DTE Energy Internal Controls Journey
August 2022 RF Technical Talk

- Internal Controls Journey Overview – Jason Smith
- Current Testing Approach – Anna Pawlak
- Improving our Compliance Programs by Increasing our Upstream Focus – Patrick Elliott
- Using a GRC (Governance Risk & Compliance) Tool to Manage NERC Compliance – Jeff Wallace

DTE

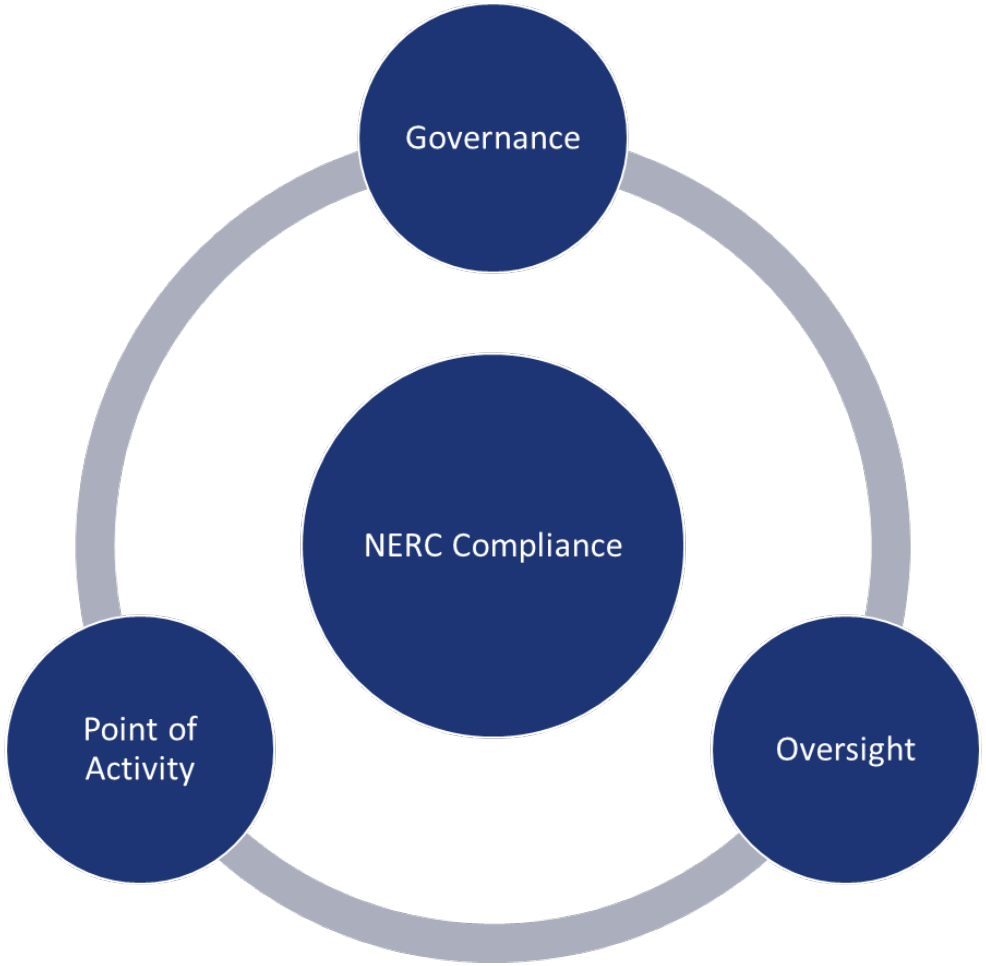
DTE and DTE Electric Overview

- DTE Energy (NYSE: DTE) is a Detroit-based diversified energy company. Its operating units include an electric utility serving 2.2 million customers in Southeastern Michigan and a natural gas utility serving 1.3 million customers in Michigan

- DTE Electric generates, transmits and distributes electricity. With an 11,084 megawatt system capacity, the company uses coal, nuclear fuel, natural gas, hydroelectric pumped storage and renewable sources to generate its electrical output. Founded in 1903, DTE Electric is the largest electric utility in Michigan and one of the largest in the nation

DTE

DTE Uses a Three-Pronged Approach to Manage NERC Compliance



1. Governance
   - NERC Executive Committee
   - NERC Violation Review Committee
   - NERC Governance Committee
2. Oversight
   - Oversight of programs and processes
   - Testing of internal controls
   - Liaison with RF
3. Point of Activity
   - Program ownership at a company level
   - Asset ownership at a business unit level
   - Ownership of point of activity processes and internal controls

NERC Compliance Office (NCO)

- DTE's NCO organization is responsible for **driving rigor and accountability** for compliance with NERC standards across the company

- Areas of focus include:
  - Future and current standards
  - Organizational training
  - Partnering with process owners on NERC related projects and process changes
  - Regulatory reporting
  - Risk assessment and compliance testing/monitoring

DTE’s NERC Compliance Journey Enablers

- Tone from the top
- Ownership – Program and point of activity
- Risk assessment
- Control activities
- Monitoring activities
- Open dialog with Reliability First

Combining Control and Detail Testing Together Strengthens our Compliance Posture

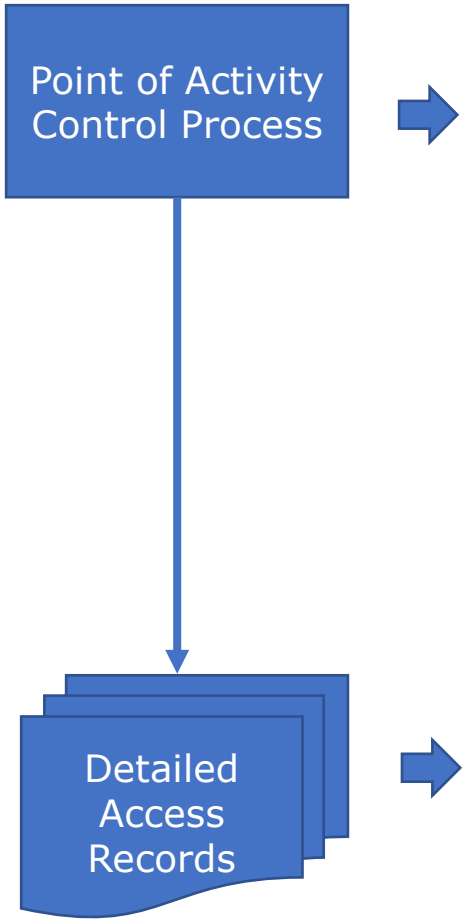
- **Control testing** is evaluating the process used by control owners to determine if they are effectively designed to protect the BES and mitigate compliance risks

- **Detail testing** is evaluating the results of the internal controls to assess compliance with reliability standards

- "*Even effectively designed and implemented internal controls cannot provide absolute assurance of compliance with NERC Reliability Standards*" (**NERC ERO Enterprise Guide for Internal Controls**)

- Control and Detail testing compliment one another – strong and effective controls reduce the risk to the BES, and of non-compliance, and impact the extent of detailed testing required to assess compliance with reliability standards

Control Testing vs. Detail Testing (Access Requirement Example)



Control Test Examples:

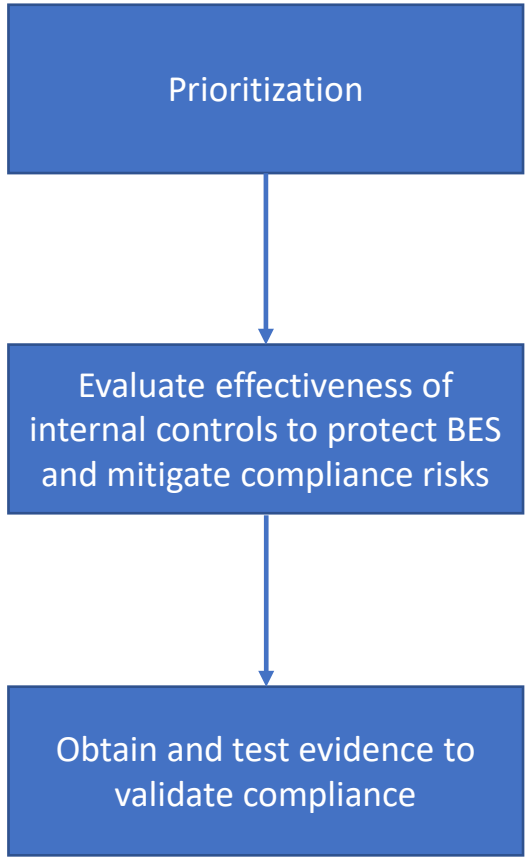
- Is there a documented process to review, add and revoke access? And does the process include verifying the correct attributes (e.g., training, need to know, supervisor approval, etc.)
- Are standard work instructions used?
- Is the process conducted timely (weekly, monthly, etc.)
- Does a supervisory review of the control take place?
- Review evidence that shows the process included a complete list of access points (locations, directories, etc.) and individuals and any discrepancies were resolved

Detail Test Examples:

- Obtain a list of all individuals with access
- Review supporting documentation to ensure the access is properly authorized and correct

Three Key Components to Designing a Compliance Testing Program

1. Risk Assessment
   - Perform annually with real-time updates
   - Use as a roadmap for testing
2. Control testing
   - Identify "key" controls with process owners
   - Test design and effectivity (understand process, test evidence to verify proper and consistent application)
   - Conclude on the effectiveness of internal control
3. Detail testing
   - Gather and test evidence
   - Testing scope and timing based on risk assessment and control testing



Current Testing Approach

- Point of activity process owners electronically submit evidence to NCO for review (primarily downstream testing)
- Risk based approach from a frequency and sample size perspective
- Program utilizes procedures similar to detail testing with the main goal being to provide reasonable assurance of compliance to NERC standards
- Rotation of tests promotes knowledge sharing and continuous improvement
- A Quality Assurance (QA) review is performed to ensure quality and feedback to testers
- Weekly huddles are used to track performance
- Testing gaps could result in the improvement of evidence/documentation, or the identification of a PNC

Recent Compliance Learnings

- Human performance is a common root cause for violations. Risks include:
  - Turnover
  - Documentation
  - Lack of peer or supervisor review

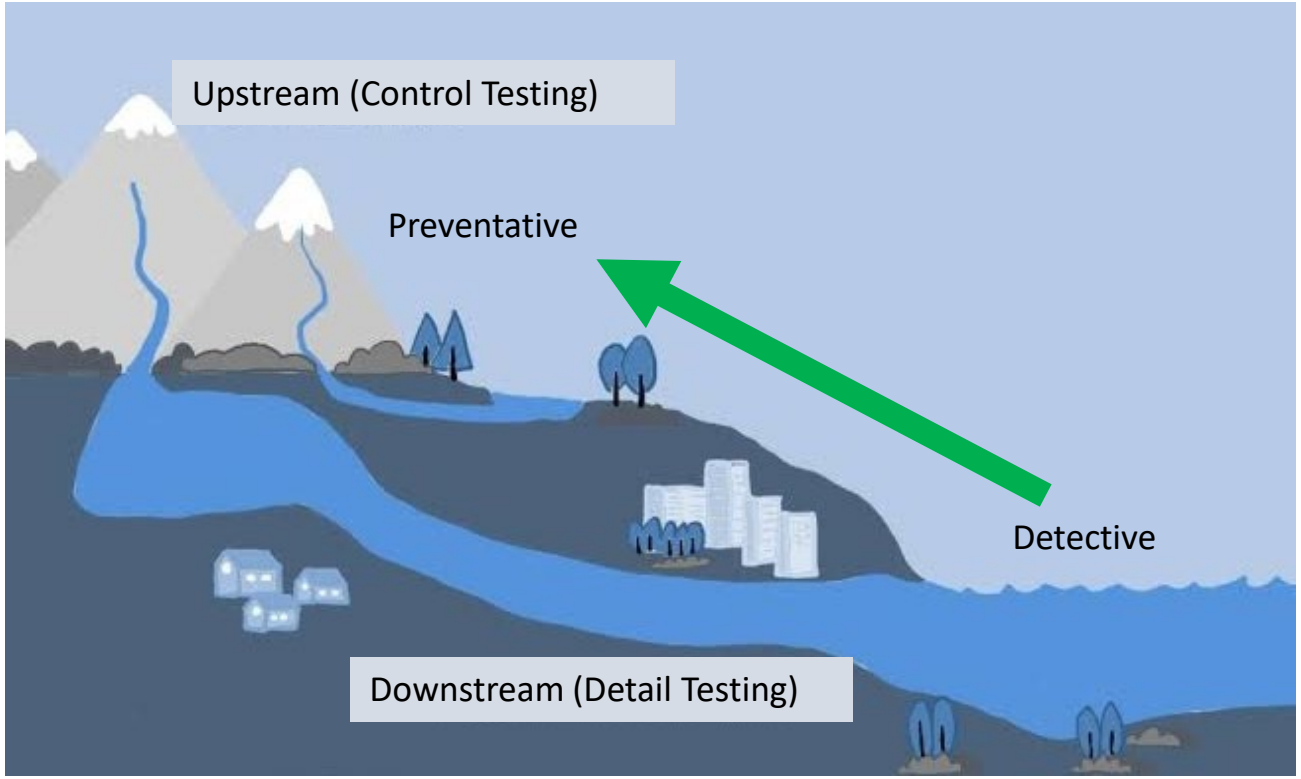
- Moving upstream can prevent violations, and provide earlier detection which reduces risk to the BES

- Prior to testing a population of evidence, the data must be verified to ensure completeness

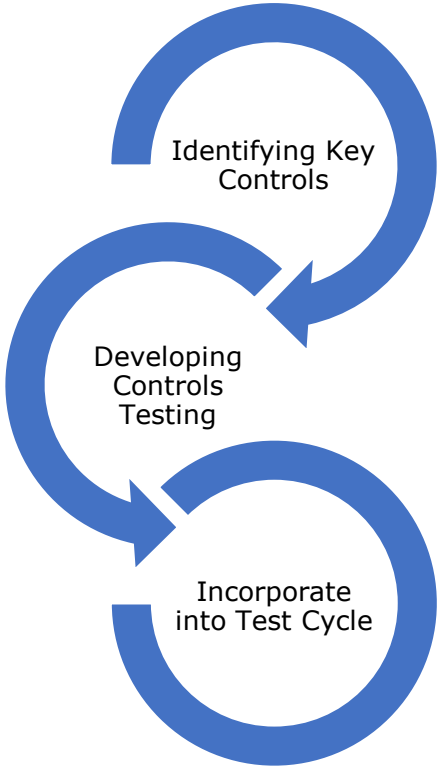
- Best practice is for process owners to have ownership of controls and evidence submissions

DTE Continues to Move "Upstream" in our Testing Approach which will Improve our Focus on the Reliability and Protection of the BES

- By continuing to add control testing to our compliance program, we are shifting some of our focus to the point of activity
- Control testing is more focused on preventing control gaps, versus detecting gaps (detail testing)



We are Committed to Enhancing our Compliance Programs by Increasing our Upstream Focus



Identifying Key Controls
- Collaborate with business partners to identify key controls
- Improving existing controls and establishing new controls

Developing Internal Controls Testing
- Developing testing to determine whether key control is working
- Identifying what evidence will be needed to test
- Determining depth of testing based on results

Incorporate into Test Cycle
- Incorporate controls, test procedures, and evidence requests into GRC (Governance Risk & Compliance) tool

- Project approach
  - Project completed by phase
  - Focusing on high-risk areas first

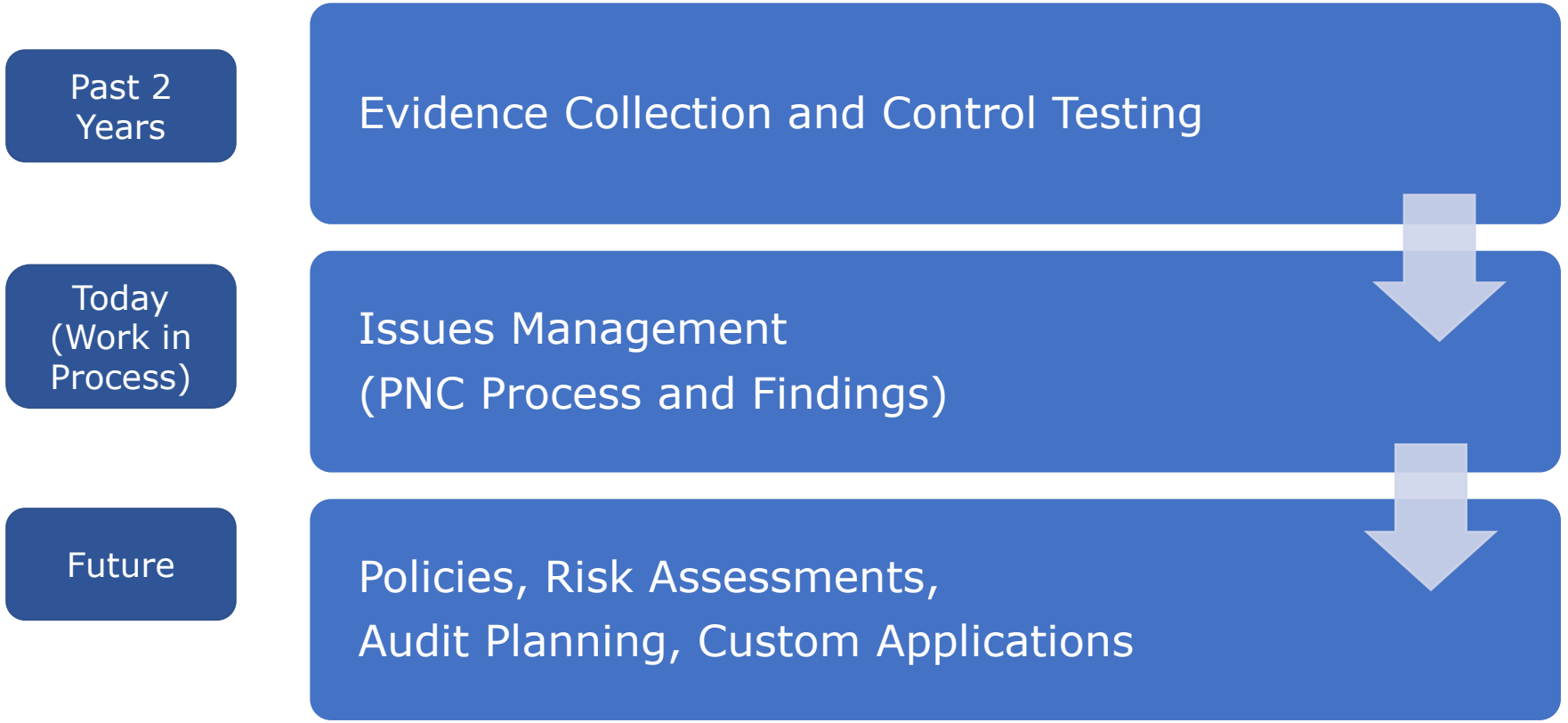
Why GRC (Governance Risk & Compliance)

- Needed a tool to support our Internal Controls Program
  - ✓Houses our control inventory
  - ✓Relational database that makes the necessary connections
  - ✓Provides automation and manages workflow
  - ✓Task management
  - ✓Improves efficiency
  - ✓Reporting and metrics

Selecting RSA Archer

- Tier 1 GRC Product
- Highly scalable system in terms of:
  - Functionality offered
  - Record count
  - Concurrent users
- Large user base and active community with a wealth of knowledge and best practices
- Customer Support

Our Archer Journey



Archer Dashboard Example