WECC

Internal Controls 101 and Third-Party Risk Management

Molly Elliott
Senior Technical Analyst, Oversight Planning

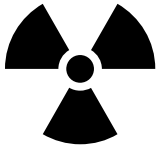
Greg Nance
Staff Risk Assessment Engineer, CIP

Michael Shaw
Enforcement Risk Assessment & Mitigation Engineer, Staff

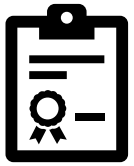
Electric Reliability & Security for the West

What is Internal Control?

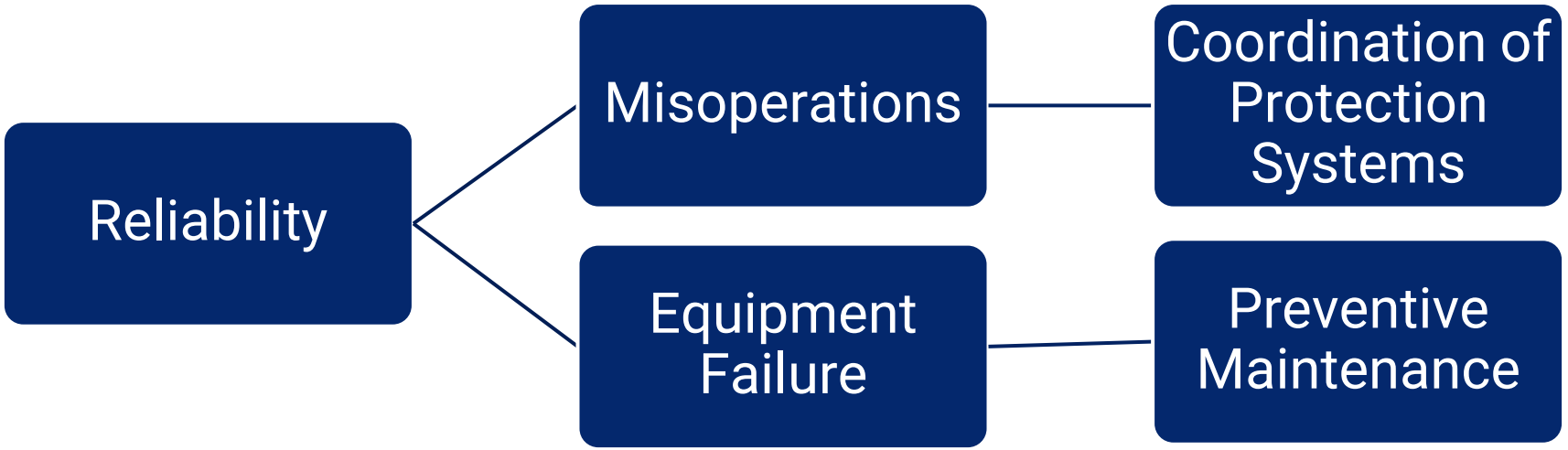
Objective



Risk



Controls



Internal Controls Framework — Simplified

Control Environment

Culture of Compliance

Thoughtful governance and oversight model

Clear separation of responsibilities and accountability

Risk Assessment

Ability to document **your** specific risk to the BES

Ability to document **your** specific operational and security risk

Thoughtful program to abate risk and measure efficacy

Control Activities

Match controls to risks (compliance vs. operations vs. security)

Controls have clarity of purpose (preventive vs. detective)

Controls and process are one and the same

Information & Communication

Holistic internal communication (training, awareness, coordination, projects, etc.)

Holistic external communication (coordination with other entities, WECC, vendors, etc.)

Information is good and current

Monitoring Activities

Internal monitoring and/or audits

Good investigations for when things go wrong

Document failures **and** near-misses through to completion of risk mitigation

Control Environment

Commitment to integrity and ethical values

Oversight of the entity's internal control system

Establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives

Commitment to recruit, develop, and retain competent individuals

Evaluate performance and hold individuals accountable for their internal control responsibilities

Control Environment

Control Environment

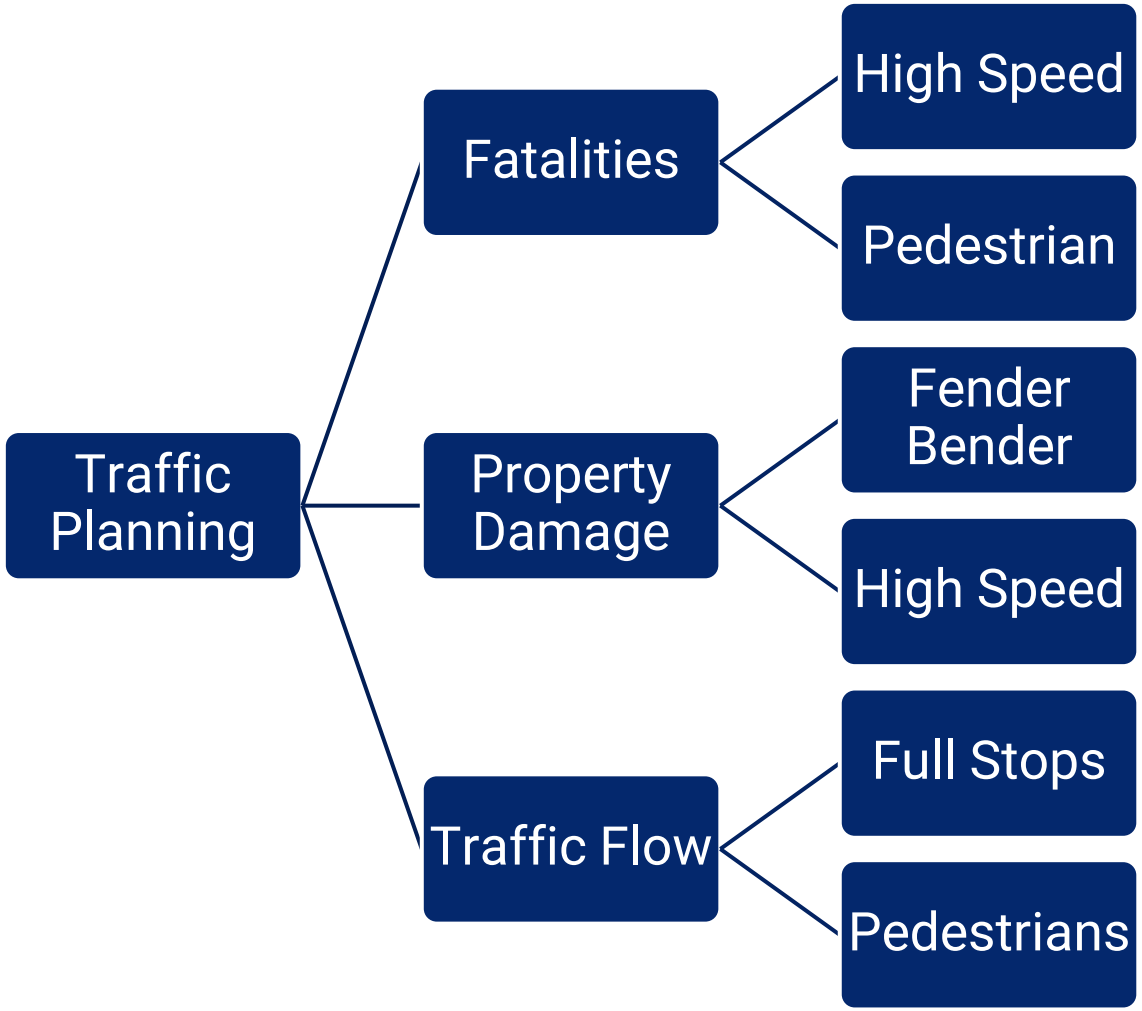
Where to start

- Get to know the business
- Use your position to improve communication between business units
- Focus on nurturing a corporate culture that emphasizes the things that matter — hiring, training, communication

Where to aim

- Add measurement that feeds into improvement programs
- Revise structures and add tools to foster learning between departments and break down silos
- Track improvement efforts

Risk Assessment



Risk Assessment

Where to start

- Enterprise Risk Management (If you have it)
- ERO Enterprise resources
- Other industry resources

Where to aim

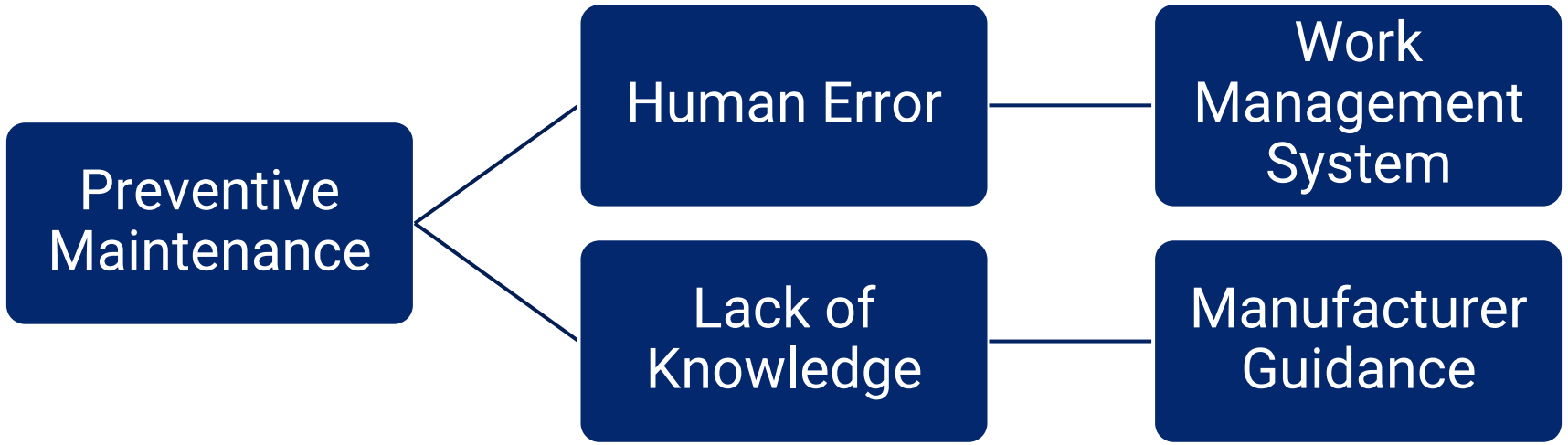
- Risk register
- Objectives are defined in measurable terms
- Understanding of the system and awareness of impact on the system (e.g., Aggregate Risk)
- Risk monitoring and continuous improvement (triggered, periodic, ongoing)

Control Activities

Control Objective

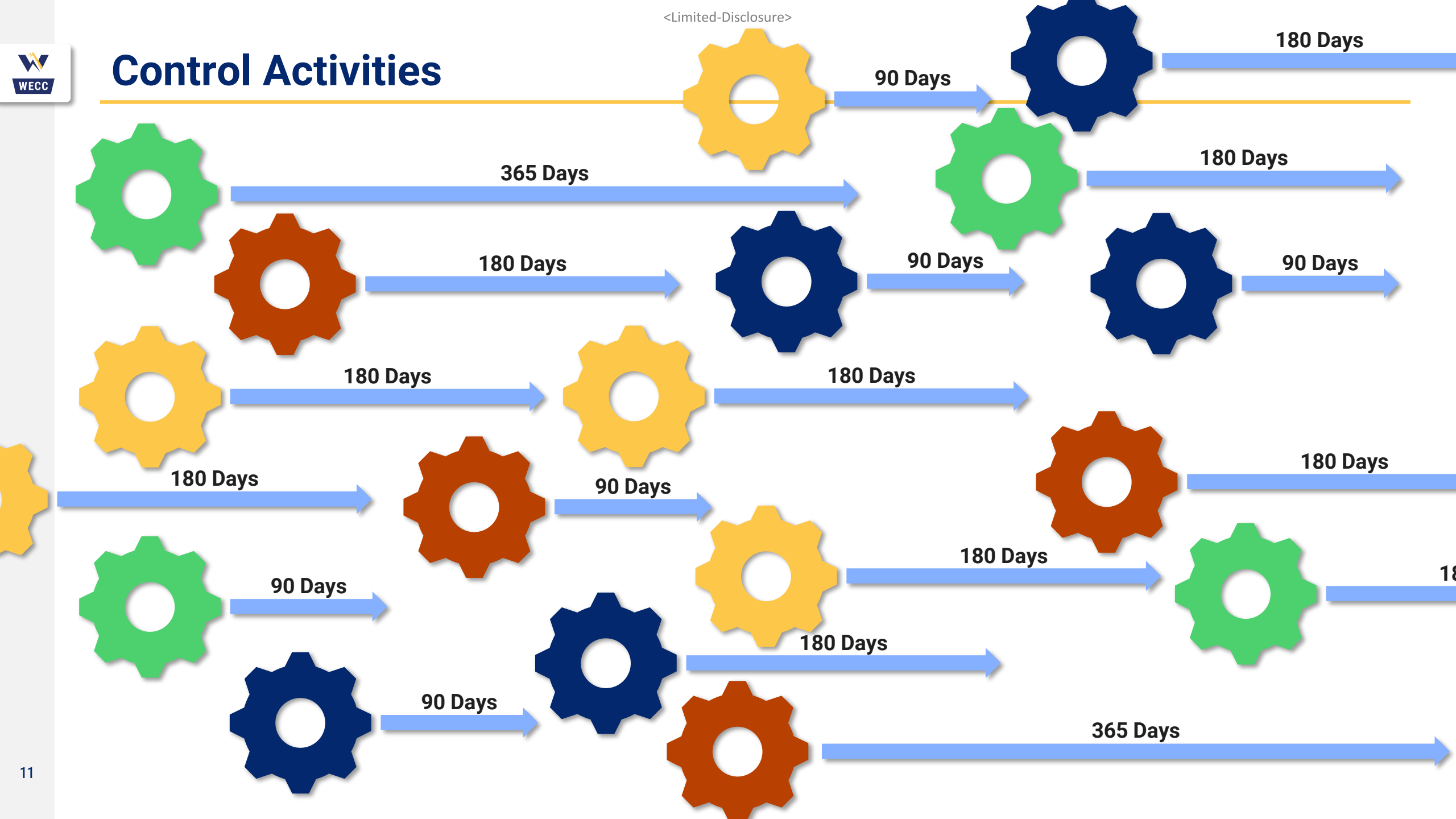
Risk

Control Activity



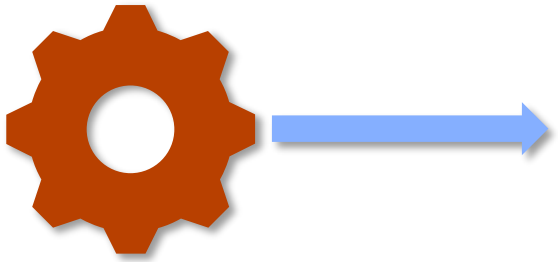
Control Activities

Control Activities



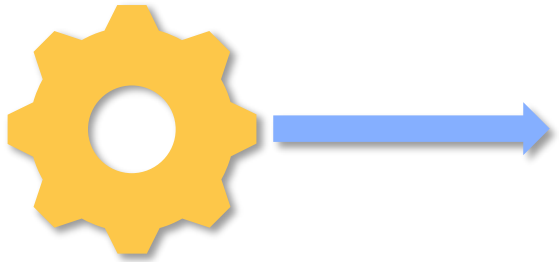
Control Activities

Forced Outage Widgets



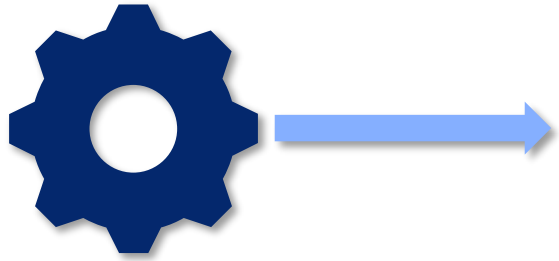
40 Widgets

Construction Widgets



100 Widgets

Staffing/Other Issue Widgets

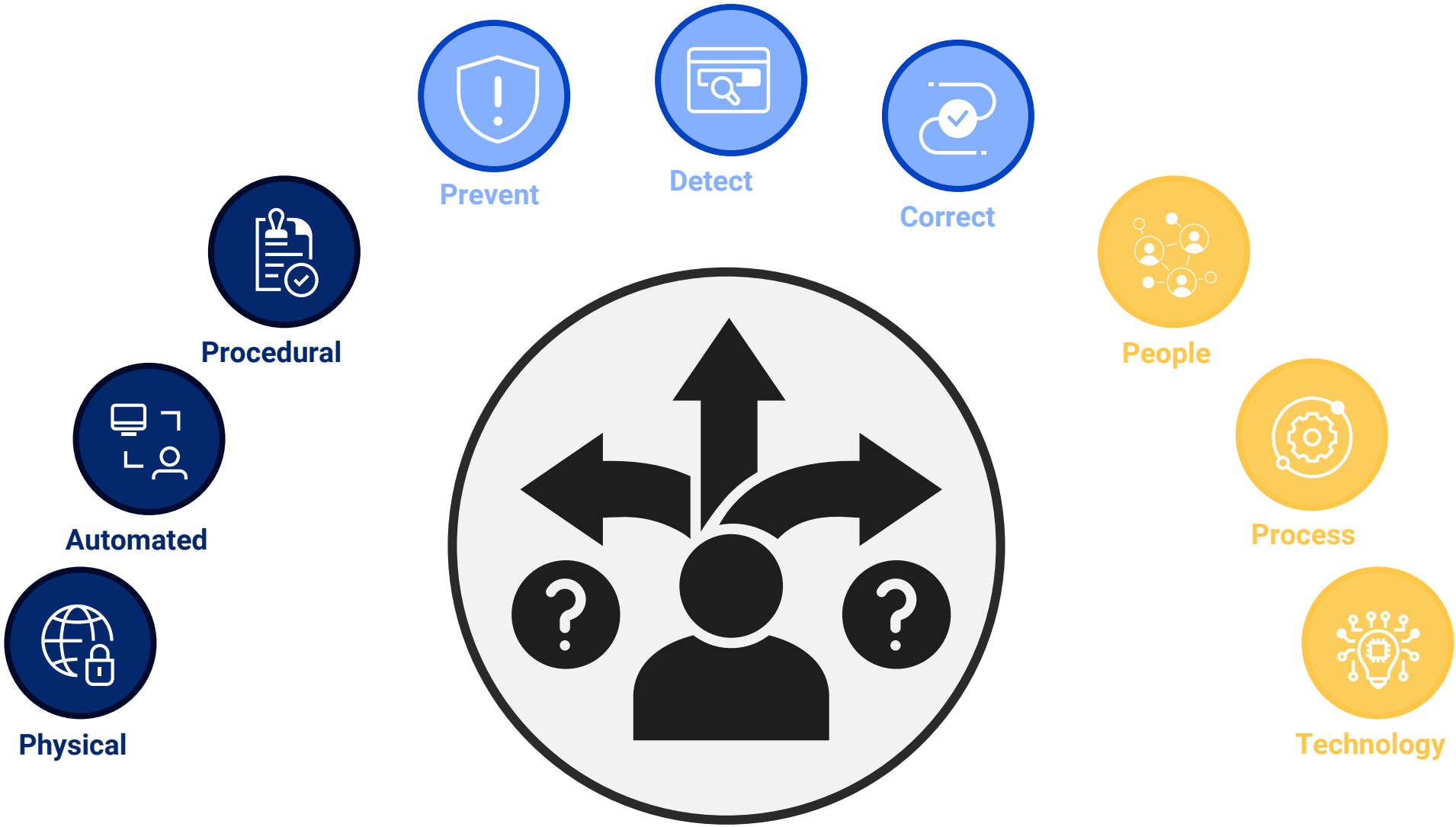


75 Widgets

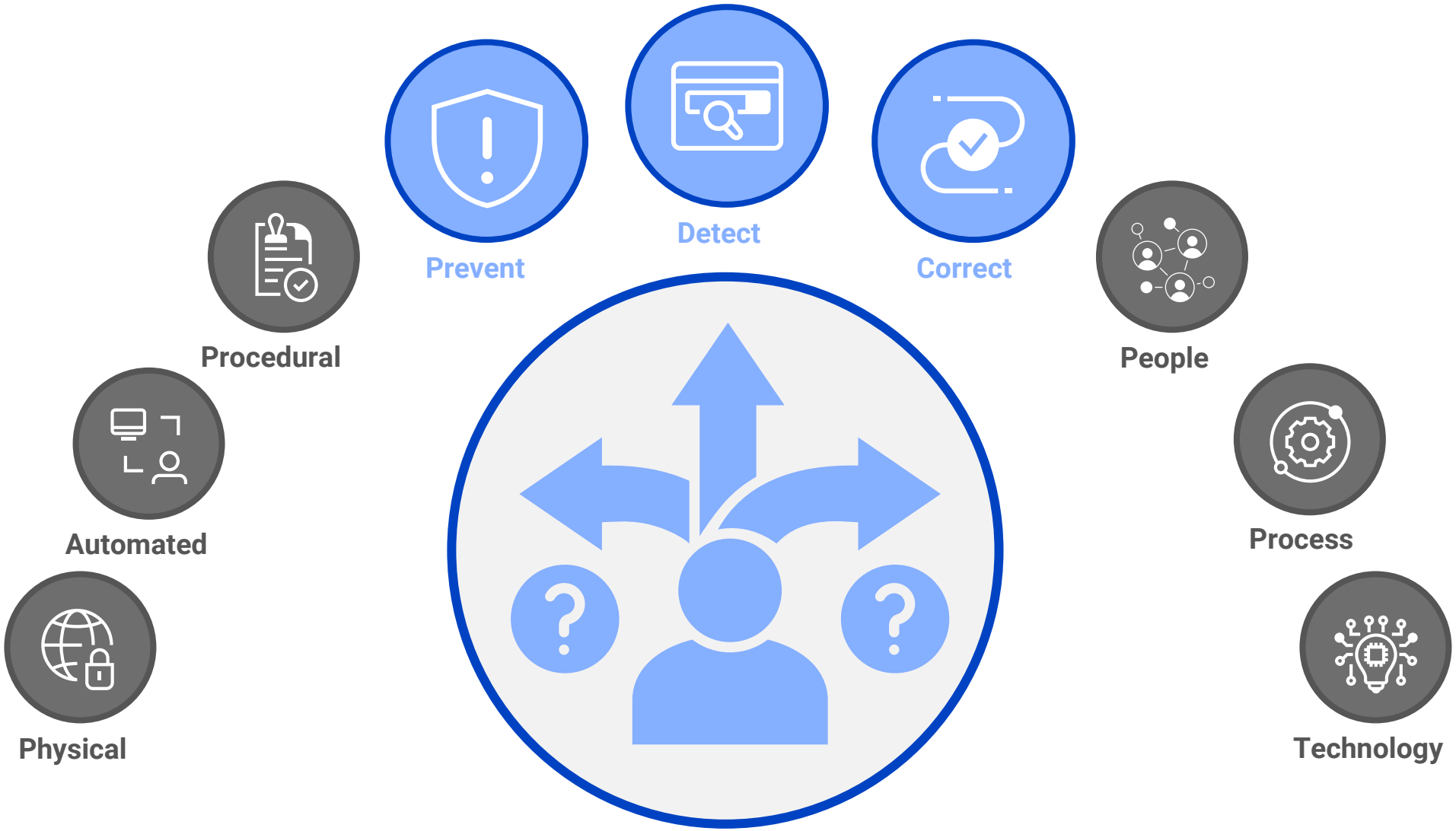
Properly Accounted for and on Track Widgets

19,785 Widgets

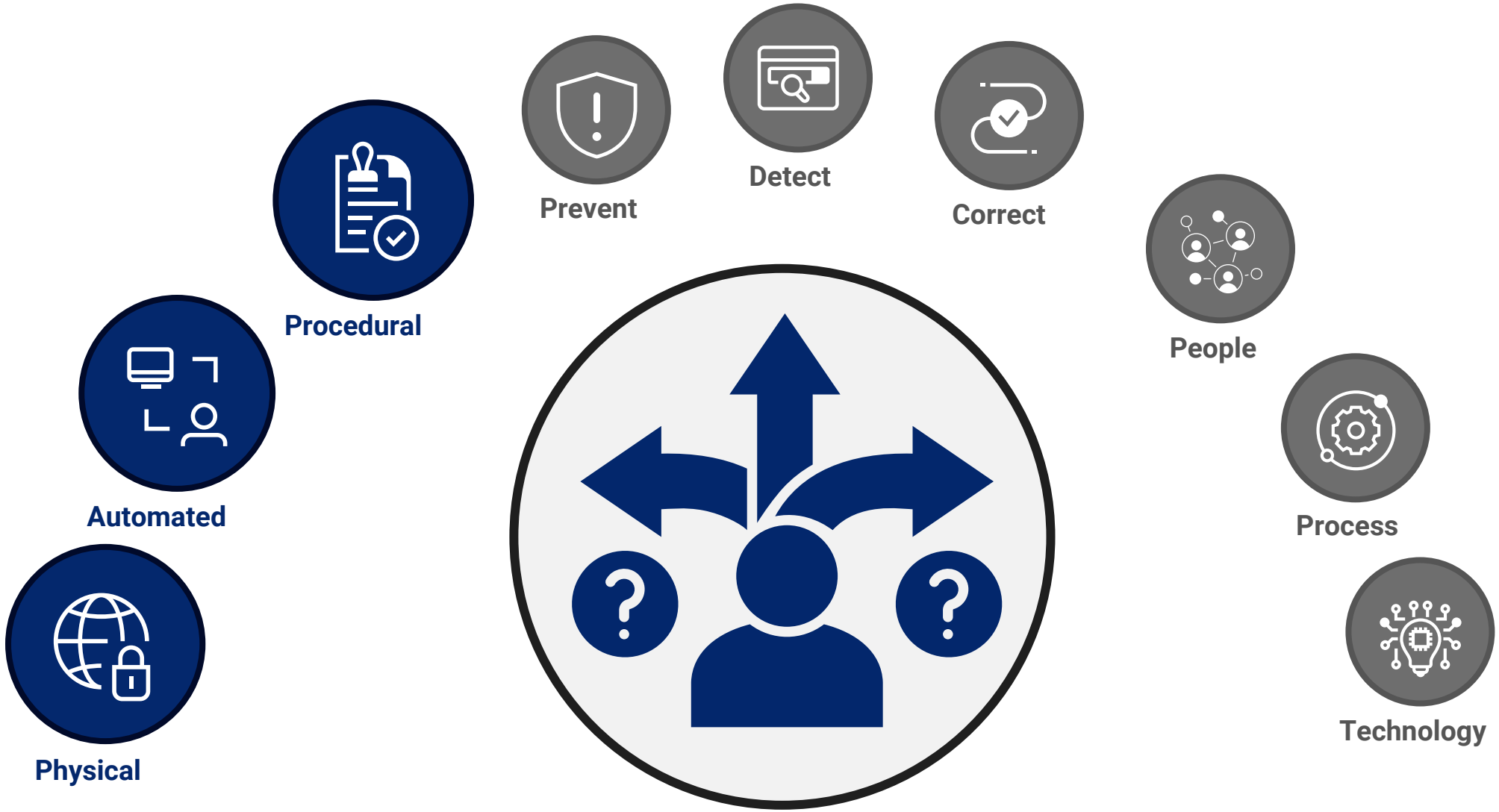
Control Activities



Control Activities



Selecting Controls



Selecting Controls

What kind of control is this?

Objective: Prevent Intrusion by Bad Actor

Fence	Security Guard	Sign-in Sheet
• Prevent • Physical • Technology	• Prevent or Detect or Correct • Procedural • People	• Prevent or Deter or Detect • Procedural • Process

Automated Controls

Higher Accuracy and Quality: Automation ensures consistency and precision, significantly lowering the potential for human error.

Real-time Management: Transition organizations from "point-in-time" snapshots to real-time visibility of their security posture and operations. This can allow for immediate, automated responses to issues.

Compliance Readiness: Automated systems can provide reliable, standard processes with built-in audit trails, ensuring adherence to regulations.

Scalability: Assist with managing expanding IT/OT environments without proportional increases in staff, costs, or errors.

Automated Controls

Target the most resource-intensive risks

- Asset/Data Management
- Access Control
- Incident Response
- Configuration Management
- Internal Security Monitoring

Ensure automation tool(s) is implemented based on “solid” policies, procedures, and processes. Avoid (GIGO), “Garbage in, garbage out”.

- Document in detail what tasks the automation tool is performing.
- Ensure strong procedures regarding manual interfaces.
- Visuals (e.g., flow charts, tables, etc.)

Procedural Controls

Procedures mitigate a risk: Lack of knowledge

- Inconsistency
- Absences
- Turnover

Benefits

- Inexpensive and easy to implement
- Track process changes and exceptions
- Support processes that are performed infrequently

Procedural Controls — What's Missing?

Pignoli

Ingredients

- 2 cans almond paste
- 2 egg whites
- 1 cup sugar
- powdered sugar
- egg white
- pine nuts

Directions

- Bake at 350° for 15 minutes

Procedural Controls — What's Missing?

Purpose: How many cookies am I making?

Incomplete information / tribal knowledge:

- What size is the can of almond paste?
- Which brand?

Step-by-step instructions:

- Blend the almond paste, sugar, and egg whites in a double boiler
- Remove from heat and cool
- Knead on board sprinkled with powdered sugar
- Third egg white is brushed on the cookie before rolling in pine nuts
- Refrigerate before shaping
- Bake on parchment paper

Layering Controls

- Procedural controls alone:
  - Easy to circumvent
  - Susceptible to human error
  - May not produce enough evidence to monitor the process

Common Control Activities

	Prevent	Detect	Correct
People	Training, communication, coordination	Peer review, manager review, performance review	Disciplinary actions, remedial training
Process	Segregation of duties, action plans, checklists, triggers, identification/scoping, change authorization	Spot checks, internal audits, inventory counts, field walkthroughs	Business continuity plans, updated policies and procedures, corrective action plans
Technology	Access controls, firewalls, fence, Locks	Alarms, alerts, reconciliations, data integrity checks, monitoring	Patching, backups

Information and Communication

- At the organizational level
  - Reporting to decision-makers
  - Understanding corporate goals
  - External communication
- At the process level
  - Training
  - Information flow between business units
  - Process coordination with relevant stakeholders
- Support corporate objectives and continuous improvement

Monitoring

Look for Indicators

- Frequency of errors/events
- High level of rework
- Length of time it takes to find issue
- Repeated root cause
- Performance vs. others

Periodic Assessment

- Have the risks changed?
- Are the risks sufficiently mitigated?

Monitoring Internal Controls

Monitoring is the structural backbone for compliance.

"Old Way" of monitoring

- Retrospective
- Manual Checklists
- Over Reliance on Small Samples

"New Way" of monitoring

- Continuous Monitoring
- Dashboard Tracking
- Full Sampling

Monitoring Internal Controls

Three-line model of monitoring

- Operations and operations managers
- Compliance and risk oversight
- Internal audit

Monitoring only works if people know their roles...

Pillars of Traceability — Design

A control is only as good as its design.

- A master map
- Dividing power
- Built-in trails
- Team safety net

Pillars of Traceability — Evidence

Strong controls produce clear evidence.

- Instant evidence
- Audit trail
- Hard guardrails
- Data integrity assurance

Testing for Effectiveness

- The logic check
- The reality check
- The proof hierarchy
- Real reperformance

Testing for Coverage

- No blind spots
- 100% data testing
- Guaranteed coverage
- Early fraud detection

Why should we care about selecting and managing third-parties? What could go wrong?

What do you consider significant risks related to reliance on third-parties?

Third-party Key Risks

- Key risks associated with reliance on third-parties:
  - **Cybersecurity and Data Breaches:** Third parties often have access to sensitive company systems and data, broadening the attack surface. A breach at a vendor can lead to stolen information, ransomware, or malware infection.
  - **Operational Disruptions:** Dependency on vendors for critical services or supplies can lead to production delays, service outages, or failure to deliver products, directly affecting business operations.
  - **Regulatory and Compliance Failures:** Third-party actions can cause companies to violate legal or industry standards, resulting in fines and penalties.

Increasing Number of Security Breaches Related to Third Parties

According to the Verizon 2025 Data Breach Investigations Report (DBIR), third-party involvement in data breaches doubled from 15% to 30% in the past year (2024–2025). This increase highlights the escalating risk of supply chain attacks, with 81% of these third-party breaches involving system intrusion.

- **Key Findings on Third-Party Risk** (2025 DBIR):
  - Supply Chain Focus: Reliance on vendors, software providers, and partners has significantly expanded the attack surface.
  - Credential Exploitation: Many third-party breaches are linked to credential reuse within partner environments.
  - Total Scope: The 2025 report analyzed 12,195 confirmed data breaches.

Third-Party Risk Management

TPRM Best Practices and Controls

- Third-party risk management (TPRM) controls include structured processes, policies, and technological safeguards used to identify, assess, and mitigate risks posed by external vendors, suppliers, and partners.
- Key controls include:
  - Comprehensive due diligence
  - Contractual security requirements
  - Continuous monitoring
  - Structured off-boarding

Key Controls for TPRM — Due Diligence and Assessment

- Due Diligence and Assessment Controls:
  - Vendor Risk Assessments: Using questionnaires to evaluate a vendor's security posture before engagement.
  - Due Diligence: Vetting vendors for financial stability, reputation, and compliance with legal or industry standards.

Key Controls for TPRM — Contractual and Legal

- Contractual and Legal Controls:
  - Right-to-audit Clauses: Ensuring contracts permit auditing vendor operational and security controls
  - Service-level Agreements (SLA): Defining performance and security standards, including uptime, required notification timing, and incident response requirements
  - Indemnification and Liability: Limiting liability and establishing financial responsibility for breaches of contract

Key Controls for TPRM — Operational and Technical

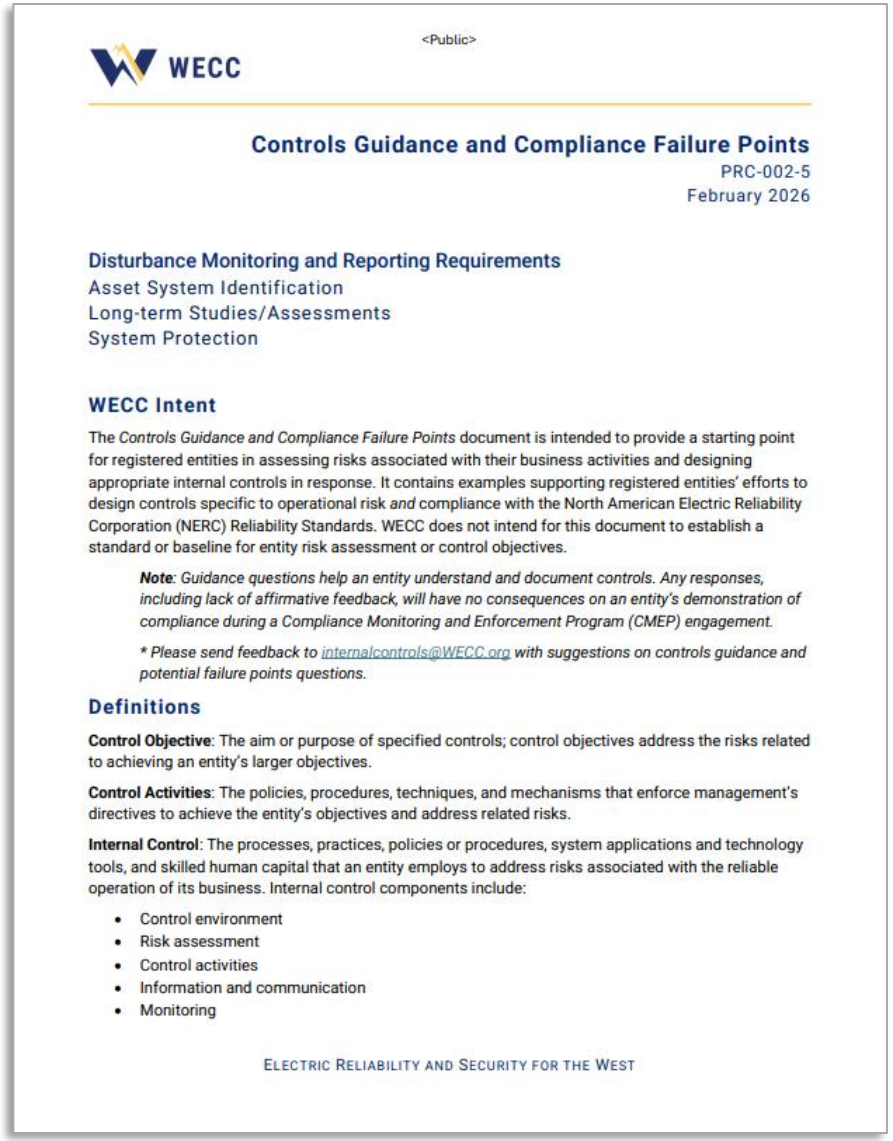
- Operational and Technical Controls:
  - Access Control and Identity Management: Restricting vendor access to only necessary systems and data (principle of least privilege)
  - Data Protection Measures: Ensuring encryption, data masking, and secure file transfers are used for data shared with third parties
  - Continuous Monitoring: Using tools to monitor vendor security posture
    - Periodic reviews
    - Monitoring performance metrics
    - Security assessments
    - Incident tracking
    - Audit

Key Controls for TPRM — Governance and Life Cycle

- Governance and Life Cycle Controls:
  - Policy: Establishing clear internal policies for onboarding, evaluating, and managing third parties
  - Third-party Inventory: Maintaining an updated inventory of all vendors and the risk level they pose.
  - Offboarding Procedures: Ensuring data is returned or destroyed and access is terminated immediately upon contract termination

Resources

- *Standards for Internal Control in the Federal Government (Green Book)*
- Controls Guidance and Compliance Failure Points
- ERO Enterprise Guide for Internal Controls
- Generator Welcome Packet
- WECC Risk Register
- Compliance Monitoring and Enforcement Program Implementation Plan (CMEP-IP)



<Public>

WECC

Controls Guidance and Compliance Failure Points
PRC-002-5
February 2026

Disturbance Monitoring and Reporting Requirements
Asset System Identification
Long-term Studies/Assessments
System Protection

WECC Intent

The *Controls Guidance and Compliance Failure Points* document is intended to provide a starting point for registered entities in assessing risks associated with their business activities and designing appropriate internal controls in response. It contains examples supporting registered entities' efforts to design controls specific to operational risk *and* compliance with the North American Electric Reliability Corporation (NERC) Reliability Standards. WECC does not intend for this document to establish a standard or baseline for entity risk assessment or control objectives.

> ***Note**: Guidance questions help an entity understand and document controls. Any responses, including lack of affirmative feedback, will have no consequences on an entity's demonstration of compliance during a Compliance Monitoring and Enforcement Program (CMEP) engagement.*
>
> ** Please send feedback to internalcontrols@WECC.org with suggestions on controls guidance and potential failure points questions.*

Definitions

Control Objective: The aim or purpose of specified controls; control objectives address the risks related to achieving an entity's larger objectives.

Control Activities: The policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks.

Internal Control: The processes, practices, policies or procedures, system applications and technology tools, and skilled human capital that an entity employs to address risks associated with the reliable operation of its business. Internal control components include:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

ELECTRIC RELIABILITY AND SECURITY FOR THE WEST

ELECTRIC RELIABILITY & SECURITY FOR THE WEST

ENGAGE WITH WECC

WECC

engage@wecc.org

www.wecc.org | 801-582-0353

155 N 400 W, Salt Lake City, Utah 84103, USA