CliftonLarsonAllen

Practical Considerations for Internal Controls in an Electronic Environment

Allison Slife, CPA

Manager, State and Local Government

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor. |

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Last Twenty Years

1992

- (COSO) released its *Internal Control – Integrated Framework* (the original framework).

2010

- COSO announced a project to review and update the 1992 *Internal Control – Integrated Framework*.

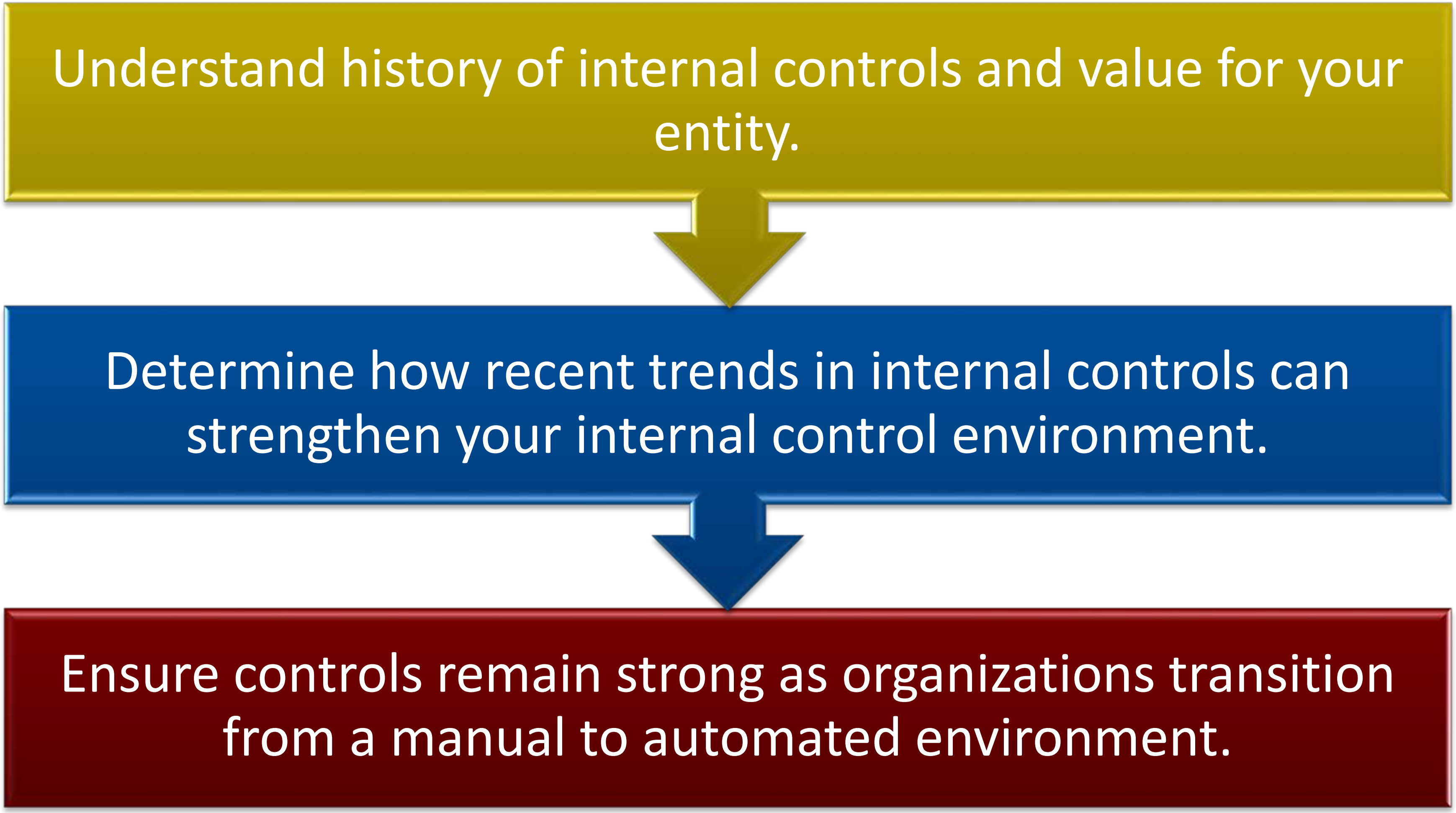
2002

- The Sarbanes-Oxley Act of 2002 was passed.

2013

- COSO issued updated *Internal Control – Integrated Framework*

Learning Objectives



Understand history of internal controls and value for your entity.

Determine how recent trends in internal controls can strengthen your internal control environment.

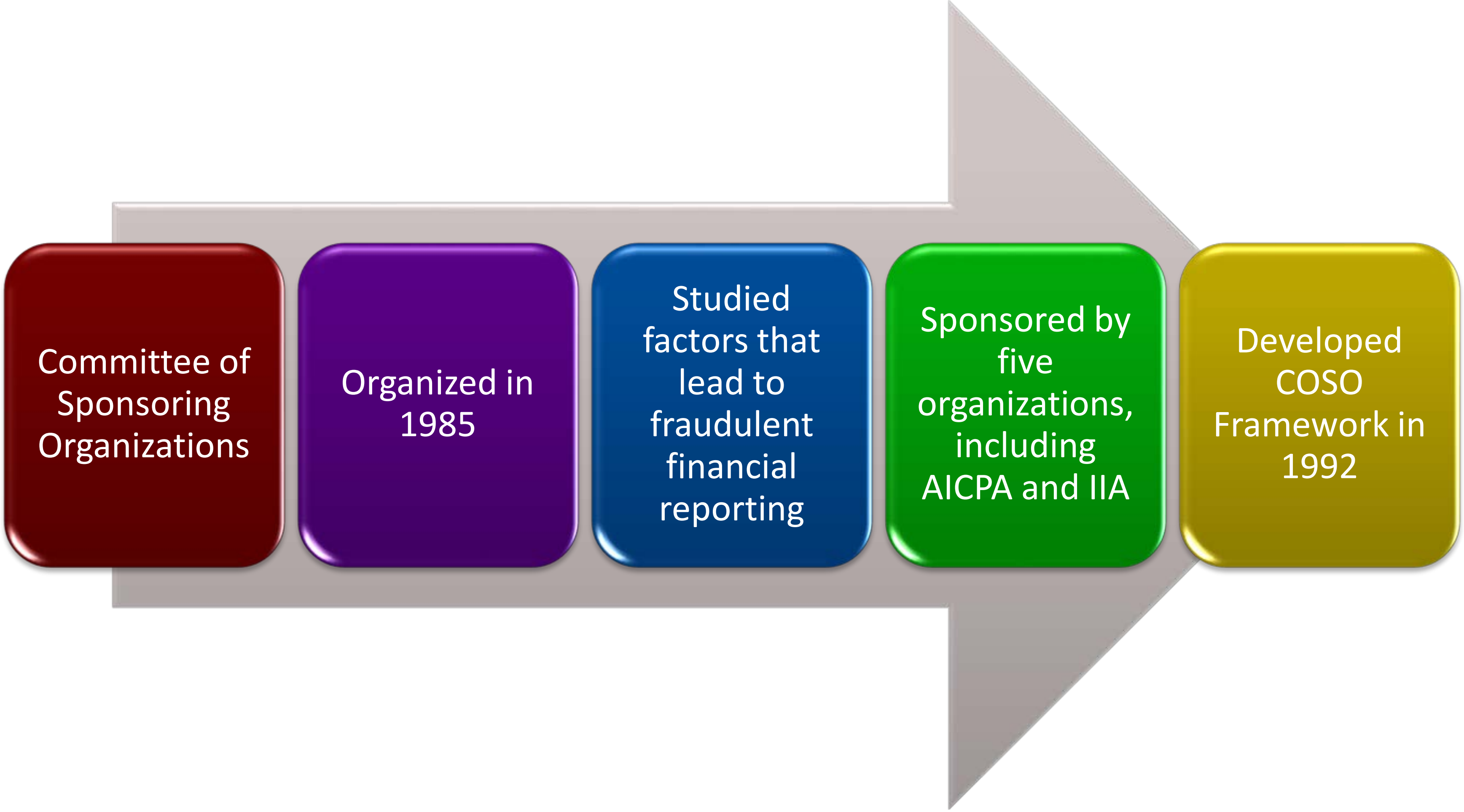
Ensure controls remain strong as organizations transition from a manual to automated environment.

Friendly Reminders

Importance of Internal Controls

- Prevention and detection of:
  - Fraud
  - Material misstatements
  - Material non-compliance
  - Operational mishaps
  - “Newspaper” risk

Who is COSO?



Committee of Sponsoring Organizations

Organized in 1985

Studied factors that lead to fraudulent financial reporting

Sponsored by five organizations, including AICPA and IIA

Developed COSO Framework in 1992

IF IT’S NOT BROKEN, DON’T FIX IT..

FALSE. IMPROVEMENT IS ALWAYS POSSIBLE……

Much has changed since 1992….

Expectations for governance oversight

Risk assessments receive greater attention

Globalization of markets

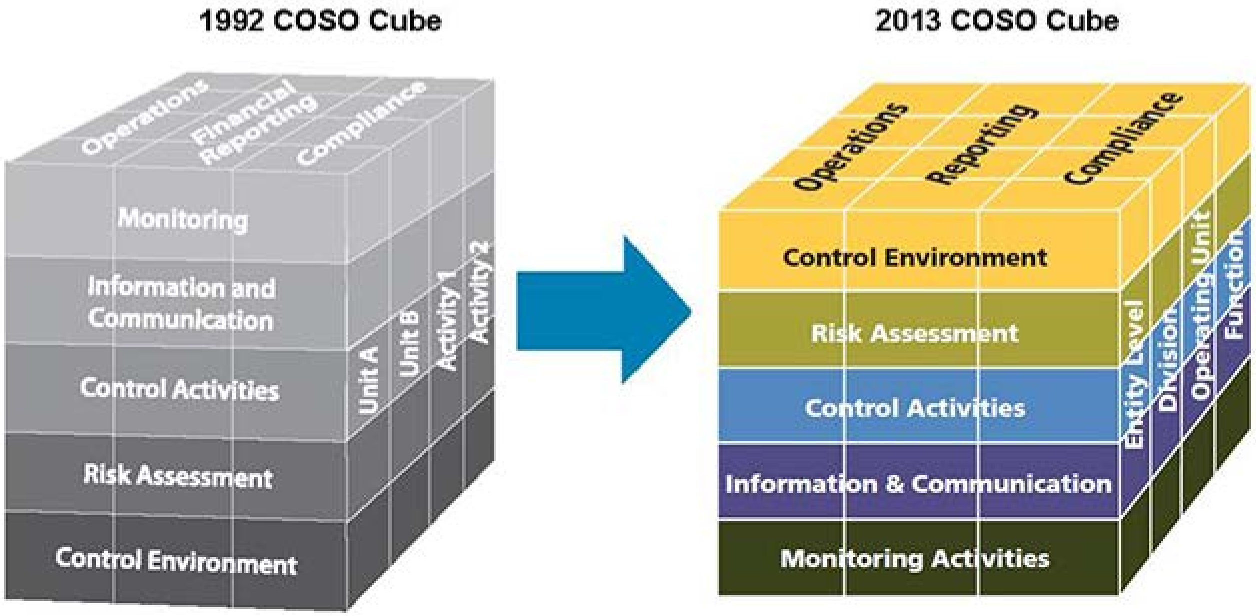
…just to name a few!

Technology

Increase in regulations and standards

What Didn't Change

- Cube stayed very similar.
  - Five Components of Internal Control
- Use of judgment.



What Did Change

17 **principles** that support 5 components of internal control.

- To increase management’s understanding as to what constitutes effective internal controls.

Each principle has supporting **points of focus** (77 total)

- To provide helpful guidance in designing, implementing, and conducting internal controls.
- Management has latitude to exercise judgement in which to evaluate.

Increased focus on…

- Technology
- Governance Oversight
- Anti-Fraud Expectations
- Non-financial reporting objectives (operations, compliance, etc.)

17 Principles

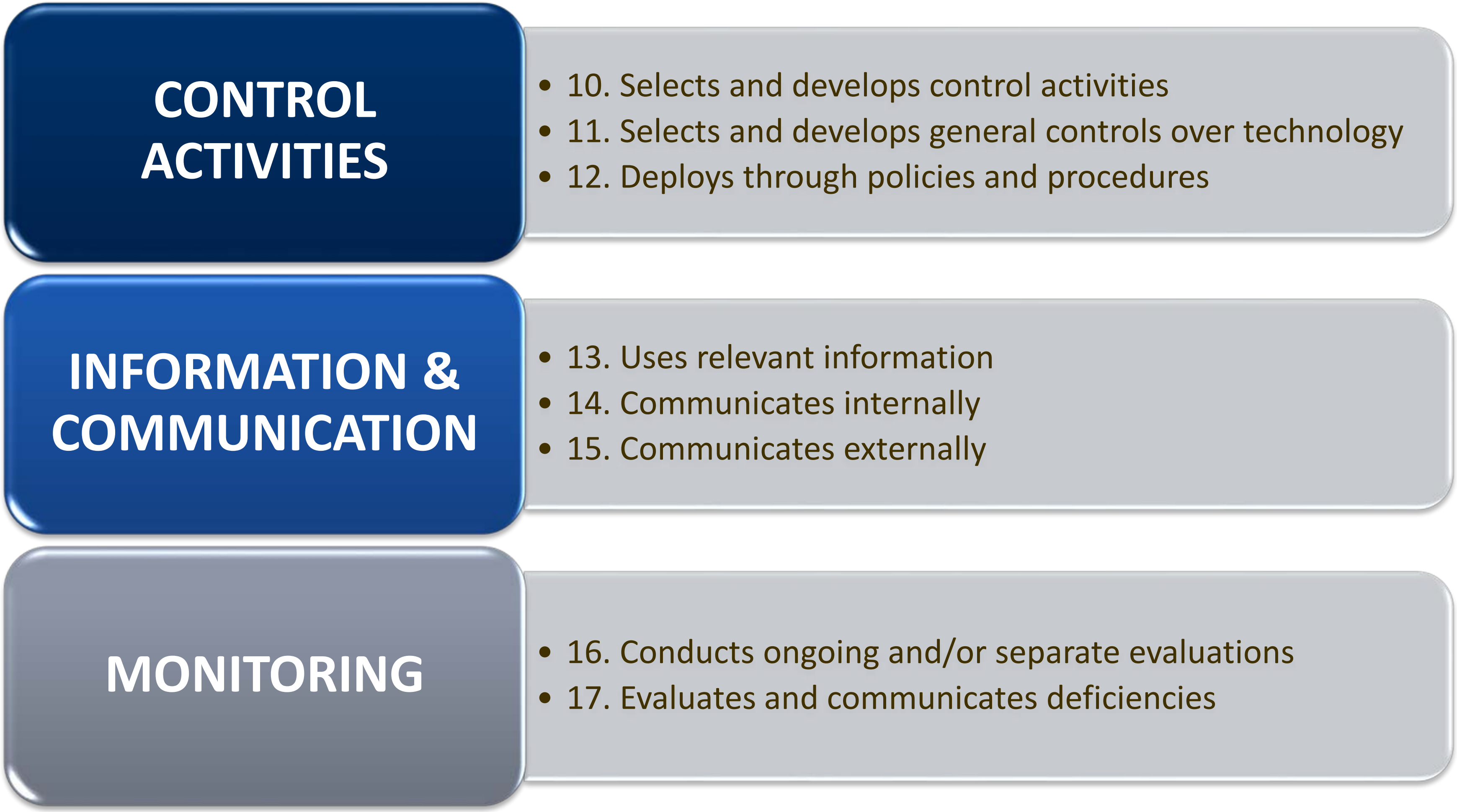
CONTROL ENVIRONMENT

- 1. Demonstrates commitment to integrity and ethical values
- 2. Exercises oversight responsibility
- 3. Establishes structure, authority, and responsibility
- 4. Demonstrates commitment to competence
- 5. Enforces accountability

RISK ASSESSMENT

- 6. Specifies suitable objectives
- 7. Identifies and analyzes risk
- 8. Assesses fraud risk
- 9. Identifies and analyzes significant change

17 Principles (Continued)



CONTROL ACTIVITIES

- 10. Selects and develops control activities
- 11. Selects and develops general controls over technology
- 12. Deploys through policies and procedures

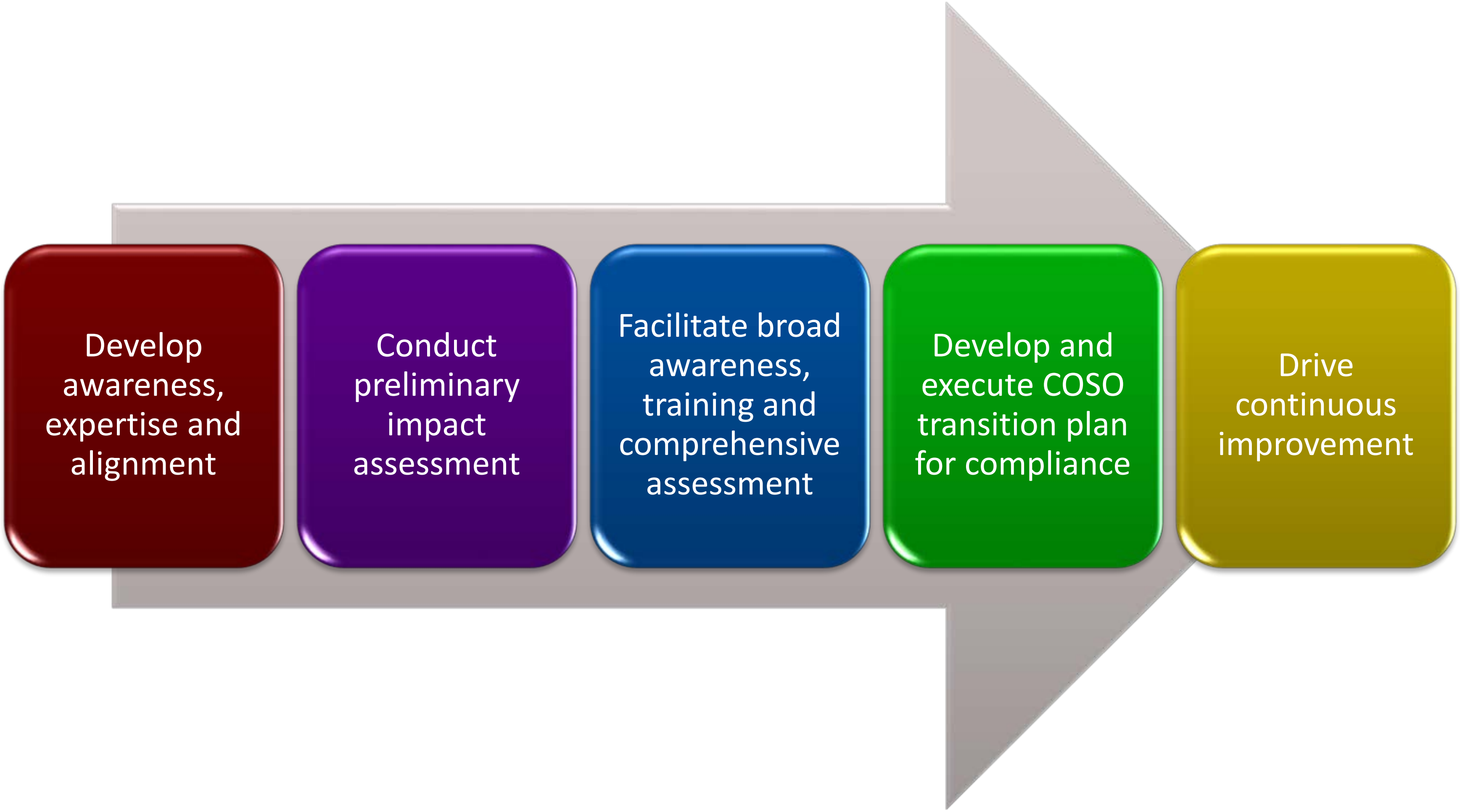
INFORMATION & COMMUNICATION

- 13. Uses relevant information
- 14. Communicates internally
- 15. Communicates externally

MONITORING

- 16. Conducts ongoing and/or separate evaluations
- 17. Evaluates and communicates deficiencies

Five Step Transition


Develop awareness, expertise and alignment

Conduct preliminary impact assessment

Facilitate broad awareness, training and comprehensive assessment

Develop and execute COSO transition plan for compliance

Drive continuous improvement

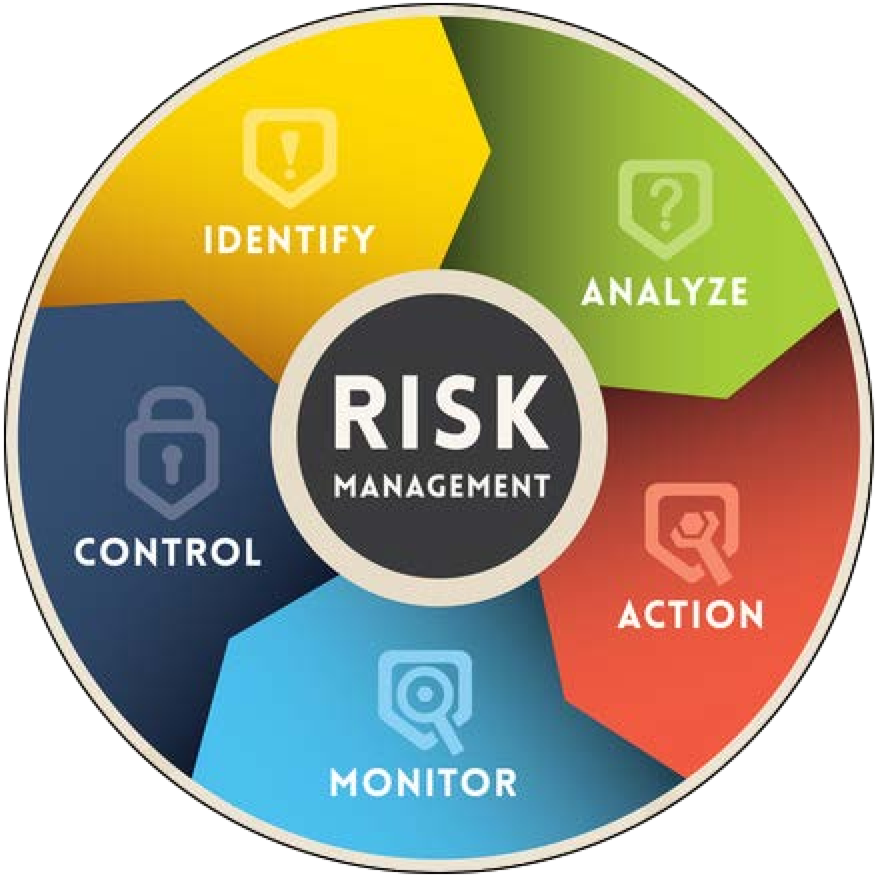
What’s Next?

Review internal control environment, policies, rules and regulations and integrate framework.

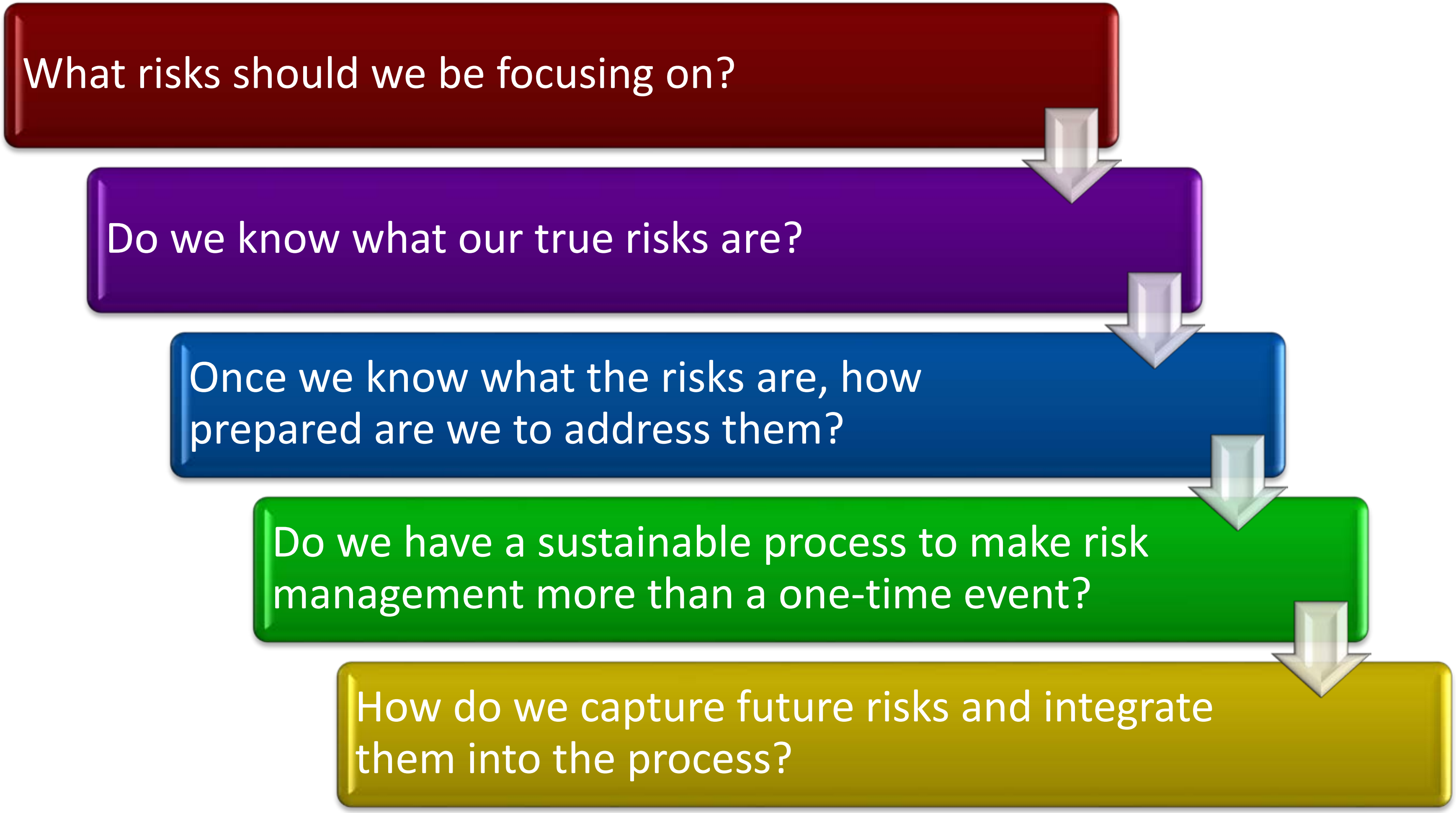
Identify and address weaknesses and gaps impacting achievement of objectives.

Perform risk management procedures.

Enterprise Risk Management



Questions Organizations Are Asking



What risks should we be focusing on?

Do we know what our true risks are?

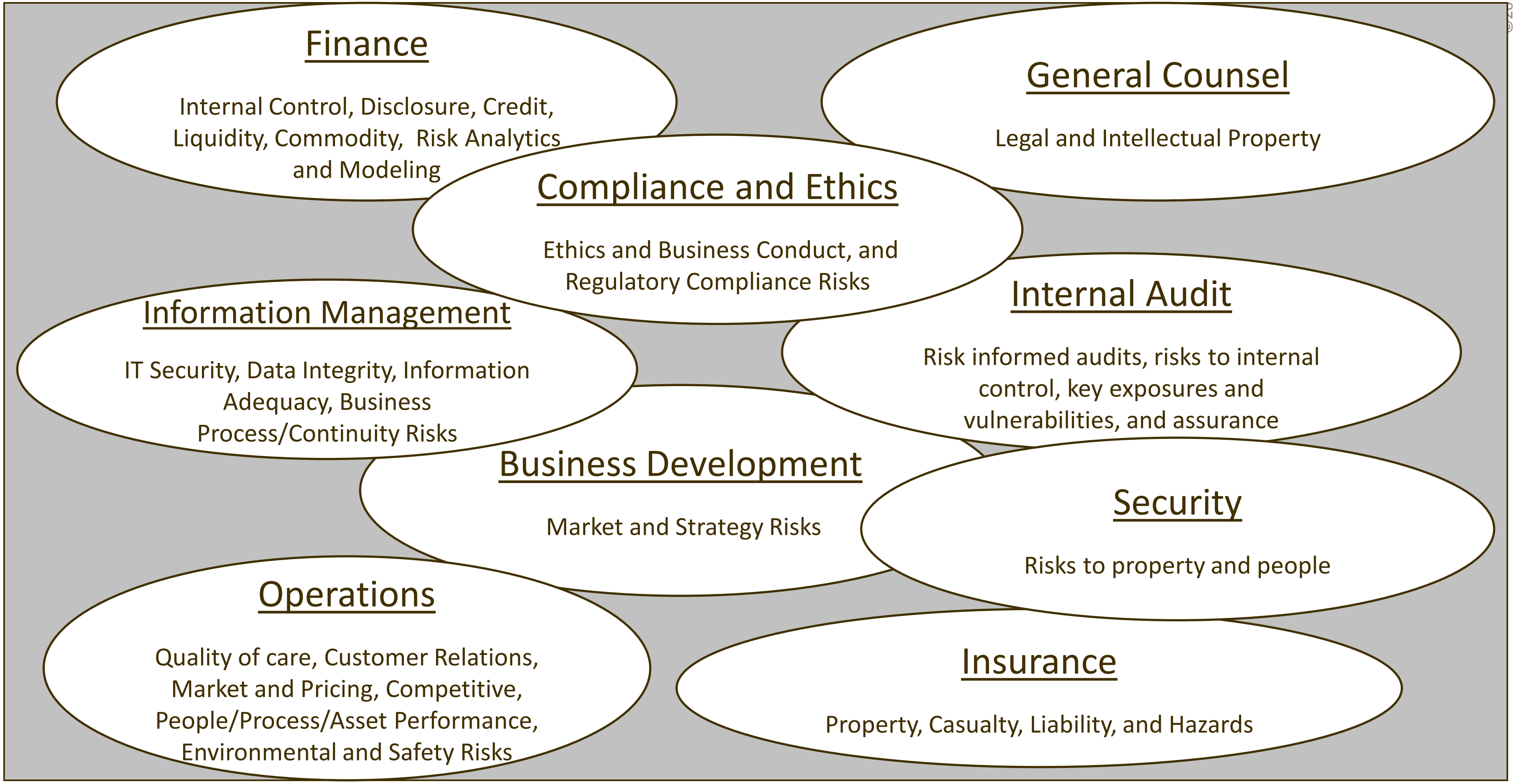
Once we know what the risks are, how prepared are we to address them?

Do we have a sustainable process to make risk management more than a one-time event?

How do we capture future risks and integrate them into the process?

Most Organizations Rely on Multiple Sources for Answers

However, risk oversight and an integrated approach is usually lacking



Finance

Internal Control, Disclosure, Credit, Liquidity, Commodity, Risk Analytics and Modeling

General Counsel

Legal and Intellectual Property

Compliance and Ethics

Ethics and Business Conduct, and Regulatory Compliance Risks

Information Management

IT Security, Data Integrity, Information Adequacy, Business Process/Continuity Risks

Internal Audit

Risk informed audits, risks to internal control, key exposures and vulnerabilities, and assurance

Business Development

Market and Strategy Risks

Security

Risks to property and people

Operations

Quality of care, Customer Relations, Market and Pricing, Competitive, People/Process/Asset Performance, Environmental and Safety Risks

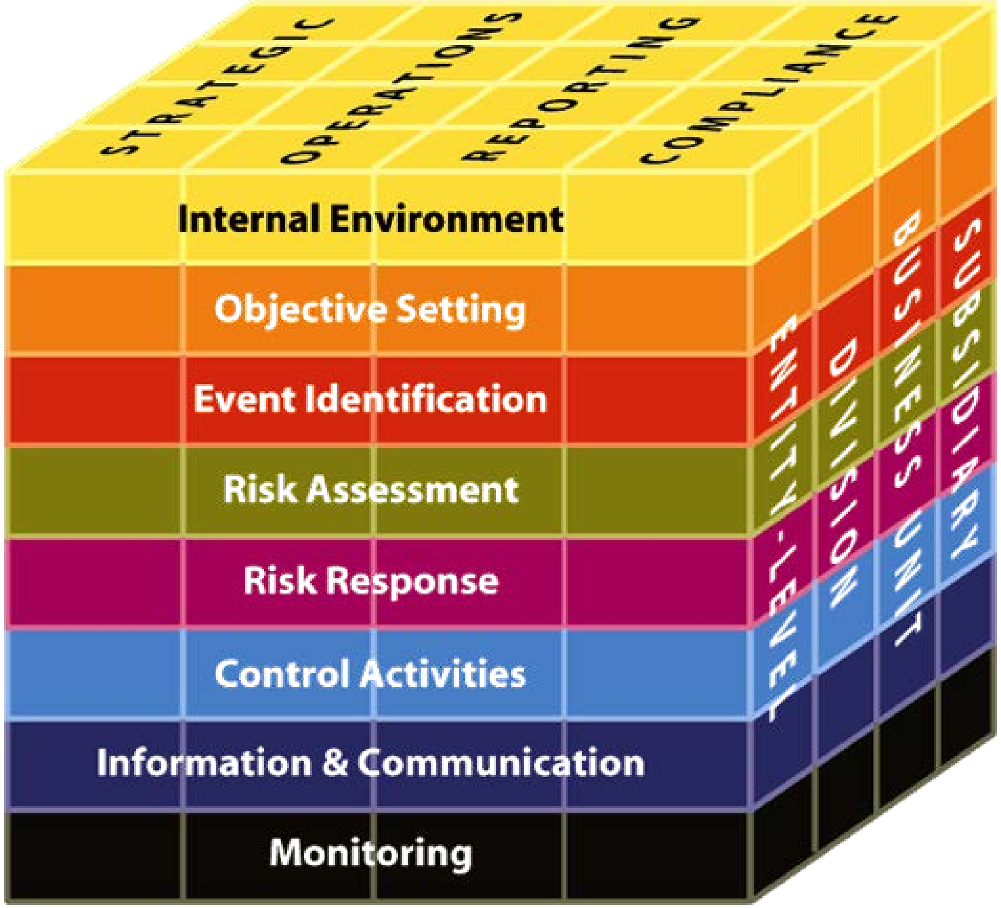
Insurance

Property, Casualty, Liability, and Hazards

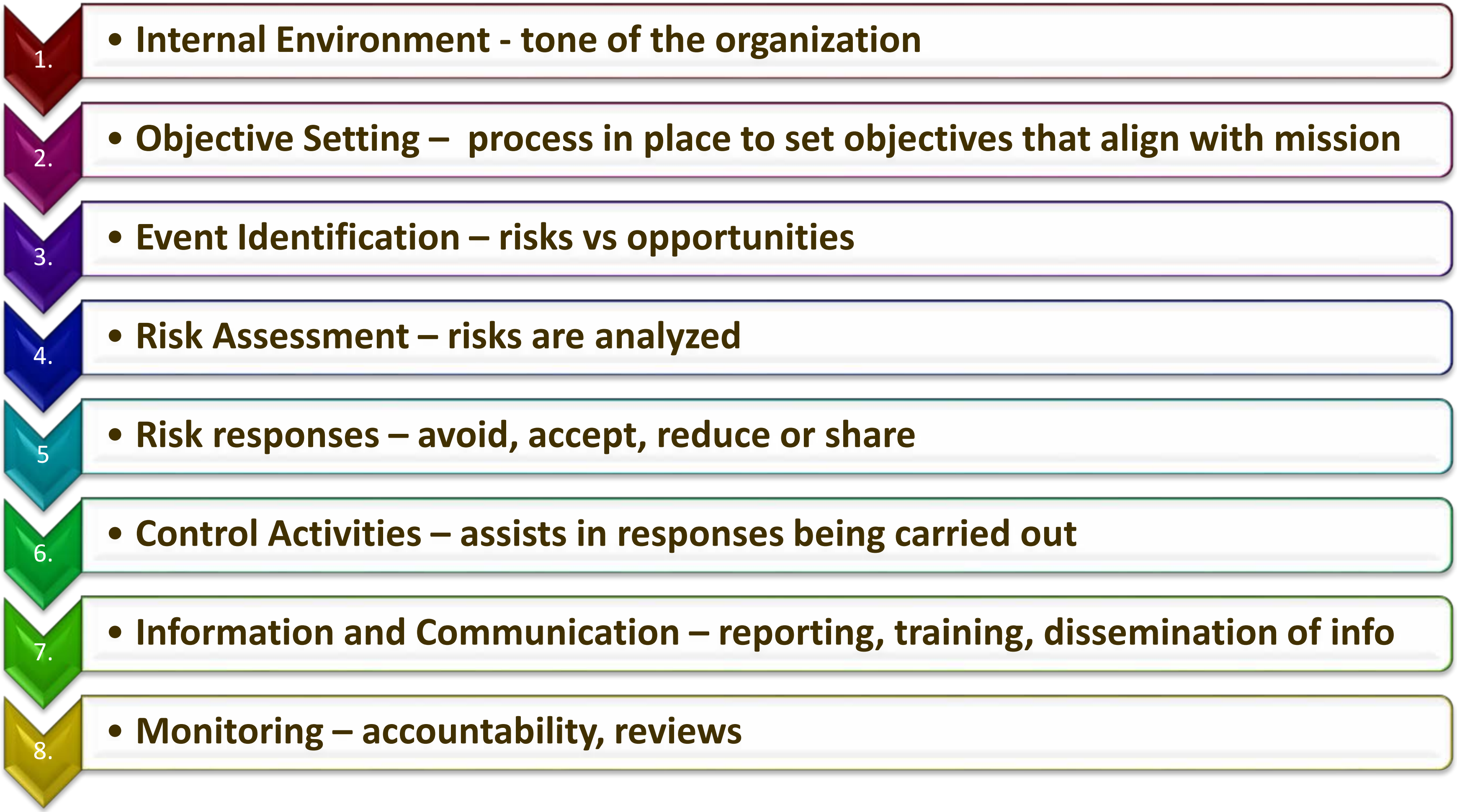
ERM provides a means to better understand, communicate, and respond to the risk knowledge that exists in the organization.

Most Popular Risk Framework

COSO integrated framework

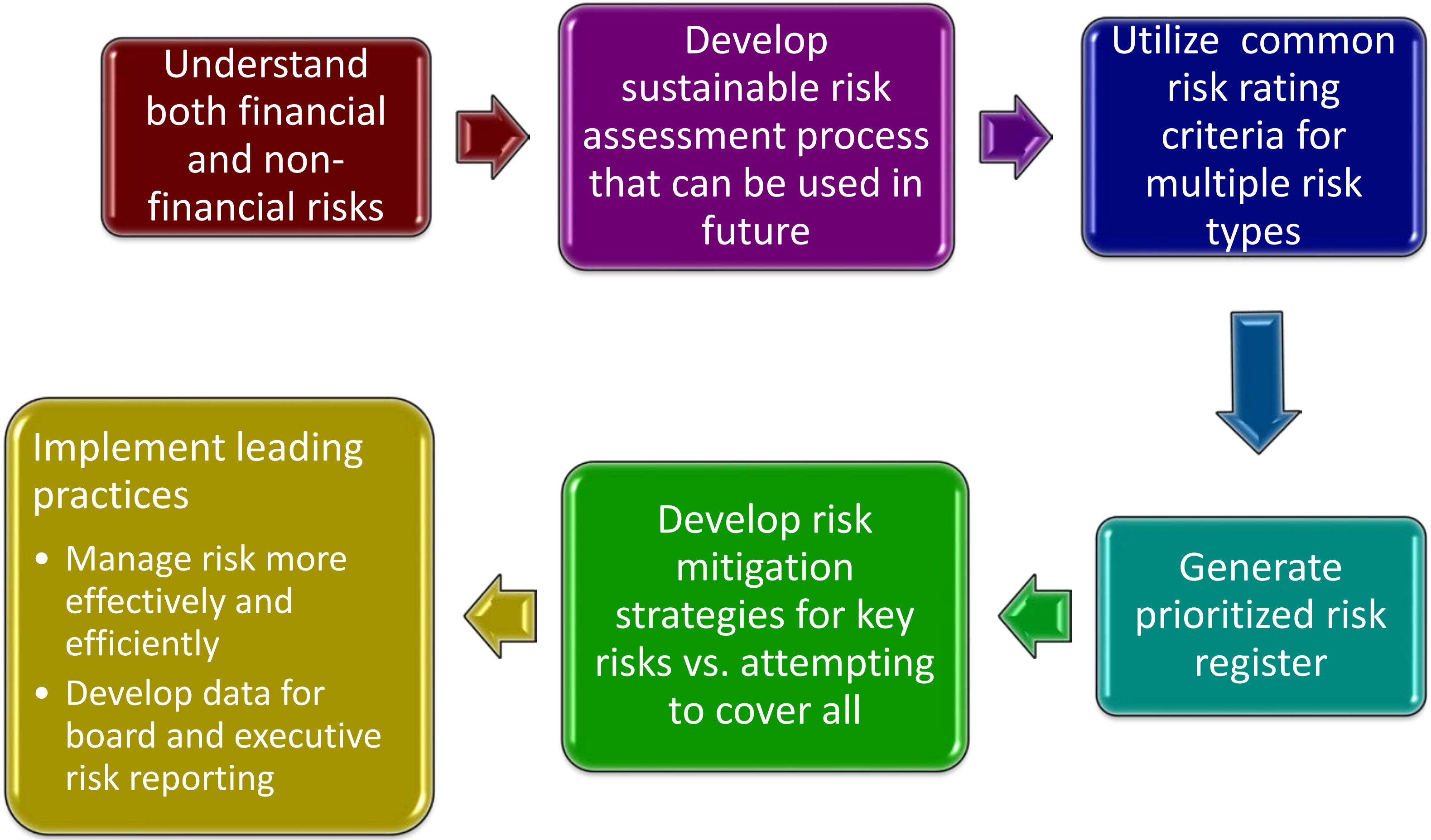


COSO ERM – Eight Interrelated Components



1. Internal Environment - tone of the organization
2. Objective Setting – process in place to set objectives that align with mission
3. Event Identification – risks vs opportunities
4. Risk Assessment – risks are analyzed
5. Risk responses – avoid, accept, reduce or share
6. Control Activities – assists in responses being carried out
7. Information and Communication – reporting, training, dissemination of info
8. Monitoring – accountability, reviews

Benefits of ERM



Understand both financial and non-financial risks

Develop sustainable risk assessment process that can be used in future

Utilize common risk rating criteria for multiple risk types

Generate prioritized risk register

Develop risk mitigation strategies for key risks vs. attempting to cover all

Implement leading practices

- Manage risk more effectively and efficiently
- Develop data for board and executive risk reporting

Example 1: Heat Map

The risk assessment process facilitates the identification of risks by rating the **Impact**, **Vulnerability** and **Speed of Onset**.

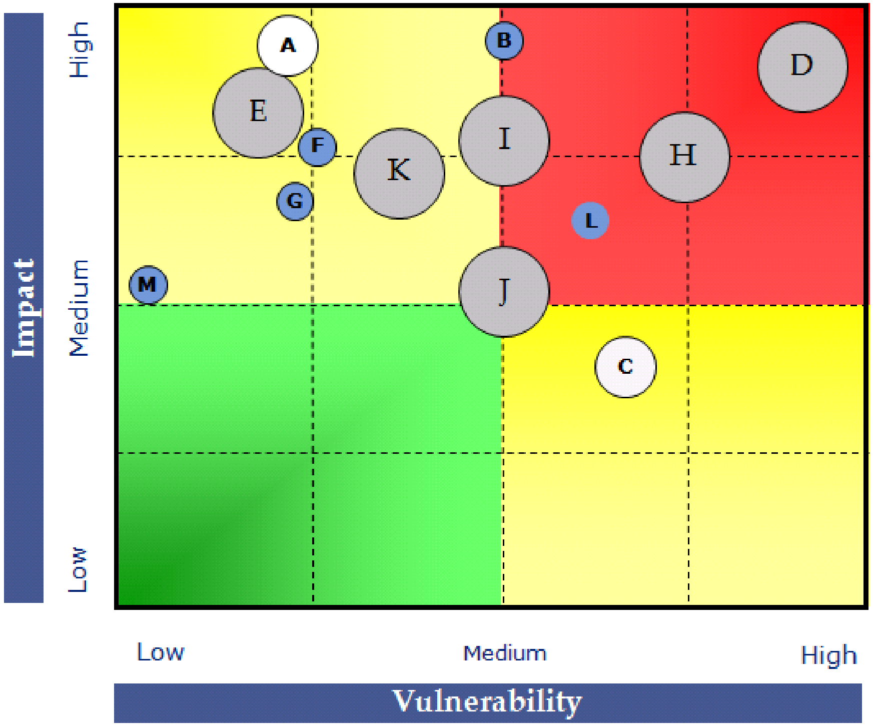
The overall types of impact of the risk can be based on multiple impact including:

Financial
Reputation
Legal/Regulatory
Customers
Employees
Operations

The overall vulnerability of the risk can be based on factors such as:

Existing controls and mitigation efforts
Risk management capability
Prior risk experience

Speed of Onset is based on how quickly the risk could occur



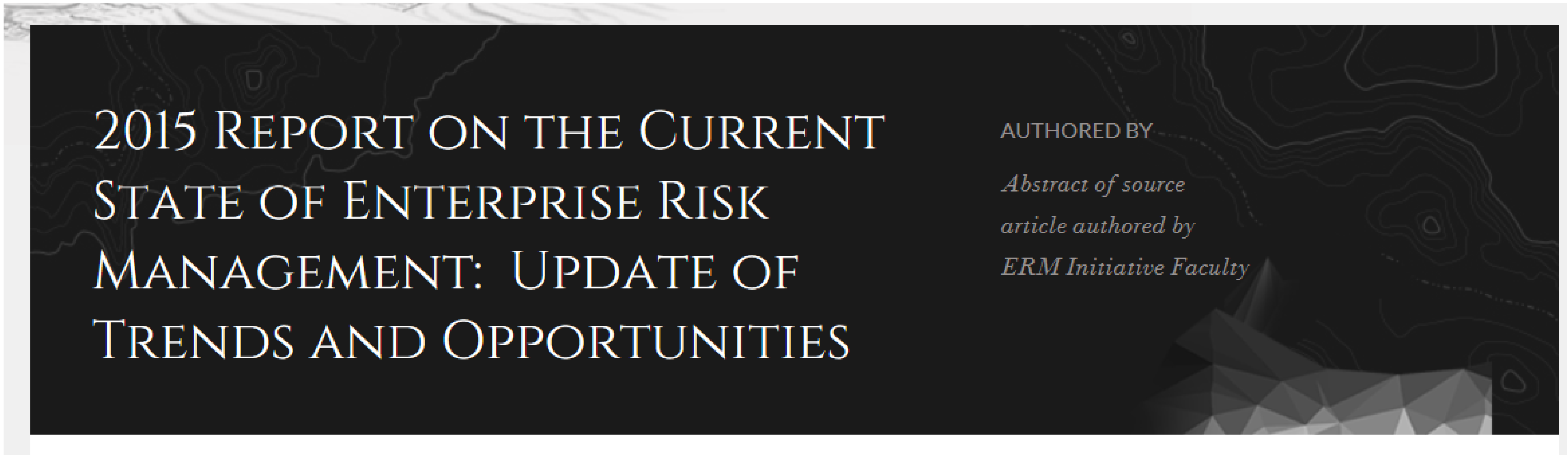
Example 2: Basic Risk Report

Risk Description	Risk Direction	Risk Response Status	Risk Owner	Status of Additional Risk Management Activities Initiated
Failure to comply with federal regulatory standards	→	🟡	Mr. Avoid	• Performing review of last 12 months of adverse compliance • Developing action plans for key trend areas identified from the review
Inaccurate billing for services	↘	🟡	Ms. Accept	• Assess customer concerns • Measure customer satisfaction
Insufficient business continuity planning	→	🔴	Mr. Reduce	• A project has been initiated to develop appropriate business continuity plans for all major operations and facilities.
Inadequate IT backup and disaster recovery processes	↗	🟡	Ms. Transfer	• Key steps have been completed to improve IT BCM: consolidated and improved the data center, documented processes, and retrained personnel.

ERM - Everyone is Involved

- Board
  - Discuss state of ERM and provide oversight.
  - Be apprised of the most significant risks.
- Senior Management
  - Chief executive assesses the risk management capabilities.
    - ◊ Internal lead?
    - ◊ Hire external?
  - Others
    - ◊ Lead Project or
    - ◊ Provide vital input
- Other Personnel
  - Discuss how they are conducting their responsibilities
  - Discuss ideas for strengthening ERM

Current State of ERM



2015 Report on the Current State of Enterprise Risk Management: Update of Trends and Opportunities

AUTHORED BY

Abstract of source article authored by ERM Initiative Faculty

Key Findings

59%: Volume and Complexity of risks have changed extensively in last 5 years

65%: Admitted they were caught off guard by an operational surprise.

25%: Complete and formal enterprise risk management process in place.

- Same as prior year.
- Larger organizations more likely

68%: Board is asking for increased senior executive involvement in risk oversight.

Key Findings

65%: Experience pressure from external parties to provide information on risks.

32%: Have a chief risk officer

42%: Barrier to ERM is seen as a competing priority

How to Get Started

Risk is like fire: If controlled it will help you; if uncontrolled it will rise up and destroy you.

Theodore Roosevelt

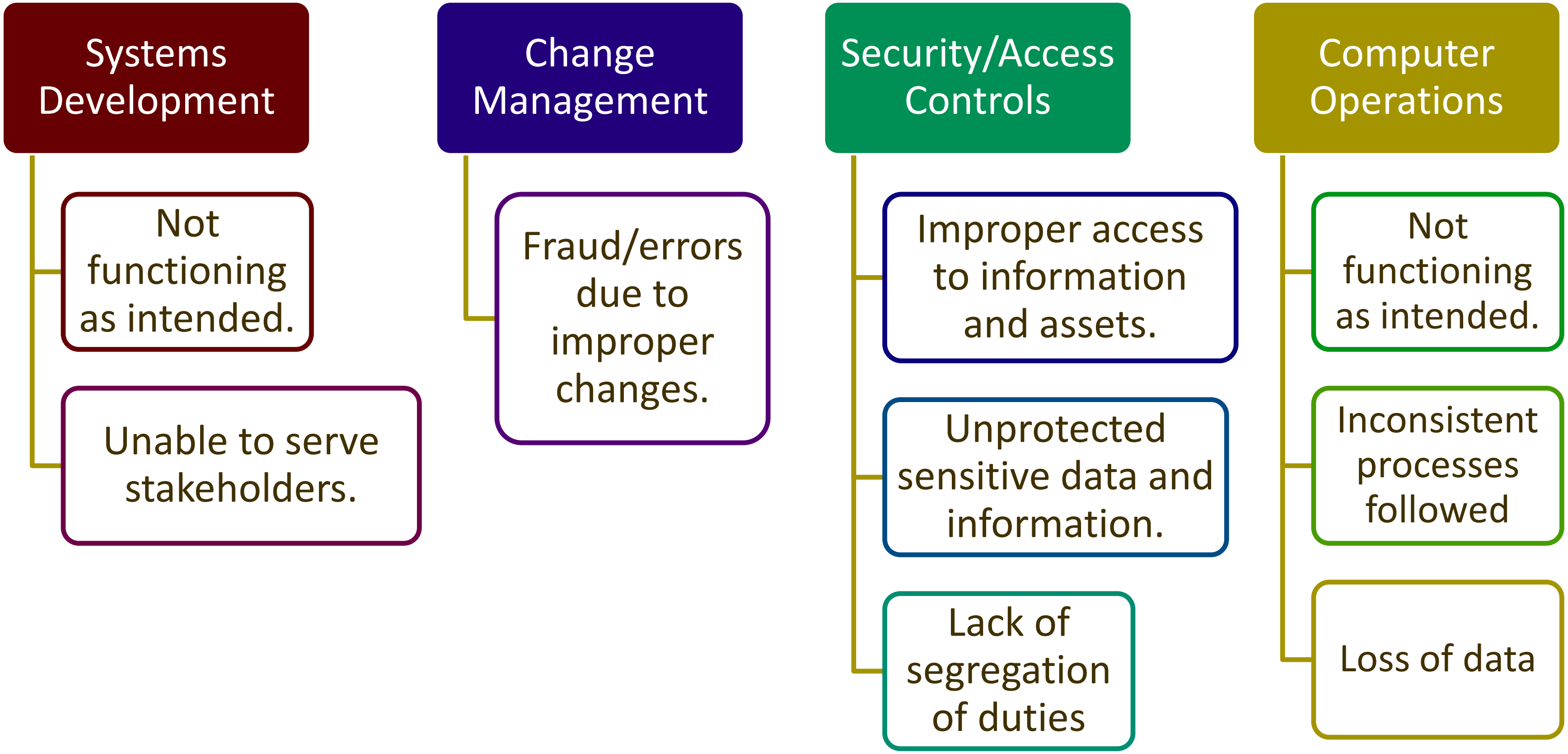
Internal Controls in an Automated Environment

Change in the Control Landscape

IT General Controls (ITGC) – What You Need to Know

- Includes:
  - Systems Development
  - Change Management
  - Security/Access Controls
  - Computer Operations
- To ensure the effective functioning of application controls.
- Ensure the continued proper operation of information systems.

ITGC's – Your Risks



Systems Development
- Not functioning as intended.
- Unable to serve stakeholders.

Change Management
- Fraud/errors due to improper changes.

Security/Access Controls
- Improper access to information and assets.
- Unprotected sensitive data and information.
- Lack of segregation of duties

Computer Operations
- Not functioning as intended.
- Inconsistent processes followed
- Loss of data

What Should You Be Doing?

Understand controls over:

- Appropriateness of User Rights
- Segregation of Duties
- Password Parameters
- Physical/Environmental
- End User Controls over Reports
- User Access Administration (internal and external)
- New Systems testing.
- Changes approved and tested
- Network security.

Identify holes and implement manual controls / reviews.

Have an ITGC/Security review to identify issues

Emphasize to organization the importance of ITGCs.

Segregation of Duties

Automated controls need segregation in same fashion as manual controls.

- Who has access to specific databases and functions?
- Can one individual perform all functions for a specific process?
- Do the right users have the right access for their job?
- What controls are in place to ensure proper SOD?

Example IT Access Testing

Financial Reporting

- Add/Change/Delete Chart of Accounts
- Open/Close Periods
- Post Journal Entries

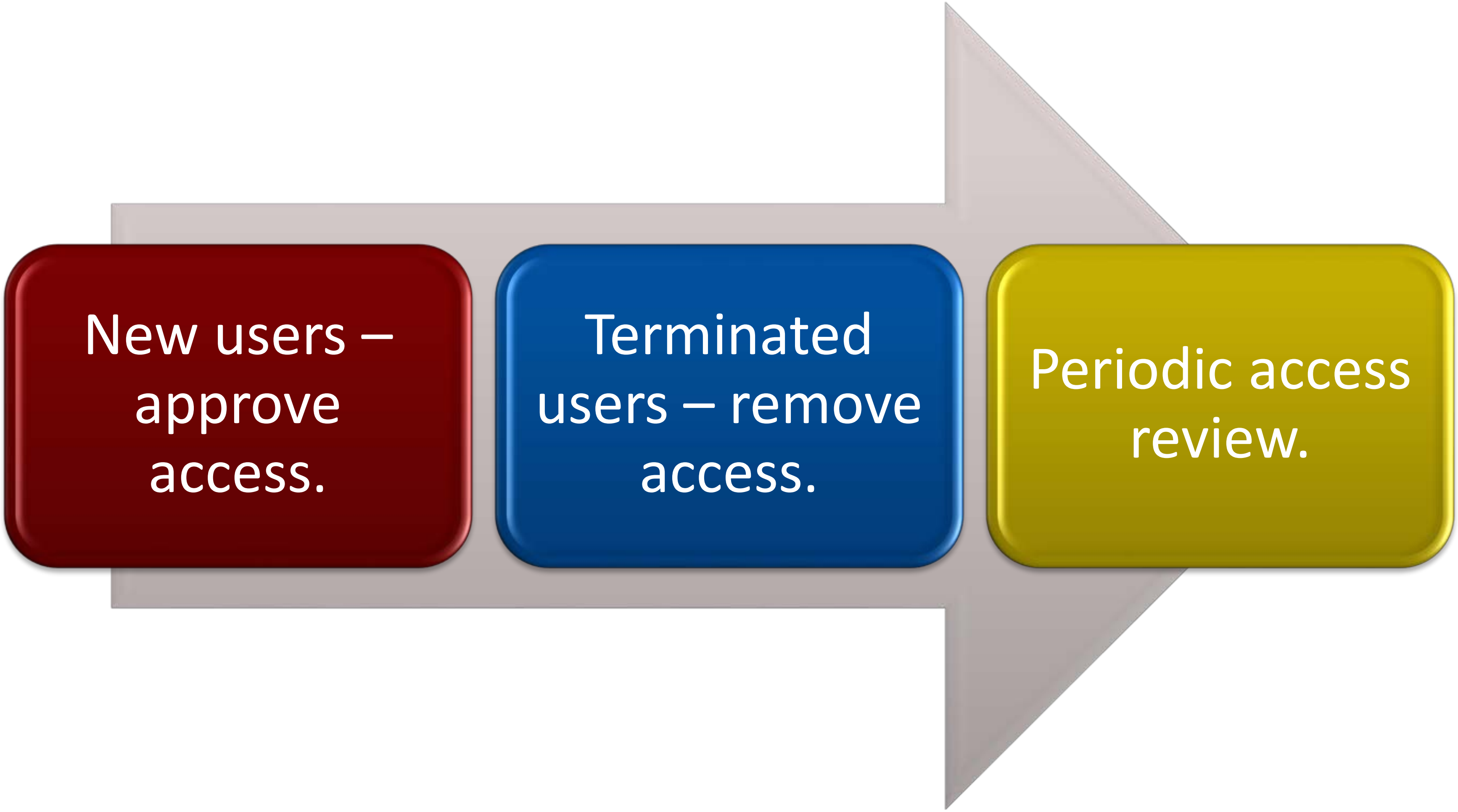
General Disbursements

- Add Vendor
- Input an Invoice/Approve an Invoice
- Process Payment to Vendor

Payroll

- Add-Change-Delete Employees
- Setup Payment Method/Establish Pay Rates
- Process Payroll/Update Paid-Time Off Accrual Thresholds

What Should You Be Doing?

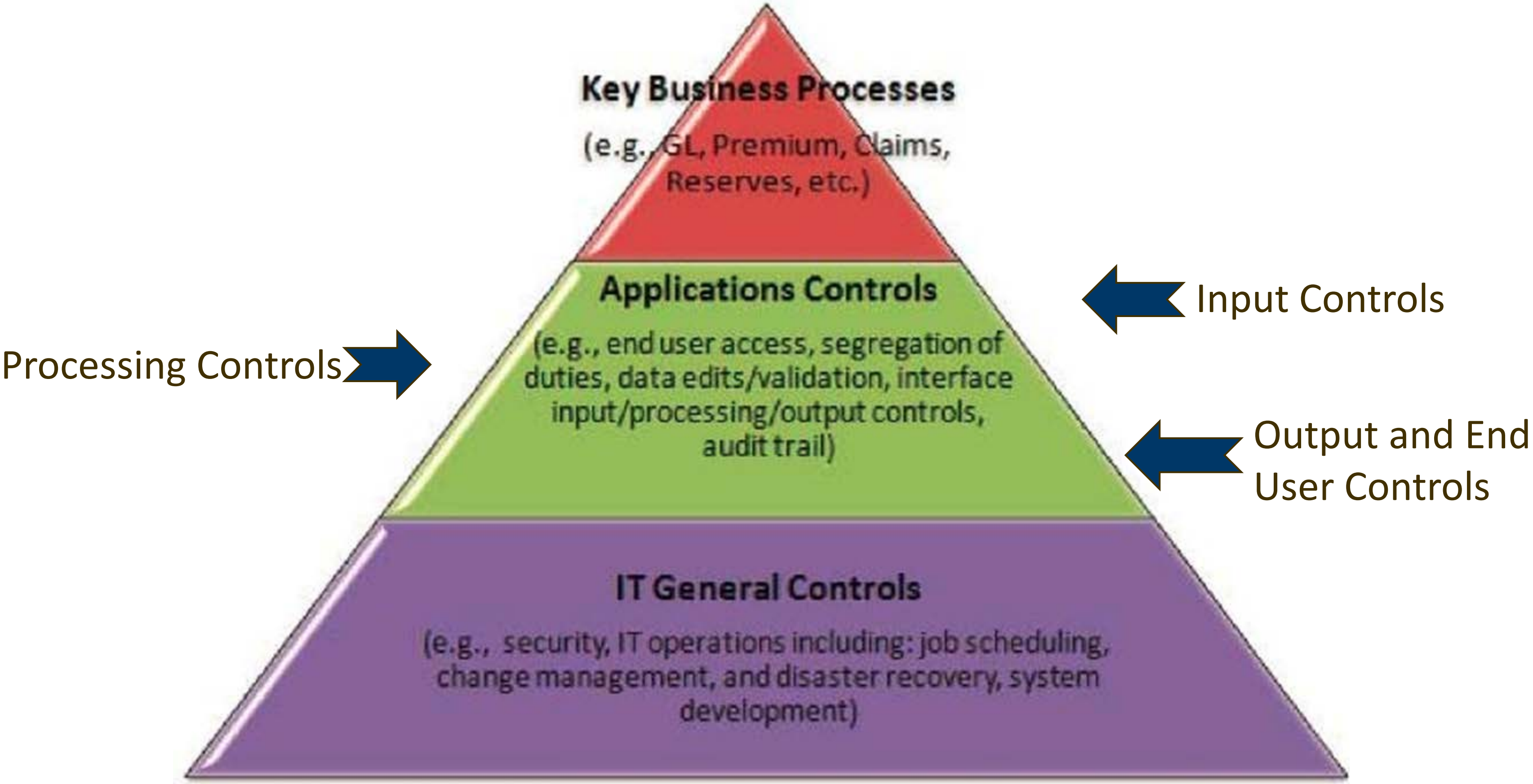


New users – approve access.

Terminated users – remove access.

Periodic access review.

Application Level Controls


Key Business Processes
(e.g., GL, Premium, Claims, Reserves, etc.)
Applications Controls
(e.g., end user access, segregation of duties, data edits/validation, interface input/processing/output controls, audit trail)
IT General Controls
(e.g., security, IT operations including: job scheduling, change management, and disaster recovery, system development)
Processing Controls
Input Controls
Output and End User Controls

Input Controls

Edit Check (Numeric field; Alphabetic field; Alphanumeric field; Valid code; Reasonableness; Completeness)

Input Authorization (Signature, form, online access control)

Batch control (total monetary amount, total items, hash totals, manual reconciliation)

Error Reporting (rejected transactions)

Processing Controls

Data Validation

- Edit checks, such as:
  - Transactions exceeding a specific dollar amount for additional approval
  - 3-way matching
  - Duplicate check, completeness

Processing checks (business rules)

Compliance controls

- Example: Student Financial Aid
  - Eligibility and Disbursement of Aid

Output and End User Controls

Control over how information is distributed to appropriate recipient (confidentiality).

Controls over access to spreadsheets or other output from systems should be in place to provide reasonable assurance the data is complete and accurate.

Access to formulas should be restricted, files should be password protected, reconciliations to source data should be performed.

How Our World Has Changed

- Approvals – no longer on paper.
  - Audit trail for approval process?
- Reliance upon system generated reports.
  - How is accuracy ensured?
- Information automatically fed to GL
  - Information getting to GL completely and accurately?
- Recording of Time Worked
  - How do you prevent employees recording false data?

Allison Slife, CPA
CliftonLarsonAllen LLP
Manager, State and Local Government
303-439-6018
Allison.Slife@CLAconnect.com

CLAconnect.com

CliftonLarsonAllen

linkedin.com/company/
cliftonlarsonallen

facebook.com/
cliftonlarsonallen

twitter.com/CLAconnect