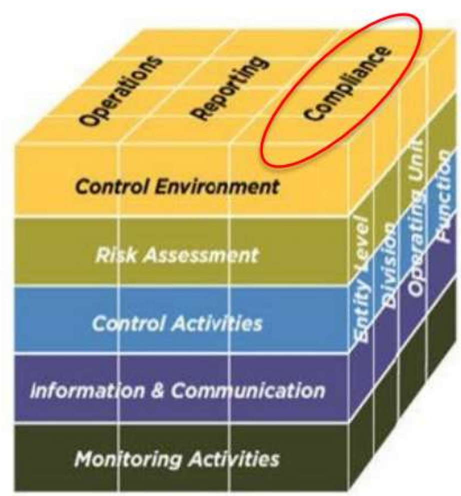
17. Management should remediate identified internal control deficiencies on a timely basis.

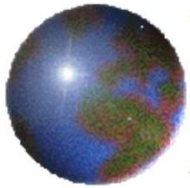
Source: GAO. | GAO-24-106889

COSO Summary In Plain English

- **Operations** – Relates to achievement of entity's mission and vision (fundamental reason for existence). Pertains to all kinds of entities.
- **Reporting** – Pertains to preparation of reports for use by management and governance
- **Compliance** – Pertains to applicable laws and regulations







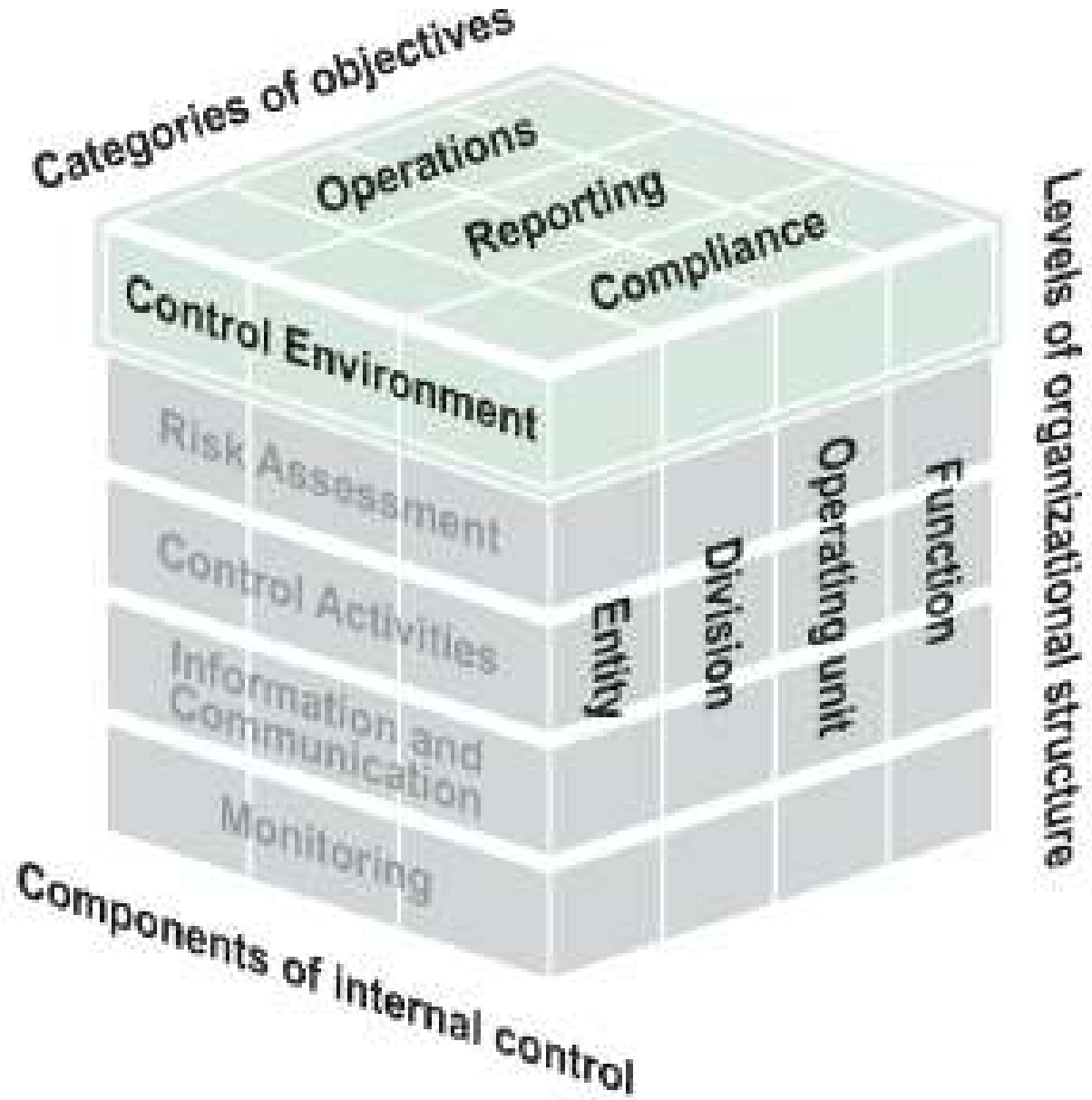
COSO Summary In Plain English

- **Control Environment** – tone at the top (do leaders promote honesty, are roles clearly defined?)
- **Risk Assessment** – spotting trouble ahead (what are the financial, legal, or operational threats?)
- **Control Activities** – the safeguards (what controls are in place to prevent or detect issues?)
- **Information & Communication** – does information flow to the right people at the right time?
- **Monitoring** – constant review and improvement (are controls still working, did we fix problems quickly, did we learn from mistakes?)

COSO – Why It Matters

- It helps prevent
  - Fraud
  - Misuse of funds
  - Compliance failures
  - Financial reporting errors
- It helps ensure
  - Public trust
  - Organizational effectiveness
  - Sound decision-making

Control Environment



Control Environment

Control Environment

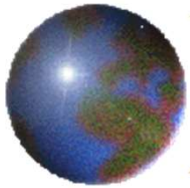
1. The oversight body and management should demonstrate a commitment to integrity and ethical values.

2. The oversight body should oversee the entity's internal control system.

3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.

4. Management should demonstrate a commitment to recruit, develop, and retain competent individuals.

5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.



Control Environment

It is the foundation for effective internal control, providing discipline and structure.

The control environment sets the tone of an organization influencing the control consciousness of its people.

Risk Assessment

Risk Assessment

Risk Assessment

6. Management should define objectives clearly to enable the identification of risks and define risk tolerances.

7. Management should identify, analyze, and respond to risks related to achieving the defined objectives.

8. Management should consider the potential for fraud, improper payments, and information security risk when identifying, analyzing, and responding to risks.

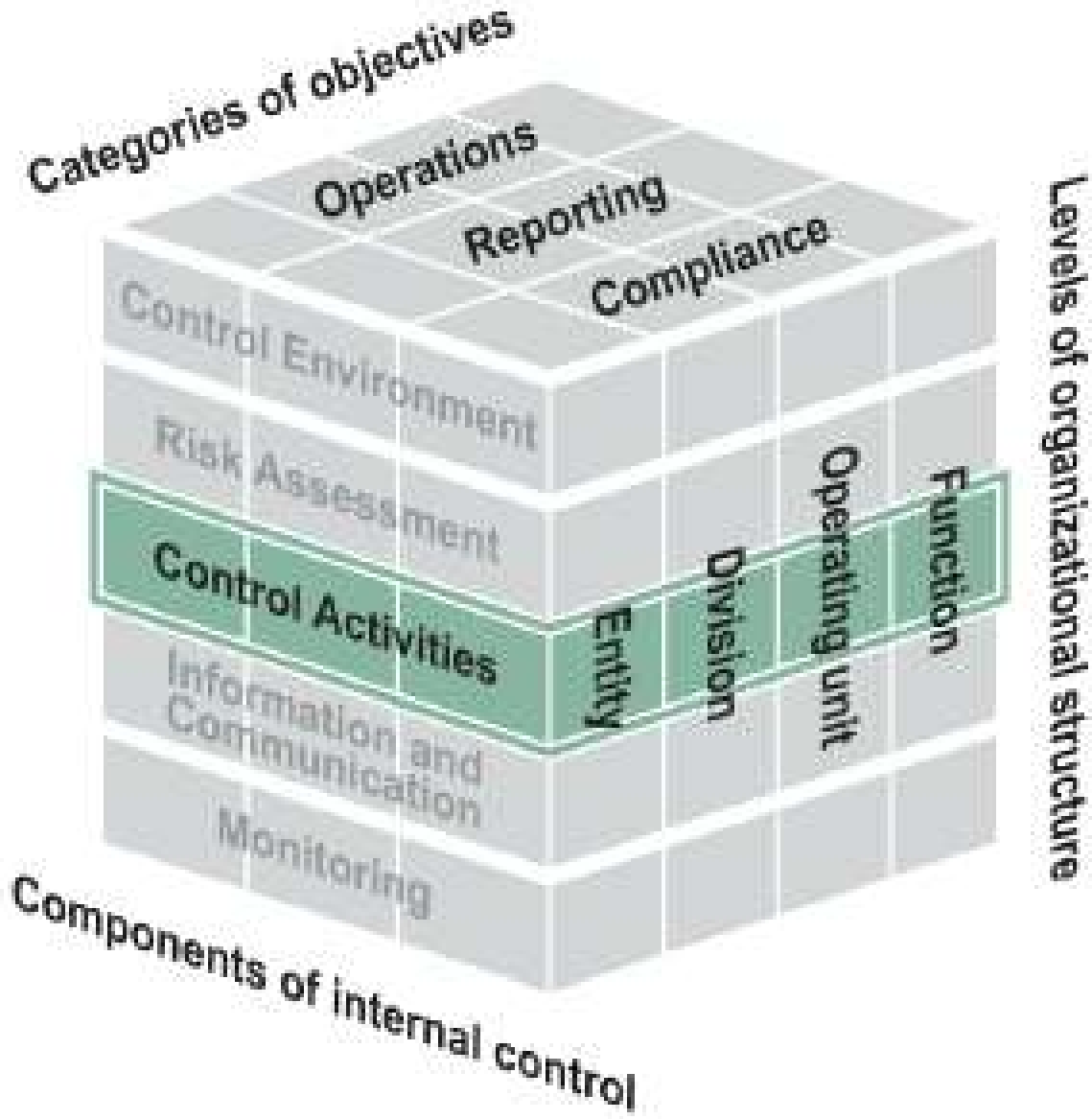
9. Management should identify, analyze, and respond to significant changes that could impact the internal control system.

Source: GAO. | GAO-24-106889

Possible Responses to Risk

- 1. Avoid it.
- 2. Live with it.
- 3. Share it (or transfer it to someone else).
- 4. Attempt to manage it.

Control Activities



Control Activities

Control Activities

10. Management should design control activities to mitigate risks to achieving the entity's objectives to acceptable levels.

11. Management should design general control activities over information technology to mitigate risks to achieving the entity's objectives to acceptable levels.

12. Management should implement control activities through policies and procedures.

Examples: Common Categories of Control Activities

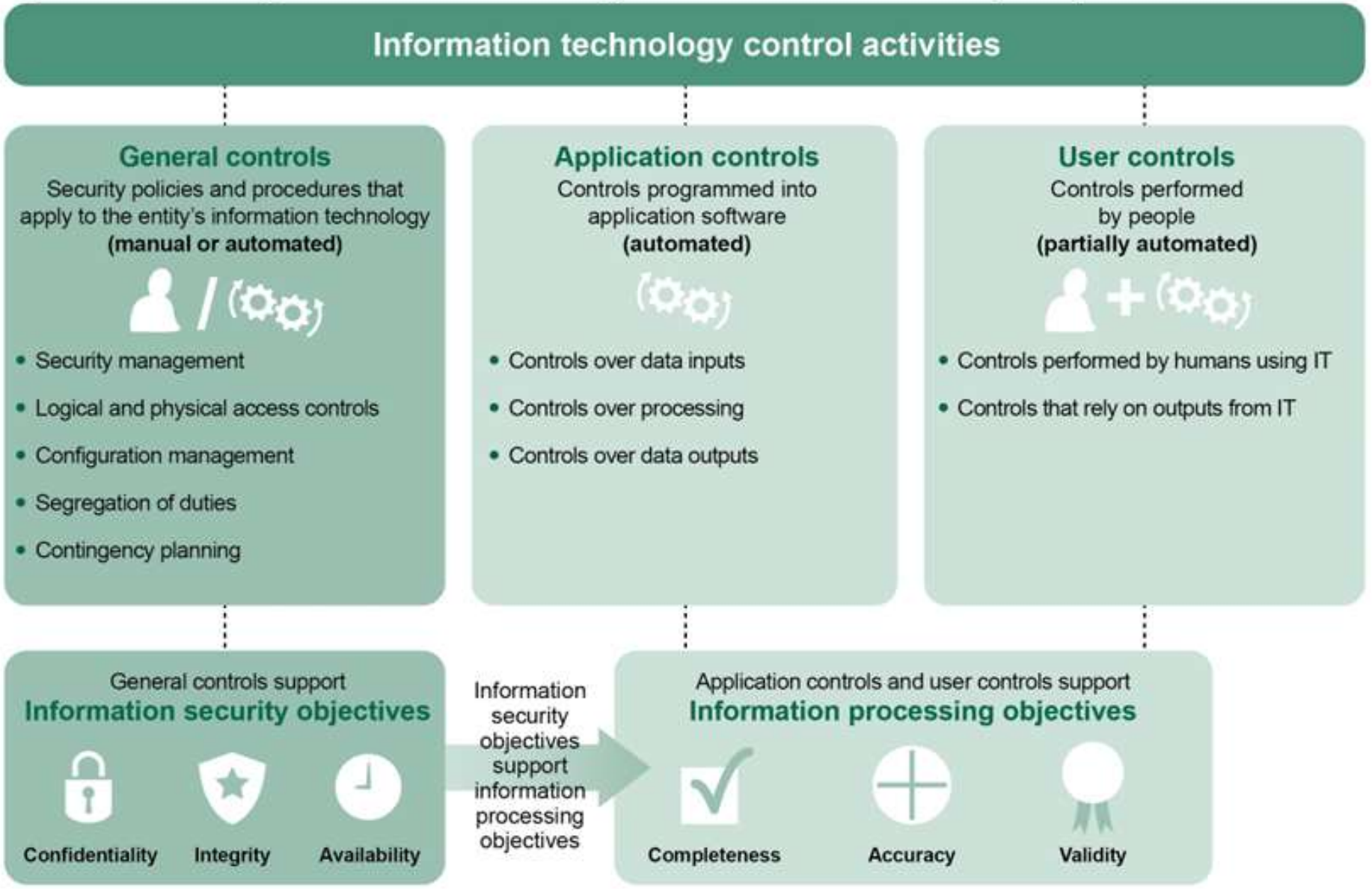
- Top-level reviews of actual performance
- Reviews by management at the functional or activity level
- Management of human capital
- Controls over information processing
- Physical control over vulnerable assets
- Establishment and review of performance measures and indicators

Examples: Common Categories of Control Activities

- Segregation of duties
- Proper execution of transactions
- Accurate and timely recording of transactions
- Access restrictions to and accountability for resources and records
- Appropriate documentation of transactions and internal control

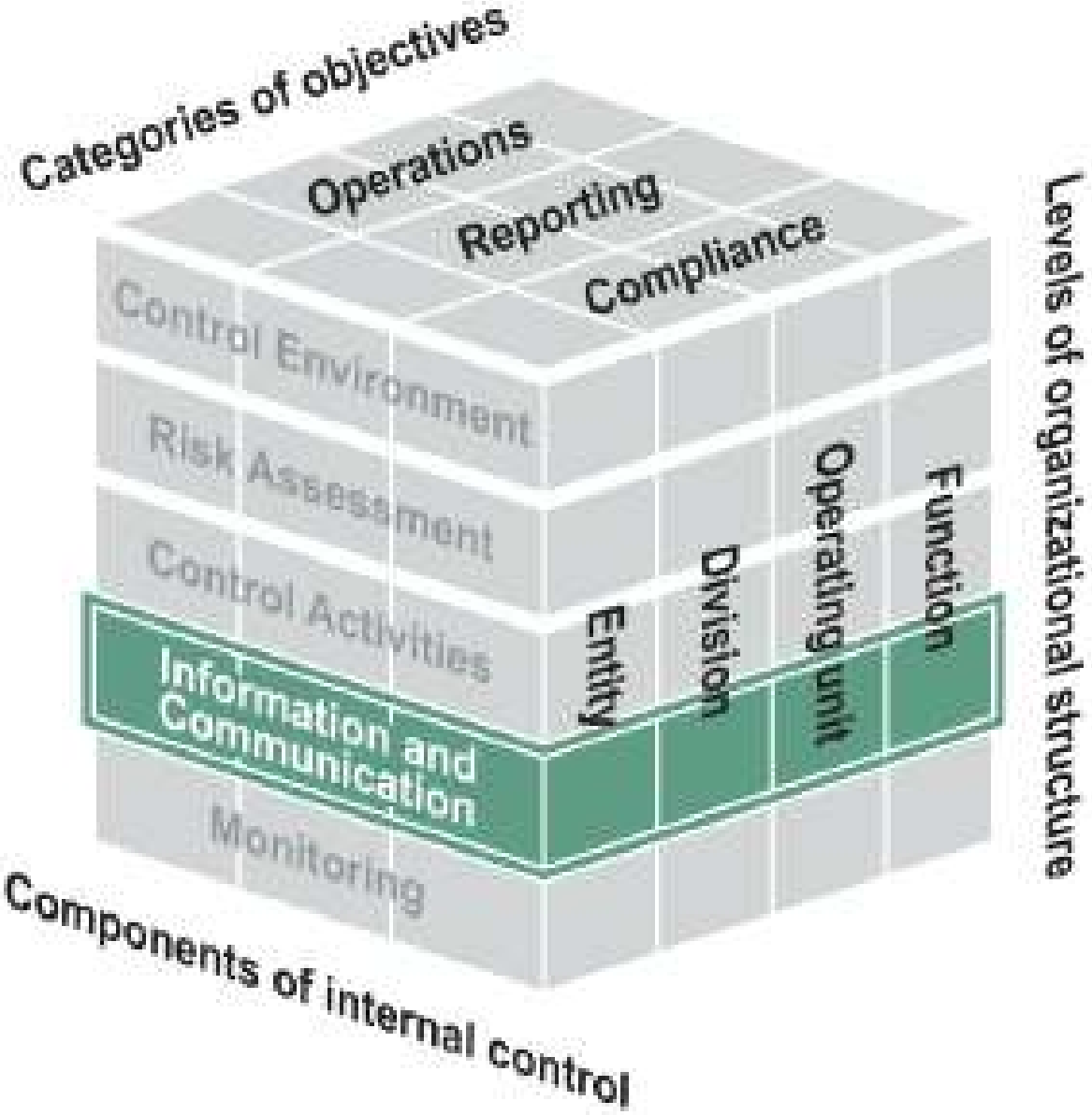
IT Control Activities

Figure 7: Common Categories of Information Technology Control Activities and Relationship to Objectives



Source: GAO. | GAO-24-106889

Information & Communication



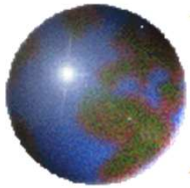
Information & Communication

Information and Communication

13. Management should obtain or generate, and use relevant, quality information to support the functioning of the internal control system.

14. Management should internally communicate relevant and quality information, including objectives and responsibilities for internal control, necessary to support the functioning of the internal control system.

15. Management should communicate relevant and quality information with appropriate external parties regarding matters impacting the functioning of the internal control system.



Appropriate Methods of Communication

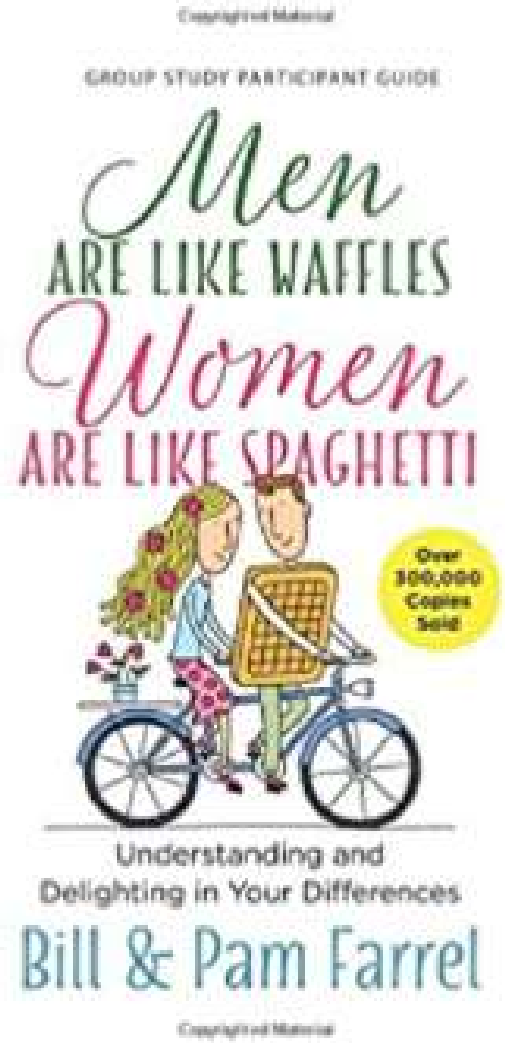
- Audience
- Nature of Information
- Availability
- Cost
- Legal or regulatory requirements
- Completeness
- Accuracy
- Validity

Communication Strategies& Modalities: Know Your Targets

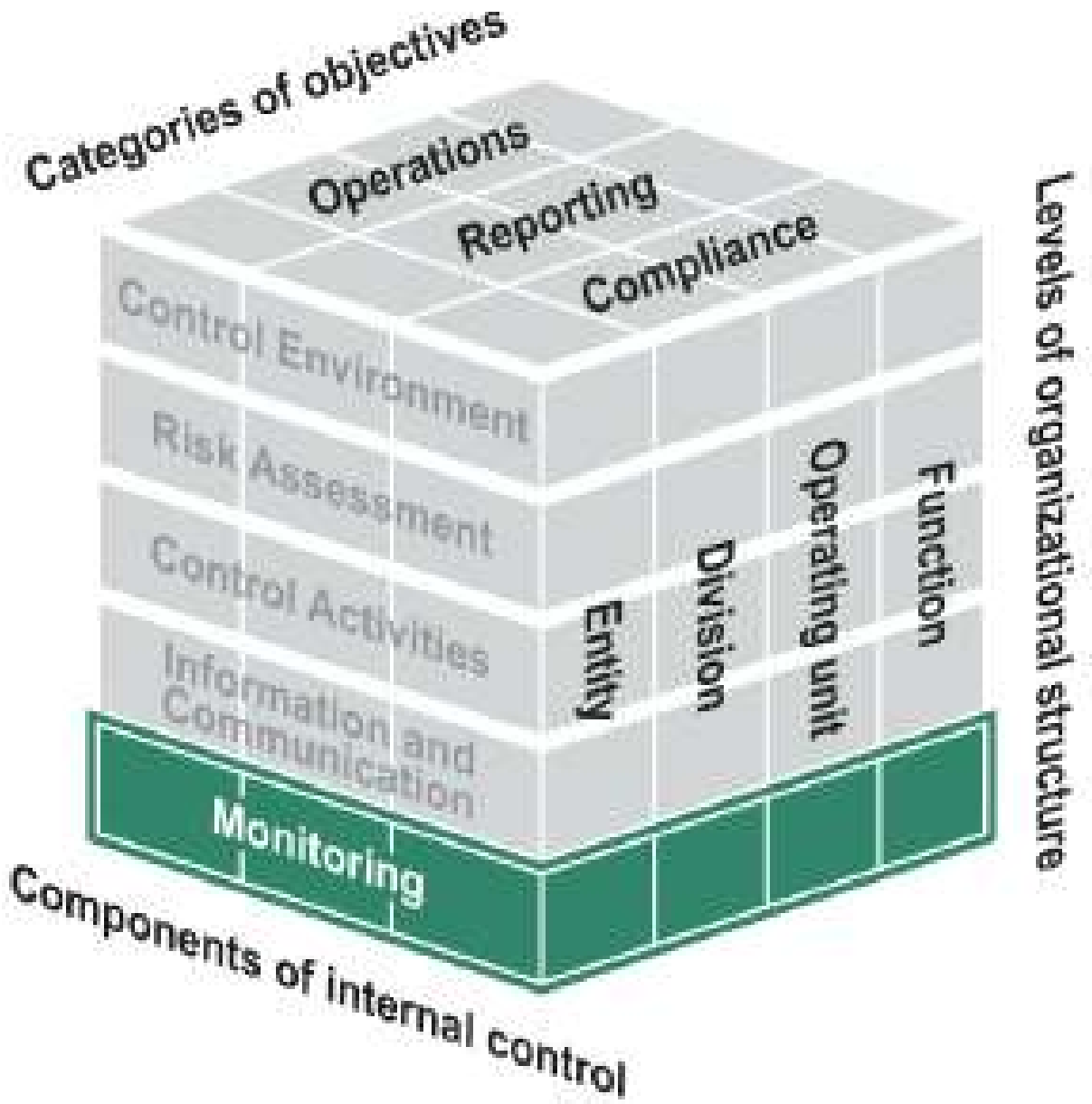
- Multiple Modalities & Generational Challenges in 2025:
  - Live and In-Person (F2F)
  - Video (Zoom, Teams, etc.)
  - Phone Call
  - Email
  - Message (text, WhatsApp, FB Messenger, LinkedIn, Slack, others)
- People often use the WRONG modality:
  - Breaking up or delivering bad news by text
  - Using Zoom or Teams when F2F is better?
  - Texting or messaging stakeholders when a phone call is best?

What Makes Communicating Work?

Knowing the difference between Spaghetti and Waffles…



Monitoring


Categories of objectives
Operations
Reporting
Compliance
Control Environment
Risk Assessment
Control Activities
Information and Communication
Monitoring
Components of internal control
Entity
Division
Operating unit
Function
Levels of organizational structure

Monitoring

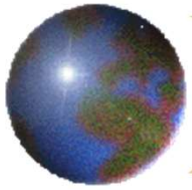
Monitoring

16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.

17. Management should remediate identified internal control deficiencies on a timely basis.

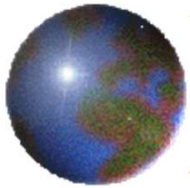
Monitoring Activities

- Establishment of a baseline
- IC system monitoring
- Reporting of issues
- Evaluation of issues & results
- Corrective actions



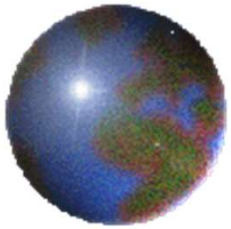
Limitations of Internal Control

- Not a cure all
- Suitability of objectives used in establishing IC system
- Cannot ensure entity's success or survival
- Cannot ensure entity will achieve operation, financial reporting, and compliance objectives
- Effectiveness limited by human judgment, hasty & faulty decision making
- External events beyond entity's control



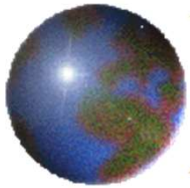
Limitations of Internal Control

- System can breakdown due to misunderstandings, mistakes in judgment, or errors committed due to carelessness, distraction, or fatigue
- Only as effective as the people who are responsible for its functioning
- Collusion can result in control failure
- Limited resources (cost/benefit)
  - excessive control is costly & counterproductive
  - too little control presents undue risk to entity



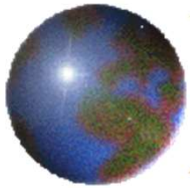
Evaluating Controls is Not a One Time Thing

Processes change, positions are not replaced, budget reductions, new threats emerge…



Appendix One

- The 5 components of IC must be effectively designed, implemented, & operating together in an integrated manner, for an IC system to be effective.
- The 17 principles of IC must be in place.
- Documentation of the IC system is a must based on size & complexity of entity.



Appendix Two

How do I use this Appendix?

Important facts and concepts related to preventive and detective control activities

What is this Appendix?

This appendix is designed to supplement the control activities component. It provides:

- Discussion on types of control activities and how control activities differ from monitoring activities
- Examples of preventive and detective control activities, and
- Sources of external data to use in control activities

Who is this Appendix for?

The oversight body | Financial managers | Program managers | Personnel

What are control activities?

Actions management establishes through policies and procedures as part of the control activities component to mitigate risks to achieving the entity's objectives to acceptable levels. They can be implemented as:

Preventive Designed to avoid an unintended event or result before it occurs

Detective Designed to discover and timely correct an unintended event or result

Selecting control activities

To mitigate risks, management designs an appropriate mix of preventive and detective controls

Management considers preventive control activities first. Preventive controls:

- Offer the most cost-efficient use of resources
- Avoid a difficult and expensive "pay and chase model"

Step 1: Preventive

Examples of preventive controls

- Training on internal control
- Password management
- Network security
- Authentication controls
- Automated approvals
- Preventive data analytics
- Identity-verification controls
- Eligibility-verification controls
- Unique identifiers to prevent duplication

Step 2: Detective

Examples of detective controls

- Post-payment reviews
- Reconciliations
- Detective data analytics
- Respond to reported risks and incidents
- Controls over automated processes
- Malicious software detection

External data sources

Management may share data with or obtain data from other entities to perform control activities. Examples include:

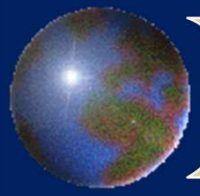
Do not pay provides a variety of data-matching and other data-analytics services for federal and state agencies to help prevent and detect improper payments

The **Death master file** is used to verify data for program beneficiaries to prevent improper payments to deceased persons

Source: GAO. | GAO-24-106889

Appendix Three - Additional Resources

- Fraud Resources:
  - GAO Fraud Risk Framework
  - GAO Antifraud Resource
  - OMB Circular A-123
- Improper Payment Resources:
  - GAO Improper Payments Framework
  - OMB Memo M-21-19, Transmittal of Appendix C to OMB Circular A-123
  - Improper Payments & Fraud: How They Are Related But Different
  - GAO Improper Payments Topic Page
  - Official Payment Accuracy Website
- Information Security Resources
  - National Institute of Standards & Technology Guidance
  - GAO Cybersecurity Topic Page
  - GAO Science & Technology Topic Page
  - OMB Circular A-130, Managing Information as a Strategic Resource



2. Anatomy of a Fraud

Fraud Triangle

In the 1970s, criminologist Donald R. Cressey wrote about a model called the "fraud triangle." The fraud triangle outlines the three conditions that lead to higher instances of occupational fraud:

- **Motivation (pressure),**
- **opportunity,**
- **rationalization.**

Fraud Triangle

What Is Fraud?

"Fraud" is any activity that relies on deception in order to achieve a gain. Fraud becomes a crime when it is a "knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment" (Black's Law Dictionary). In other words, if you lie in order to deprive a person or organization of their money or property, you're committing fraud.

- Association of Certified Fraud Examiners

What Is Fraud?

Characteristics of Fraud: AU-C 240.02 and .03

- Two types of intentional misstatement that are relevant to auditors
- Misstatements in financial statements can arise from - Fraud or Error
- Misstatements resulting from fraudulent financial reporting
- Misstatements resulting from misappropriation of assets

Fraudulent Financial Reporting

AU-C 240.45 illustrates:

- Fraud is accomplished by:
  - Manipulation, falsification (including forgery), or alteration of accounting records or supporting documentation from which the financial statements are prepared
  - Misrepresentation in, or intentional omission from, the financial statements of events, transactions, or other significant information
  - Intentional misapplication of accounting principles relating to amounts, classification, manner of presentation, or disclosure

Responsibility for Prevention and Detection

AU-C 240.04:

The **primary responsibility** for the prevention and detection of fraud **rests with both those charged with governance of the entity and management**:

- Important that these individuals place a strong emphasis on fraud prevention, which can reduce opportunities, and fraud deterrence, which could persuade individuals not to commit such acts
- This commitment involves creating a culture of honesty and ethical behavior

Governance must consider the potential override of controls or other inappropriate influence over financial reporting

Examples of Circumstances That Indicate the Possibility of Fraud, AU-C 240, Appendix C

Discrepancies in the accounting records, including the following:

- Transactions that are not recorded in a complete or timely manner
- Last-minute adjustments that significantly affect financial results

Conflicting or missing evidence, including the following:

- Missing documents
- Significant unexplained items on reconciliations

Conditions relating to governmental entities or not-for-profit organizations:

- Significant transfers or transactions between funds or programs, or both, lacking supporting documents
- Significant budget adjustments

3. Common Internal Control Weaknesses

Internal Controls – Why It Matters

- Reduces audit findings and repeat comments. More findings can mean a higher risk to the audit and more testing by the auditor
- Protects public assets and reputation
- Increases efficiency and accountability
- Meets compliance requirements (Yellow Book, GASB, grant compliance)

Common Internal Control Weaknesses

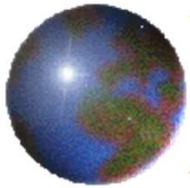
- Lack of segregation of duties
- Inadequate review of journal entries or reconciliations (including no *documentation* of review)
- Bank reconciliations not performed or not timely
- Weak IT and access controls
- Grant compliance controls
- Outdated policies & procedures, or policies simply not followed

Lack of Segregation of Duties

- **Common Weakness:** One person handles cash, records, and also does the reconciling
- **Risk:** Increased risk of fraud or error being undetected
- **Solution:** Separate out duties, implement compensating controls (i.e. reviews by someone else)

Inadequate Review of Journal Entries or Reconciliations

- **Common Weakness:** No review of journal entries by someone other than the preparer
- **Risk:** An entry could have a major error, be backwards, not have support, and no one would question it
- **Solution:** Ensure that someone is knowledgeable in reviewing and approving journal entries and supporting the entries on a regular basis. Retain documentation of the review



Management Override of Controls – Journal Entries

AU-C 240.31

- Management is in a unique position to perpetuate fraud because of management's ability to manipulate accounting records and prepare fraudulent financial statements by overriding controls that otherwise appear to be operating effectively.
- Risk of management override of controls is present in all entities.
- The risk exists in every audit.
- Due to the unpredictable way in which such an override could occur, it is a risk of material misstatement due to fraud and, thus, a significant risk.

Management Override of Controls

AU-C 240.A6

- Recording fictitious journal entries to manipulate operating results or achieve other objectives
- Inappropriately adjusting assumptions and changing judgments used to estimate account balances
- Omitting, advancing, or delaying recognition in the financial statements of events and transactions that have occurred during the reporting period
- Omitting, obscuring, or misstating required disclosures that are necessary to achieve fair presentation
- Concealing facts that could affect the amounts recorded in the financial statements
- Engaging in complex transaction that are structured to misrepresent the financial position or financial performance of the entity
- Altering record and terms related to significant and unusual transactions

Bank Reconciliations

- **Common Weakness:** Untimely or unreconciled bank accounts
- **Risk:** Misstatement of financials; Not having a proper level of cash for operational purposes
- **Solution:** Ensure that monthly reconciliations with independent review are occurring; Implement checklists with due dates

Grant Compliance Controls

- **Common Weakness**: Poor tracking of grant requirements (such as required reporting), poor tracking of allowable costs
- **Risk:** Grantor not reimbursing funds, loss of the grant
- **Solution:** Create a grant checklist, assign specific people to tasks, and assign deadlines for grant requirements

IT and Access Controls

- **Common Weakness:** Shared logins
- **Risk:** Cannot determine who performed tasks, cannot hold people accountable
- **Solution:** Ensure users are set up separately with access needs that fit their job duties

IT and Access Controls

- **Common Weakness:** Not immediately removing access from terminated employees
- **Risk**: A terminated employee can still get into the system
- **Solution**: Ensure there is a process in place for immediate removal of access to important systems. Retain a checklist and ensure removal was completed.

IT and Access Controls

- **Common Weakness:** Improper policy over backups
- **Risk**: Loss of data (could be the result of a data breach or a natural disaster)
- **Solution**: Ensure there is a process in place for regular backups as well as storing backups (off-site location). Check backups occasionally to make sure they are working

IT and Access Controls

- **Common Weakness**: No review of SOC 1 Type II reports for service organizations
- **Risk**: Service organizations are an extension of your controls. Controls are essentially delegated to the organization (i.e., outside payroll provider).
- **Solution**: Obtain the report annually (before the audit) and review it for deficiencies. Ensure that the complementary user controls at the City are implemented as required.

Outdated policies & procedures

- **Common Weakness**: Old policies and procedures, not updated regularly, or simply not being followed
- **Risk**: Not in compliance with laws or grant requirements, missing controls (*internal controls are embedded in the policies & procedures*), increased fraud and error risk
- **Solution**: Review regularly and update as necessary. Ensure staff are following written policies and *held accountable*

Outdated policies & procedures

Keep them adaptable and relevant to the entity structure

- *Policies* reflect what should be done to effect control
- *Procedures* are actions that implement policies

Example Controls

- Cash receipts (revenues)
- Cash disbursements
- Procurement and contract management
- Grant management
- Payroll and timekeeping
- Debt
- Medical Billing Controls

Cash Receipts

- **Segregation of duties between receiving, recording, and depositing funds**
- **Daily or weekly reconciliation of collections to deposit slips or accounting records**
- **Timely deposits (daily)**
- **Restricted access to bank accounts**
- **Independent review of bank reconciliations and statements**
- **Monitoring receivables and aging reports**

Cash Disbursements

- **Dual authorization on payments (dept. head, finance)**
- **Vendor invoices matched to POs and receiving documents (3-way match)**
- **Pre-numbered checks and system-generated payments with audit trails (ACH or online payments need an audit trail of approval)**
- **Use approved vendor lists**

Procurement and Contract Management

- **Formal procurement policy based on dollar thresholds and competitive bidding**
- **Approval hierarchy for purchases**
- **Conflict-of-interest check for procurement staff**
- **Written contracts reviewed by legal counsel before execution**
- **Centralized tracking of contracts, amendments, and expiration dates**
- **Periodic vendor audits or performance reviews**

Grant Management

- Centralized tracking of grant applications, awards, deadlines
- Clear assignments of responsibilities for grant compliance and reporting, especially if non-finance departments are involved
- Budget to actual comparisons in grant funded activities
- Supporting documentation for grant-expenditures
- Reimbursement requests reviewed for eligibility and submission
- Grant closeout procedures

Payroll and Timekeeping

- **Use of a timekeeping system with supervisor approval of time**
- **Separation of payroll processing, approval, and distribution**
- **Review and approval of payroll register by someone other than the preparer**
- **Restricted access to the payroll system and personnel records**
- **Regular reconciliation of payroll to the general ledger**
- **Clear procedures for handling changes in pay rates, job status, and benefits**
- **Monitoring overtime and leave balances**

Debt Management

- **Centralized recordkeeping of all debt agreements and schedules**
- **Governing board approval for issuance of new debt**
- **Compliance with legal limits, covenants, reporting requirements**
- **Independent review of bond and loan terms before acceptance**
- **Disclosure filings on time (EMMA reporting)**
- **Periodic analysis of refinancing opportunities or cost savings**

Medical Billing & Referral

- **Staff familiarity with medical coding**
  - **Common codes in each clinic/service area**
  - **Standard coding forms for each clinic/service area**
  - **Use of bundled codes where appropriate**
  - **Upcoding awareness**
  - **Compliance with Medical referral policies**
  - **Staff and physician training in coding & compliance**

4. Role of Auditor vs. Management

Management's Role

- **Design, implement, and maintain internal controls**
- **Establish policies and procedures**
- **Accurate and timely financial reporting**
- **Safeguard assets**
- **Respond to and correct audit findings**
- **Preventing and detecting errors and fraud**