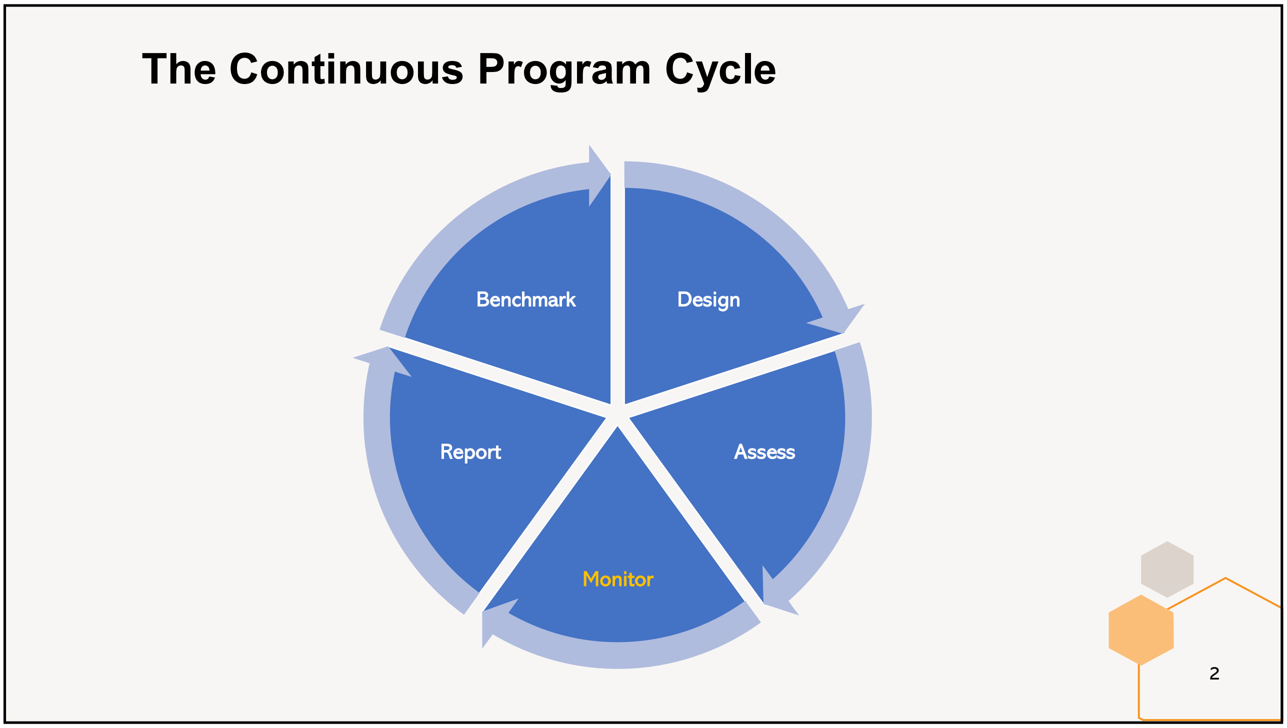
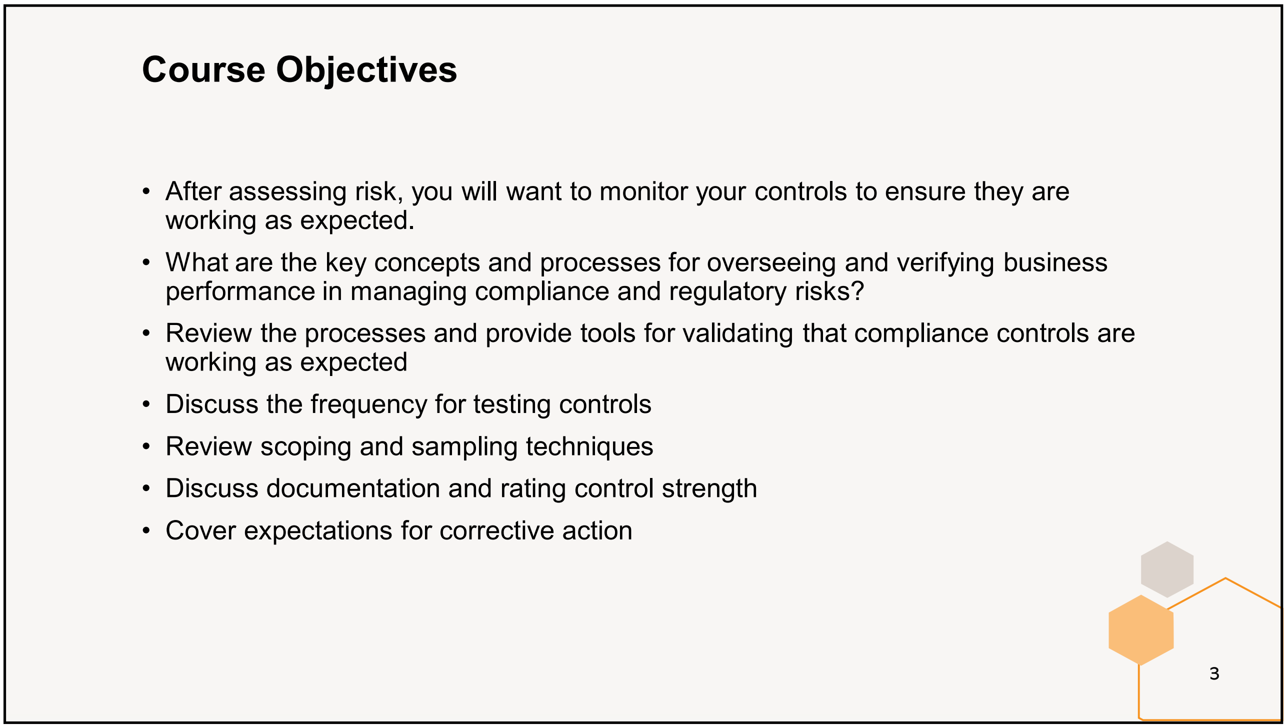
Managing Compliance Risk: Monitoring

Patti D. Joyner, CRCM
Financial Solutions
July 2024



The Continuous Program Cycle

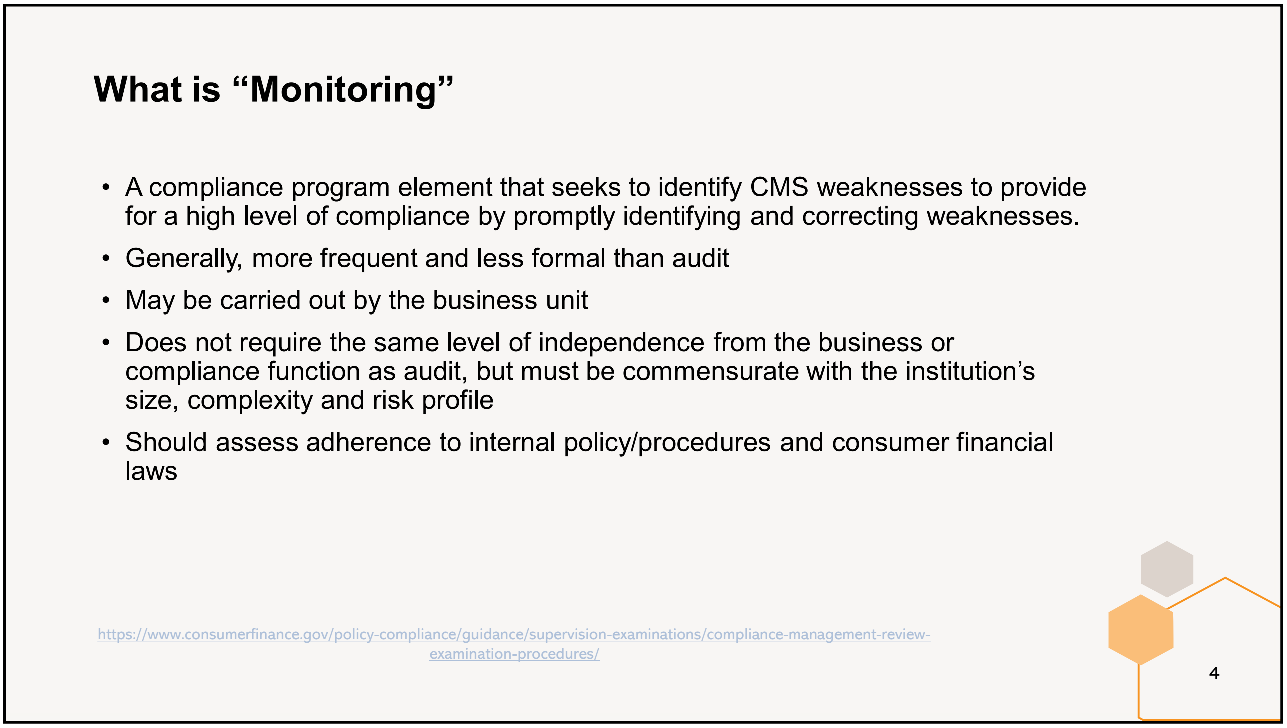
2



Course Objectives

- After assessing risk, you will want to monitor your controls to ensure they are working as expected.
- What are the key concepts and processes for overseeing and verifying business performance in managing compliance and regulatory risks?
- Review the processes and provide tools for validating that compliance controls are working as expected
- Discuss the frequency for testing controls
- Review scoping and sampling techniques
- Discuss documentation and rating control strength
- Cover expectations for corrective action

3

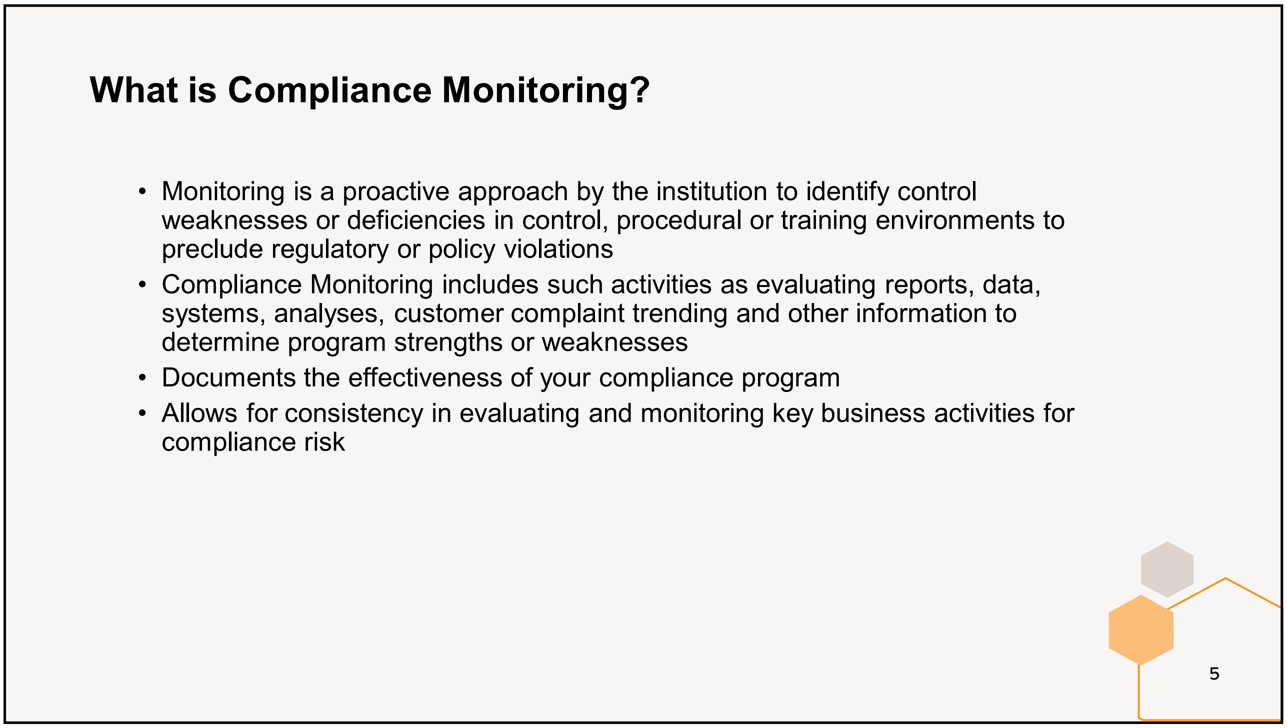


What is “Monitoring”

- A compliance program element that seeks to identify CMS weaknesses to provide for a high level of compliance by promptly identifying and correcting weaknesses.
- Generally, more frequent and less formal than audit
- May be carried out by the business unit
- Does not require the same level of independence from the business or compliance function as audit, but must be commensurate with the institution’s size, complexity and risk profile
- Should assess adherence to internal policy/procedures and consumer financial laws

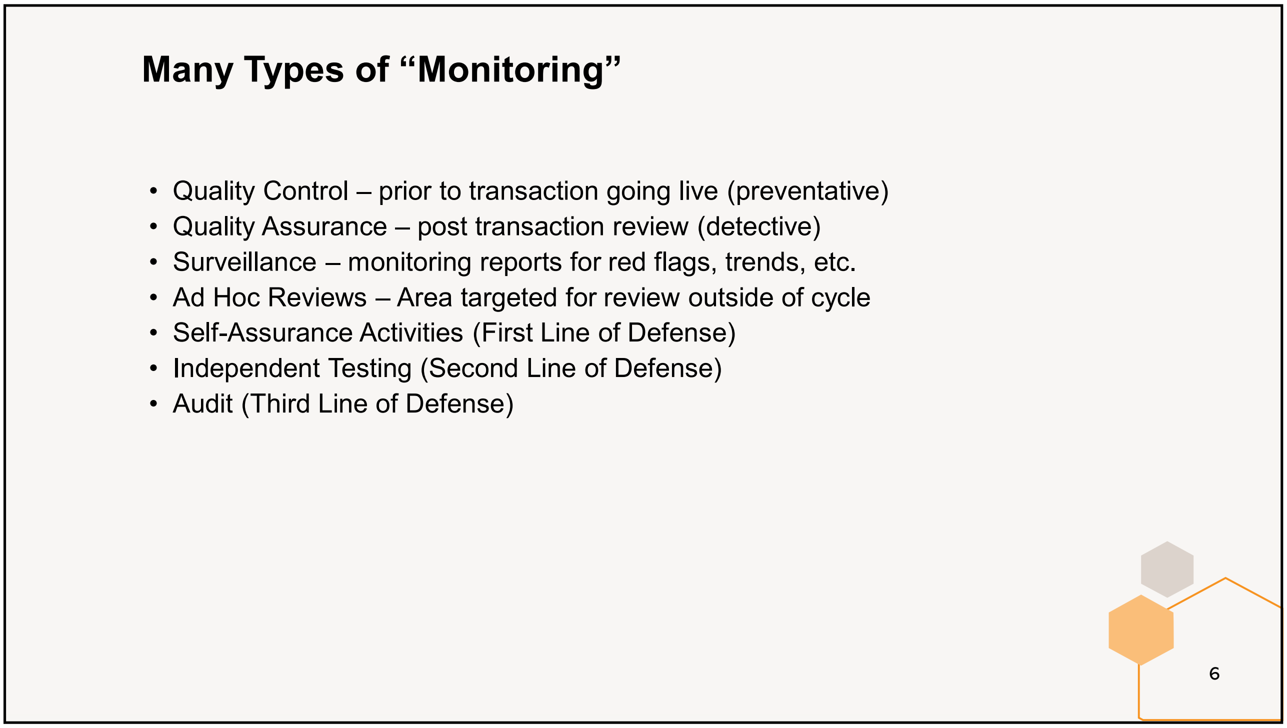
https://www.consumerfinance.gov/policy-compliance/guidance/supervision-examinations/compliance-management-review-examination-procedures/

4



What is Compliance Monitoring?

- Monitoring is a proactive approach by the institution to identify control weaknesses or deficiencies in control, procedural or training environments to preclude regulatory or policy violations
- Compliance Monitoring includes such activities as evaluating reports, data, systems, analyses, customer complaint trending and other information to determine program strengths or weaknesses
- Documents the effectiveness of your compliance program
- Allows for consistency in evaluating and monitoring key business activities for compliance risk



Many Types of “Monitoring”

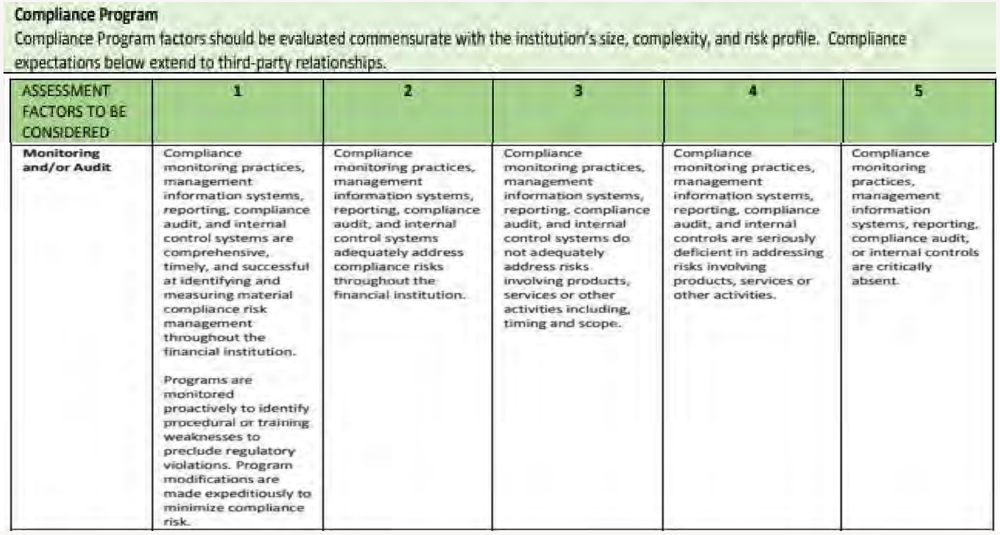
- Quality Control – prior to transaction going live (preventative)
- Quality Assurance – post transaction review (detective)
- Surveillance – monitoring reports for red flags, trends, etc.
- Ad Hoc Reviews – Area targeted for review outside of cycle
- Self-Assurance Activities (First Line of Defense)
- Independent Testing (Second Line of Defense)
- Audit (Third Line of Defense)

Compliance Monitoring Considerations

Monitoring includes taking a risk-based approach to evaluating risk and/or conducting regular reviews of regulations/policies/processes in multiple areas of compliance. Based on the institution's compliance exposure, risk profile and tolerance, leadership should consider including any of these topics in their monitoring program:

- Complaints that could reflect compliance trends
- Disclosures and calculations for various product offerings
- Document filing and retention procedures;
- Posted notices, marketing literature, and advertising
- Consumer protection laws and regulations
- Third-party service provider operations
- Internal compliance communication systems that update and revise the applicable laws and regulations to management and staff.
- Emerging compliance trends based on regulatory guidance or enforcement actions

FFIEC Rating Definitions: Monitoring/Audit

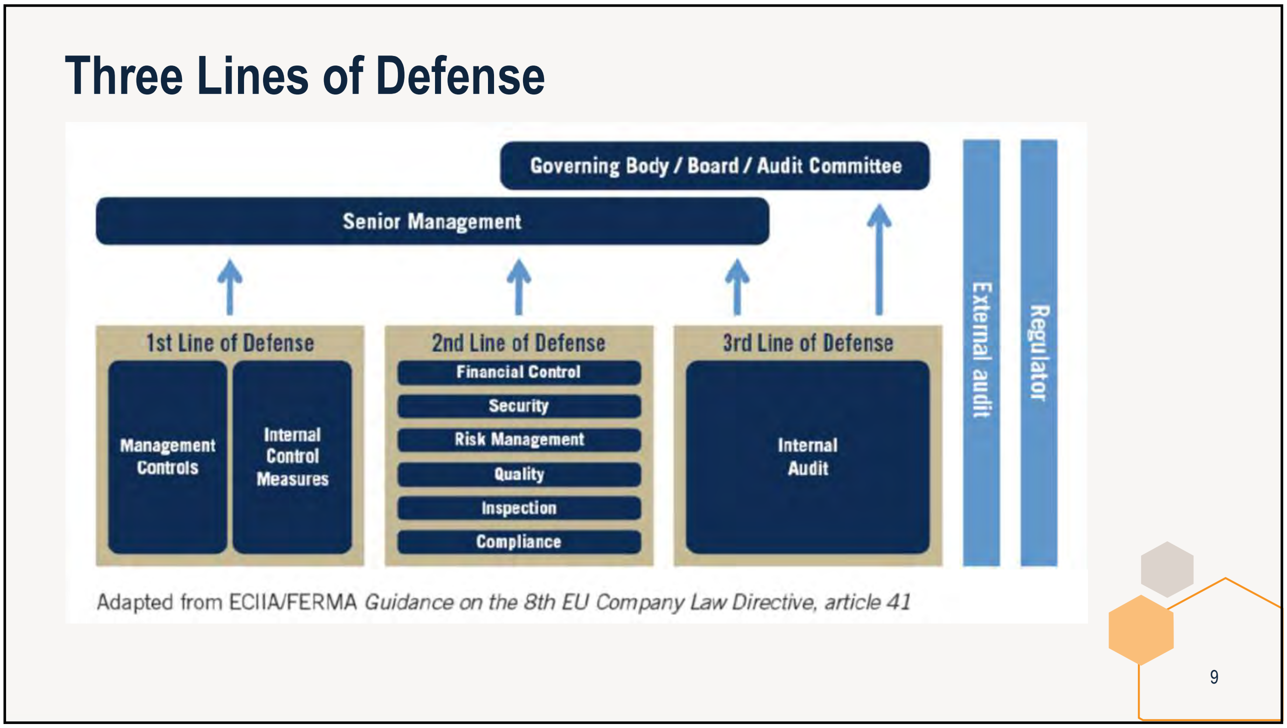


Compliance Program

Compliance Program factors should be evaluated commensurate with the institution's size, complexity, and risk profile. Compliance expectations below extend to third-party relationships.

ASSESSMENT FACTORS TO BE CONSIDERED	1	2	3	4	5
Monitoring and/or Audit	Compliance monitoring practices, management information systems, reporting, compliance audit, and internal control systems are comprehensive, timely, and successful at identifying and measuring material compliance risk management throughout the financial institution. Programs are monitored proactively to identify procedural or training weaknesses to preclude regulatory violations. Program modifications are made expeditiously to minimize compliance risk.	Compliance monitoring practices, management information systems, reporting, compliance audit, and internal control systems adequately address compliance risks throughout the financial institution.	Compliance monitoring practices, management information systems, reporting, compliance audit, and internal control systems do not adequately address risks involving products, services or other activities including, timing and scope.	Compliance monitoring practices, management information systems, reporting, compliance audit, and internal controls are seriously deficient in addressing risks involving products, services or other activities.	Compliance monitoring practices, management information systems, reporting, compliance audit, or internal controls are critically absent.

https://www.ffiec.gov/press/PDF/FFIEC_CCR_SystemFR_Notice.pdf



Three Lines of Defense

Governing Body / Board / Audit Committee

Senior Management

1st Line of Defense
- Management Controls
- Internal Control Measures

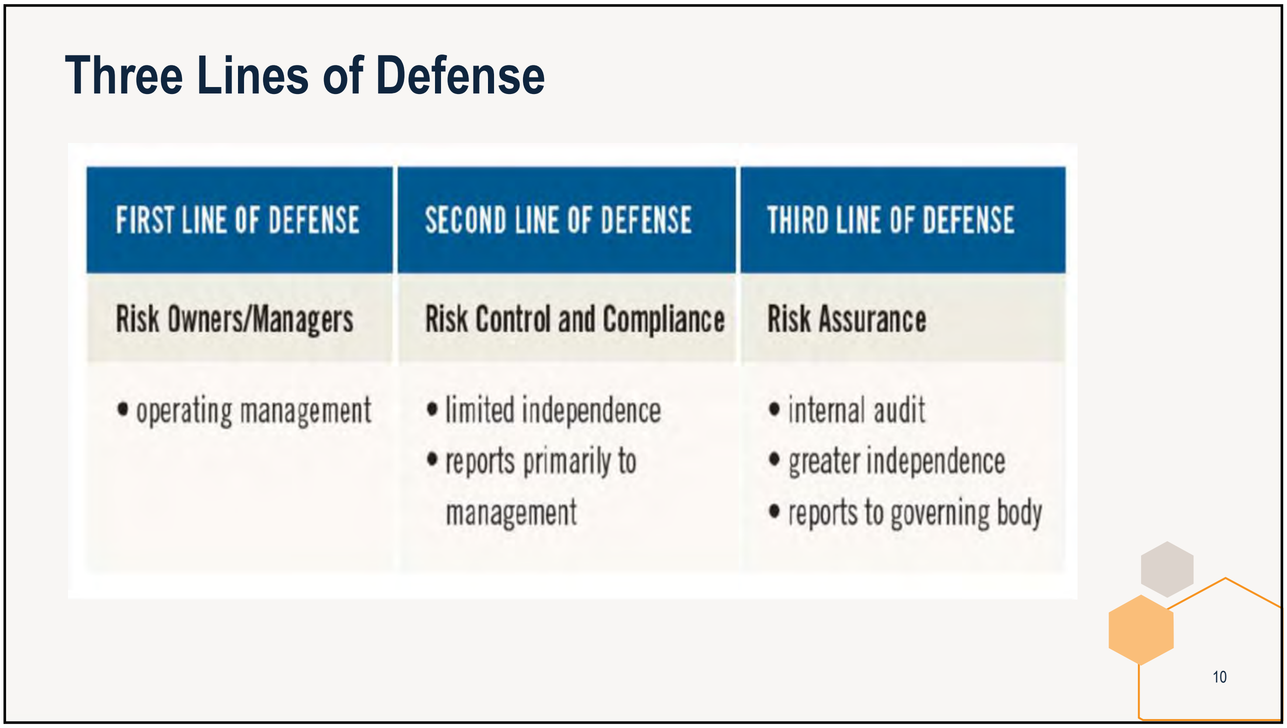
2nd Line of Defense
- Financial Control
- Security
- Risk Management
- Quality
- Inspection
- Compliance

3rd Line of Defense
- Internal Audit

External audit

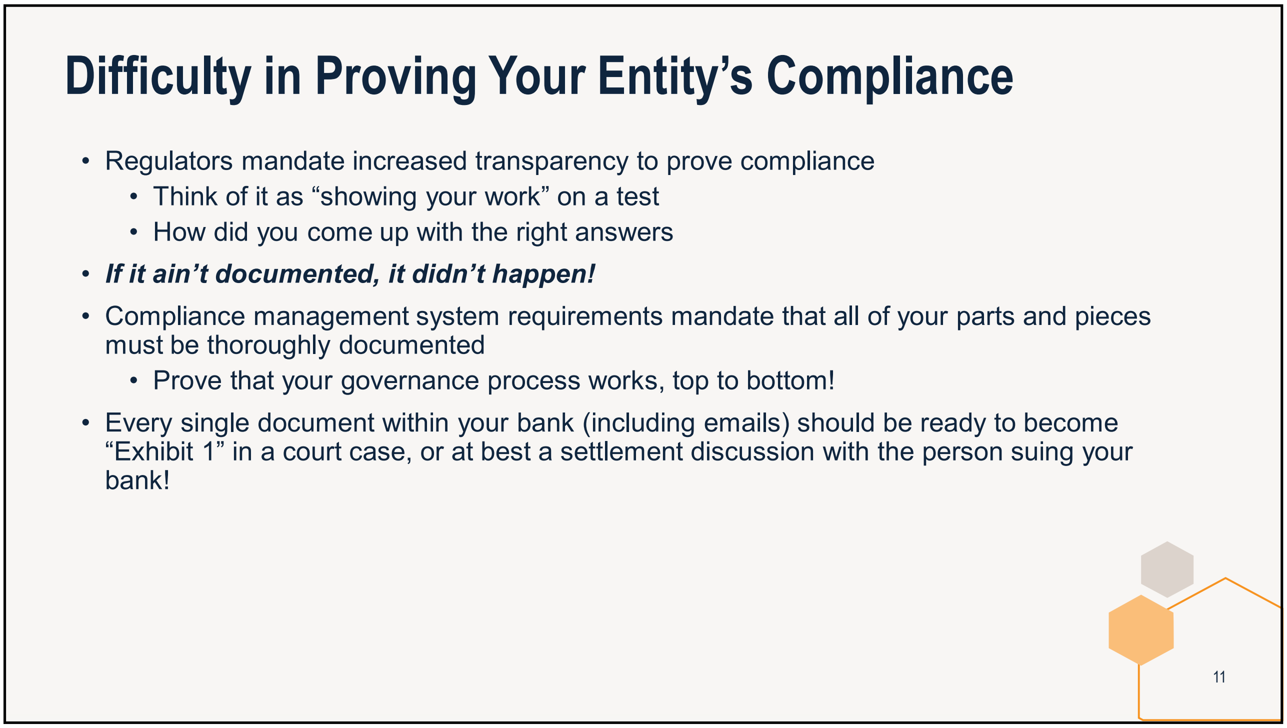
Regulator

Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*



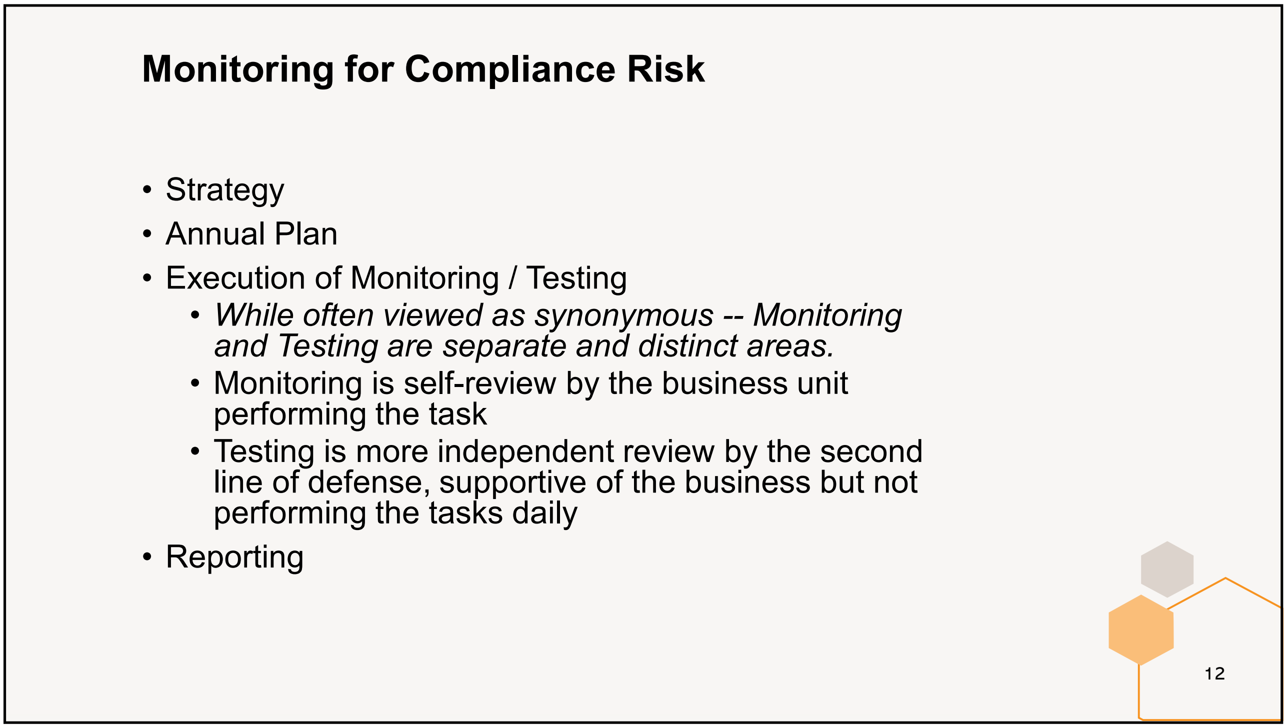
Three Lines of Defense

FIRST LINE OF DEFENSE	SECOND LINE OF DEFENSE	THIRD LINE OF DEFENSE
Risk Owners/Managers	Risk Control and Compliance	Risk Assurance
• operating management	• limited independence • reports primarily to management	• internal audit • greater independence • reports to governing body



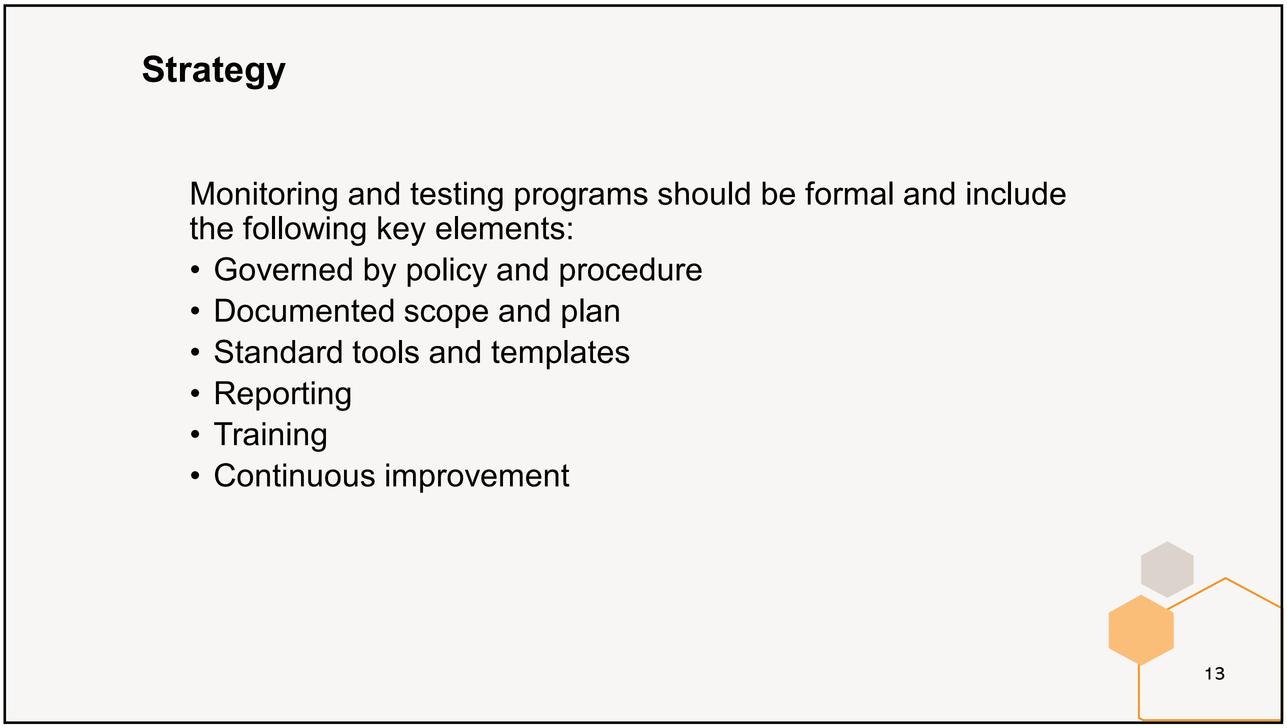
Difficulty in Proving Your Entity’s Compliance

- Regulators mandate increased transparency to prove compliance
  - Think of it as “showing your work” on a test
  - How did you come up with the right answers
- ***If it ain’t documented, it didn’t happen!***
- Compliance management system requirements mandate that all of your parts and pieces must be thoroughly documented
  - Prove that your governance process works, top to bottom!
- Every single document within your bank (including emails) should be ready to become “Exhibit 1” in a court case, or at best a settlement discussion with the person suing your bank!



Monitoring for Compliance Risk

- Strategy
- Annual Plan
- Execution of Monitoring / Testing
  - *While often viewed as synonymous -- Monitoring and Testing are separate and distinct areas.*
  - Monitoring is self-review by the business unit performing the task
  - Testing is more independent review by the second line of defense, supportive of the business but not performing the tasks daily
- Reporting

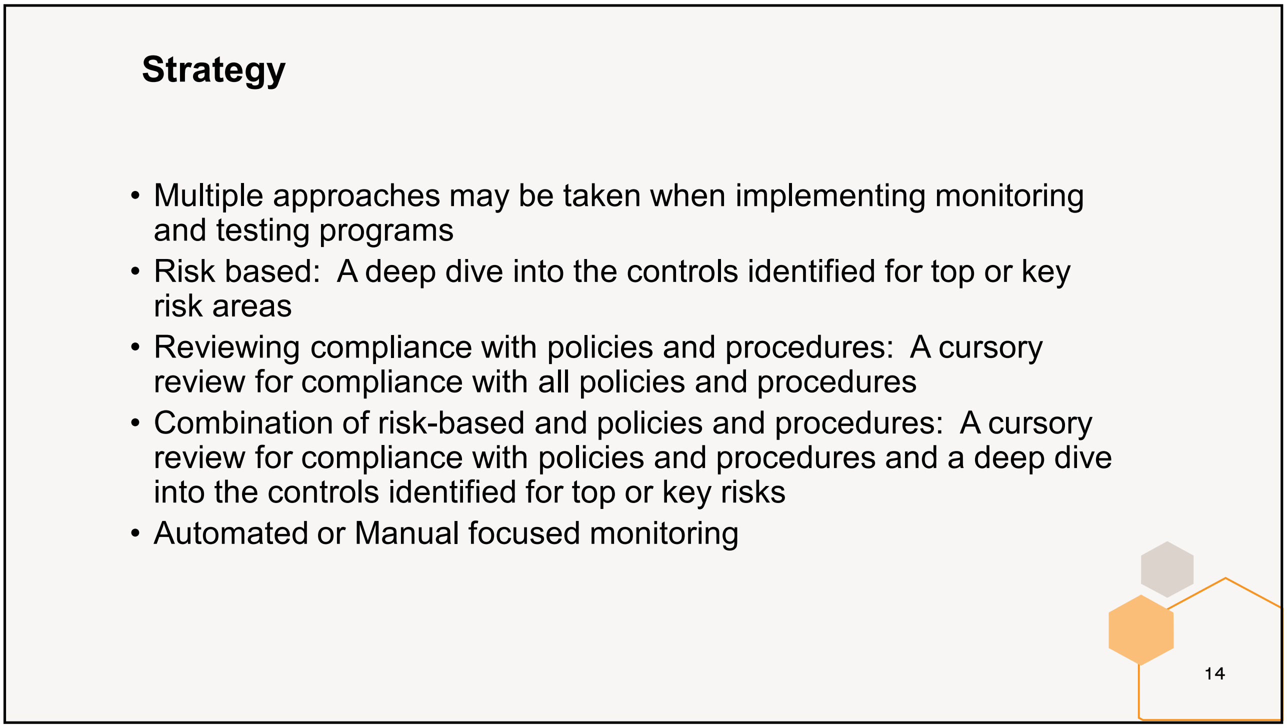


Strategy

Monitoring and testing programs should be formal and include the following key elements:

- Governed by policy and procedure
- Documented scope and plan
- Standard tools and templates
- Reporting
- Training
- Continuous improvement

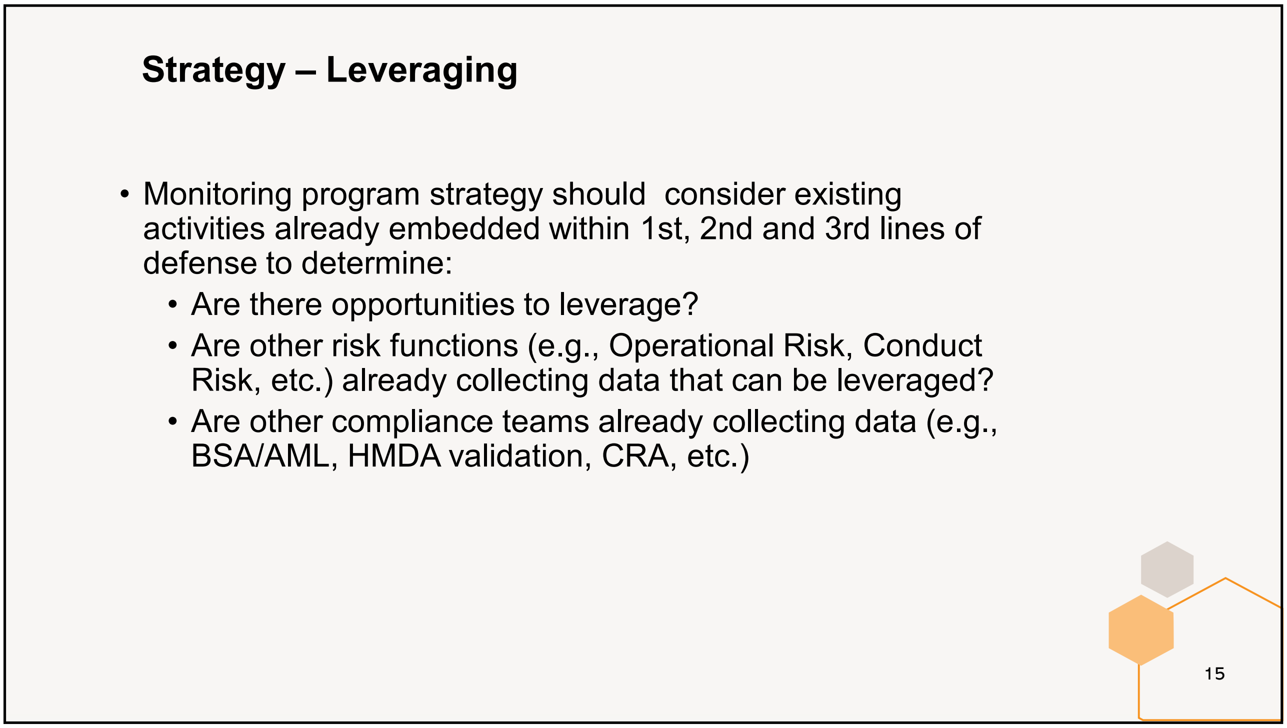
13



Strategy

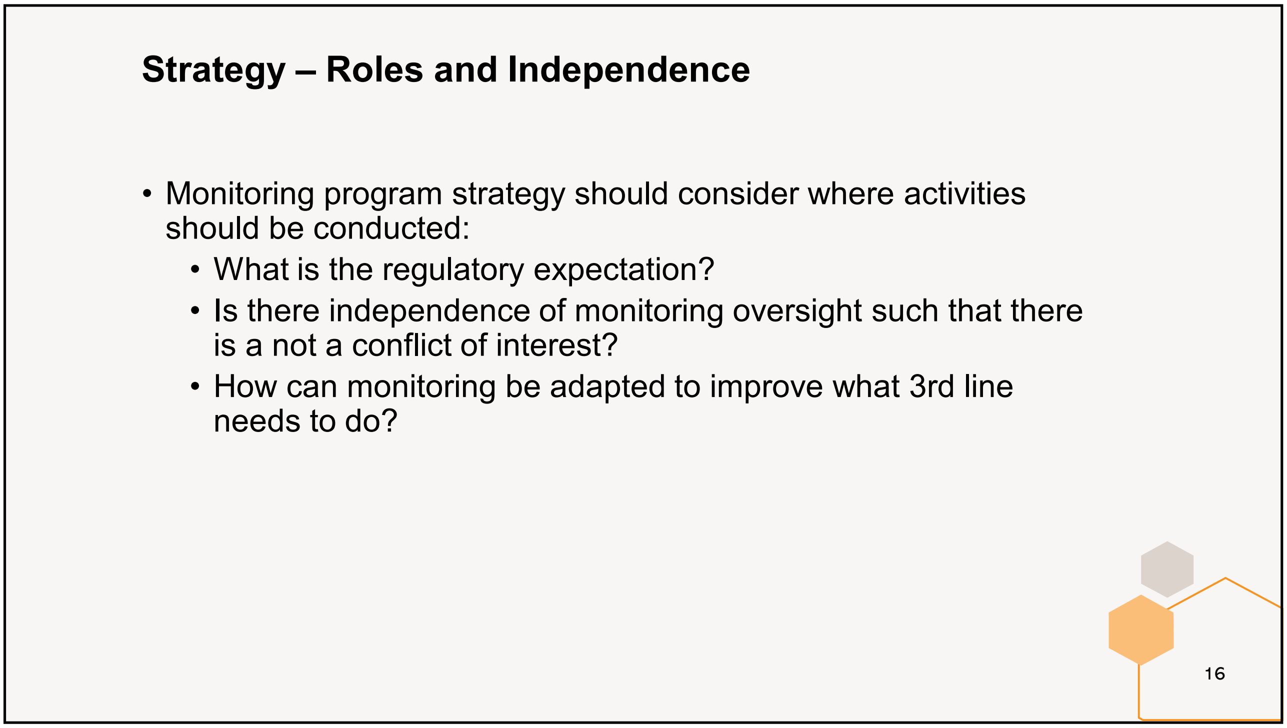
- Multiple approaches may be taken when implementing monitoring and testing programs
- Risk based: A deep dive into the controls identified for top or key risk areas
- Reviewing compliance with policies and procedures: A cursory review for compliance with all policies and procedures
- Combination of risk-based and policies and procedures: A cursory review for compliance with policies and procedures and a deep dive into the controls identified for top or key risks
- Automated or Manual focused monitoring

14



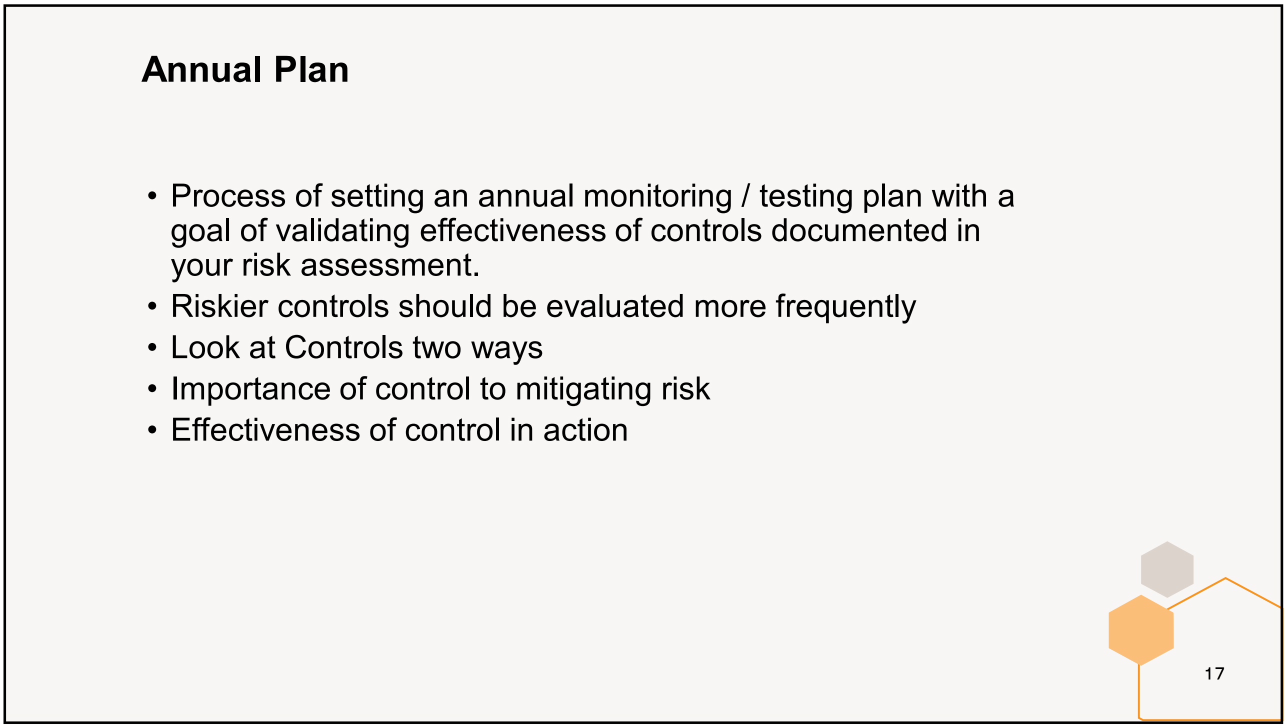
Strategy – Leveraging

- Monitoring program strategy should consider existing activities already embedded within 1st, 2nd and 3rd lines of defense to determine:
  - Are there opportunities to leverage?
  - Are other risk functions (e.g., Operational Risk, Conduct Risk, etc.) already collecting data that can be leveraged?
  - Are other compliance teams already collecting data (e.g., BSA/AML, HMDA validation, CRA, etc.)



Strategy – Roles and Independence

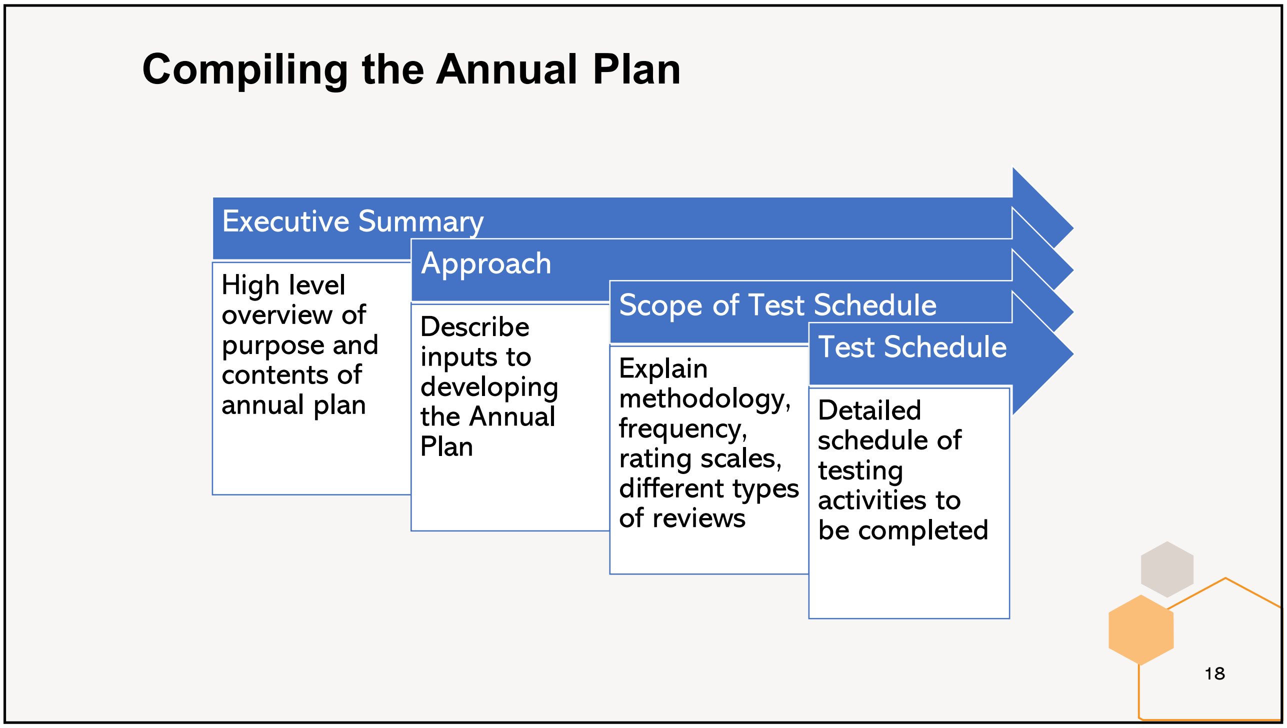
- Monitoring program strategy should consider where activities should be conducted:
  - What is the regulatory expectation?
  - Is there independence of monitoring oversight such that there is a not a conflict of interest?
  - How can monitoring be adapted to improve what 3rd line needs to do?



Annual Plan

- Process of setting an annual monitoring / testing plan with a goal of validating effectiveness of controls documented in your risk assessment.
- Riskier controls should be evaluated more frequently
- Look at Controls two ways
- Importance of control to mitigating risk
- Effectiveness of control in action

17



Compiling the Annual Plan

Executive Summary

High level overview of purpose and contents of annual plan

Approach

Describe inputs to developing the Annual Plan

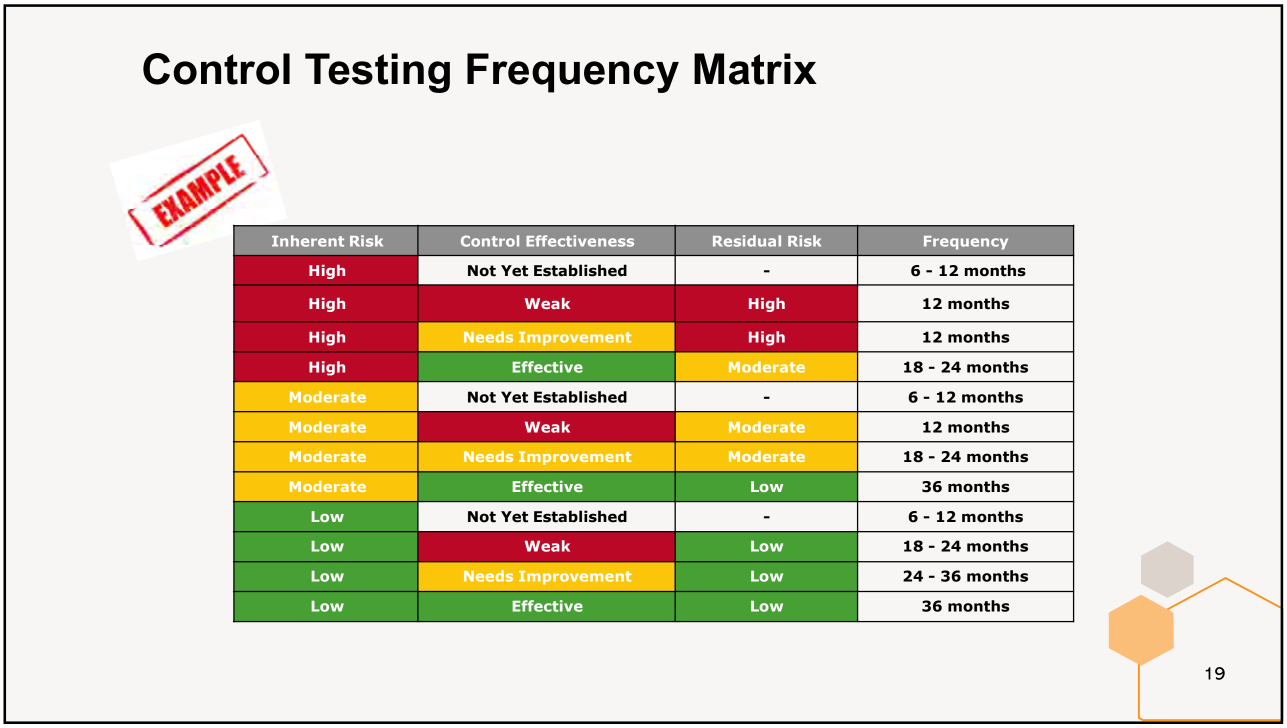
Scope of Test Schedule

Explain methodology, frequency, rating scales, different types of reviews

Test Schedule

Detailed schedule of testing activities to be completed

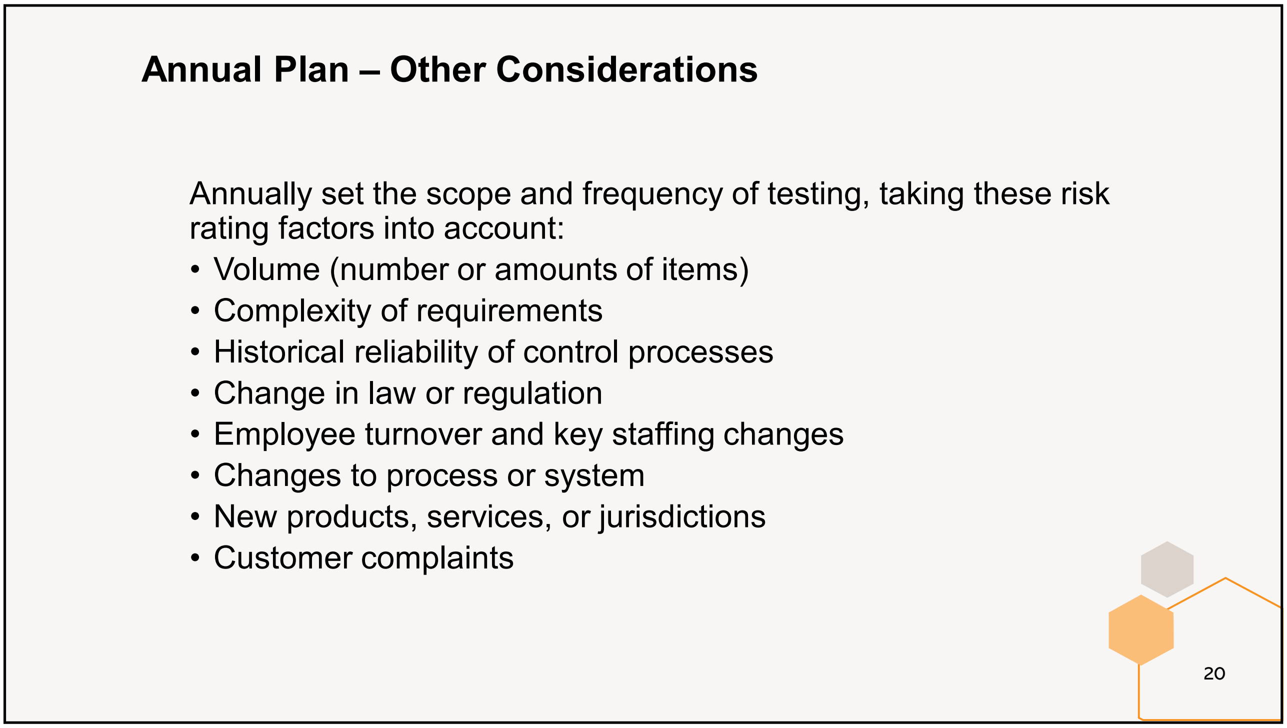
18



Control Testing Frequency Matrix

EXAMPLE

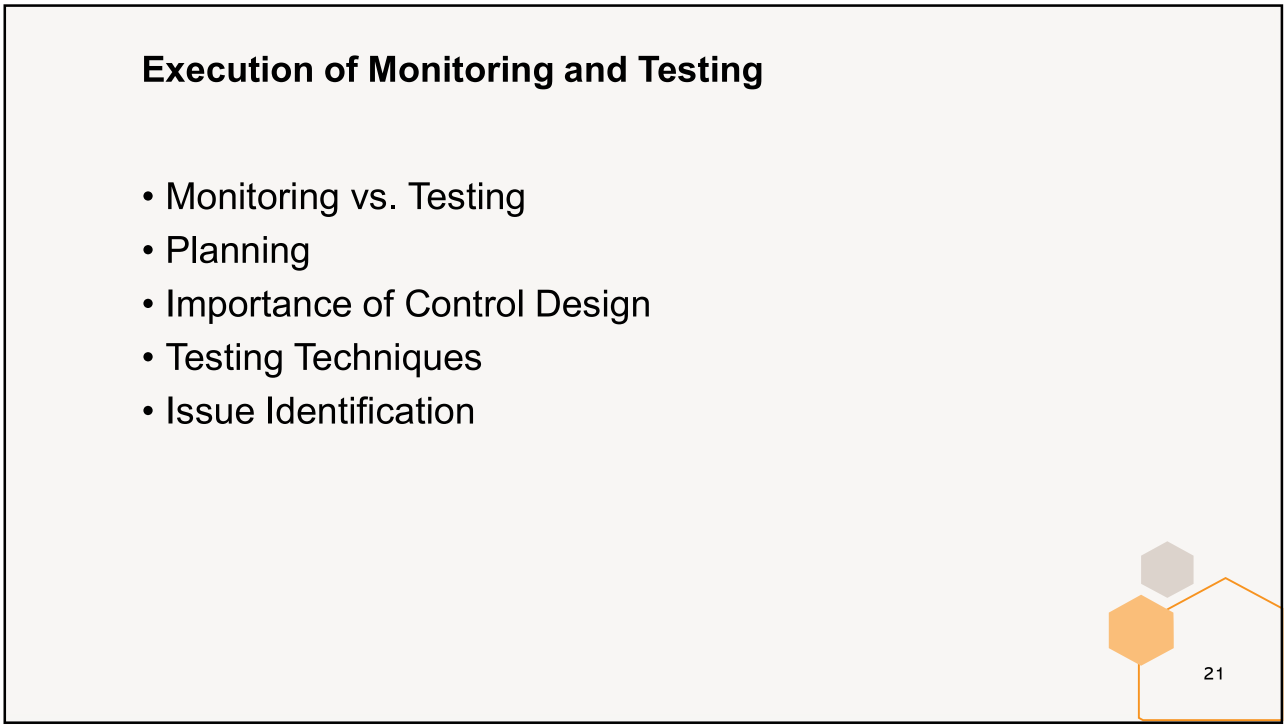
Inherent Risk	Control Effectiveness	Residual Risk	Frequency
High	Not Yet Established	-	6 - 12 months
High	Weak	High	12 months
High	Needs Improvement	High	12 months
High	Effective	Moderate	18 - 24 months
Moderate	Not Yet Established	-	6 - 12 months
Moderate	Weak	Moderate	12 months
Moderate	Needs Improvement	Moderate	18 - 24 months
Moderate	Effective	Low	36 months
Low	Not Yet Established	-	6 - 12 months
Low	Weak	Low	18 - 24 months
Low	Needs Improvement	Low	24 - 36 months
Low	Effective	Low	36 months



Annual Plan – Other Considerations

Annually set the scope and frequency of testing, taking these risk rating factors into account:

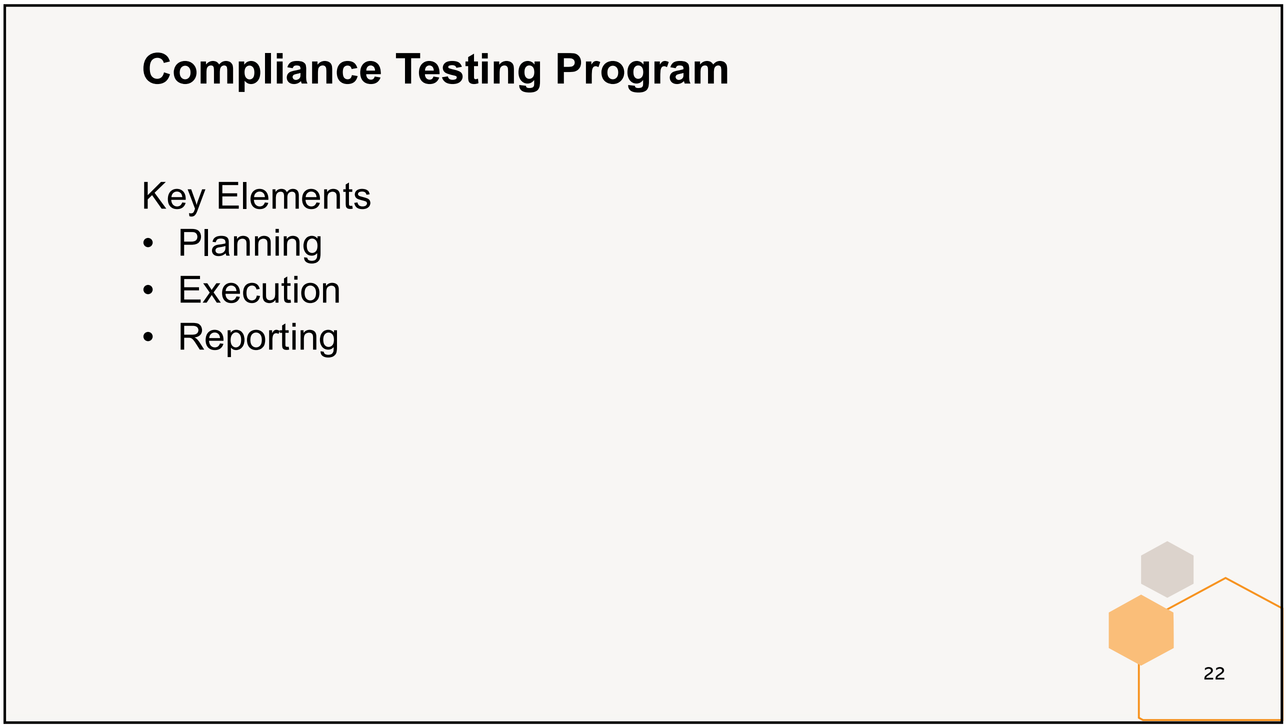
- Volume (number or amounts of items)
- Complexity of requirements
- Historical reliability of control processes
- Change in law or regulation
- Employee turnover and key staffing changes
- Changes to process or system
- New products, services, or jurisdictions
- Customer complaints



Execution of Monitoring and Testing

- Monitoring vs. Testing
- Planning
- Importance of Control Design
- Testing Techniques
- Issue Identification

21

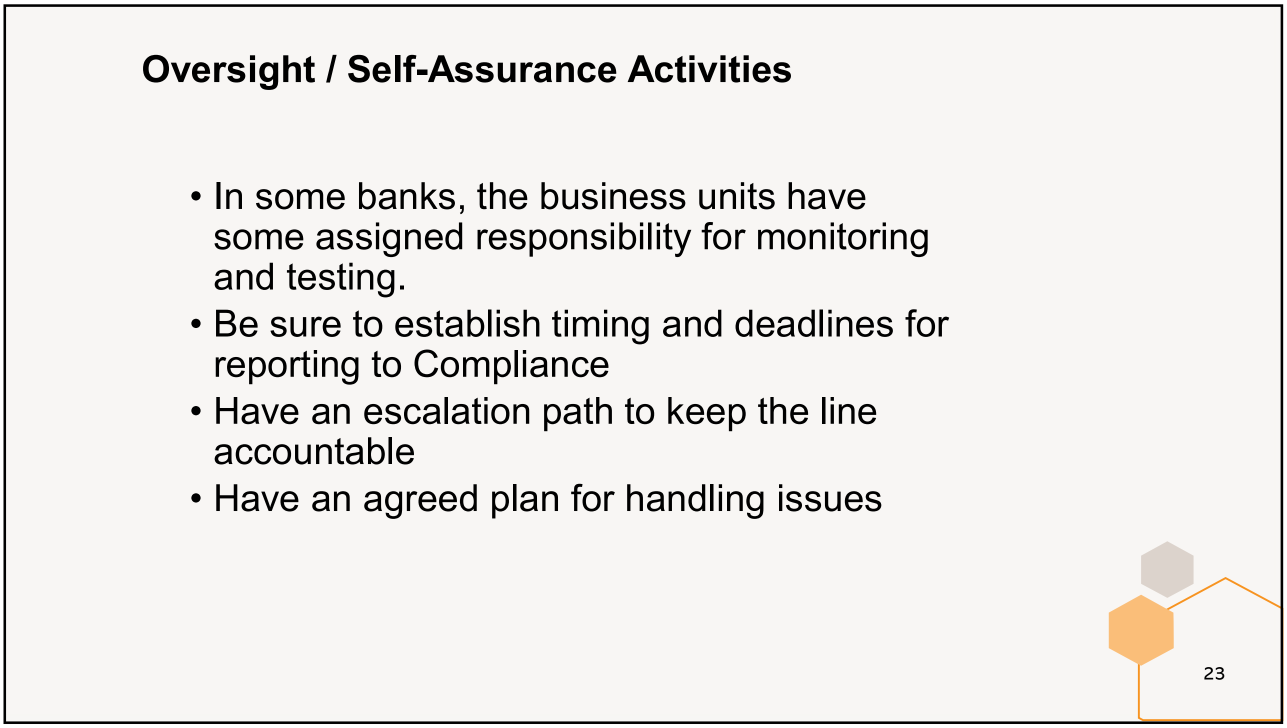


Compliance Testing Program

Key Elements

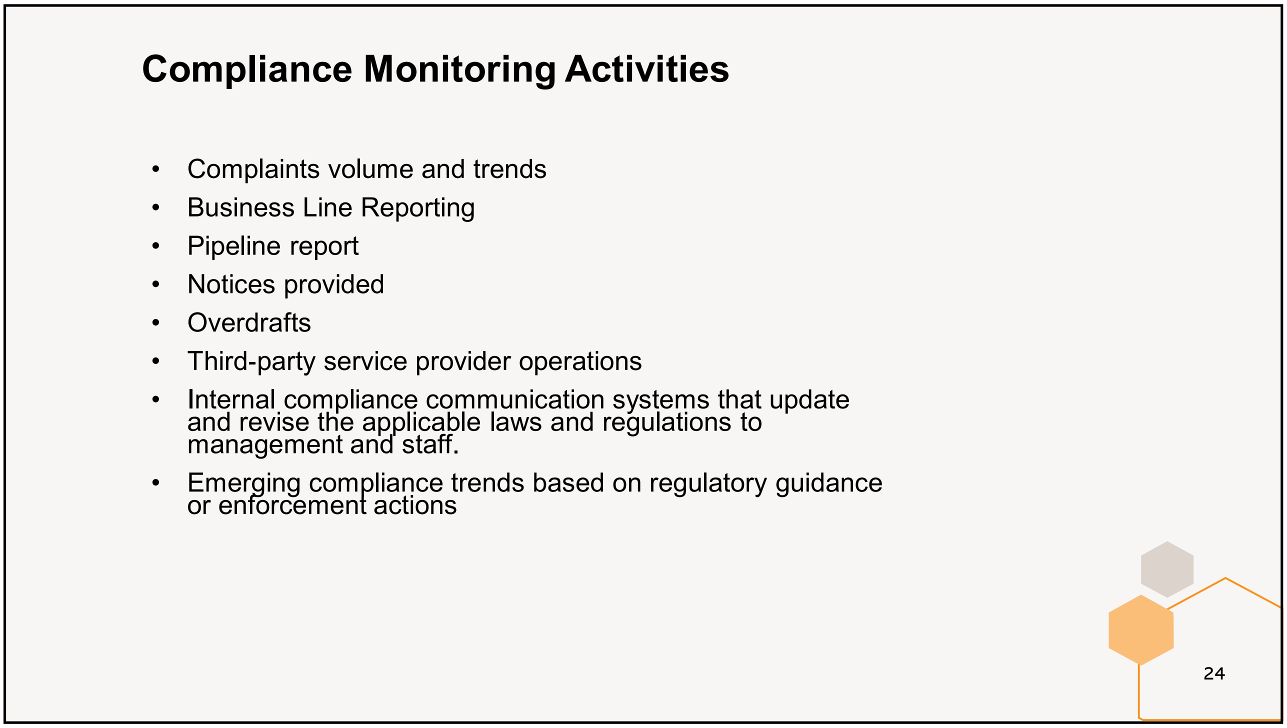
- Planning
- Execution
- Reporting

22



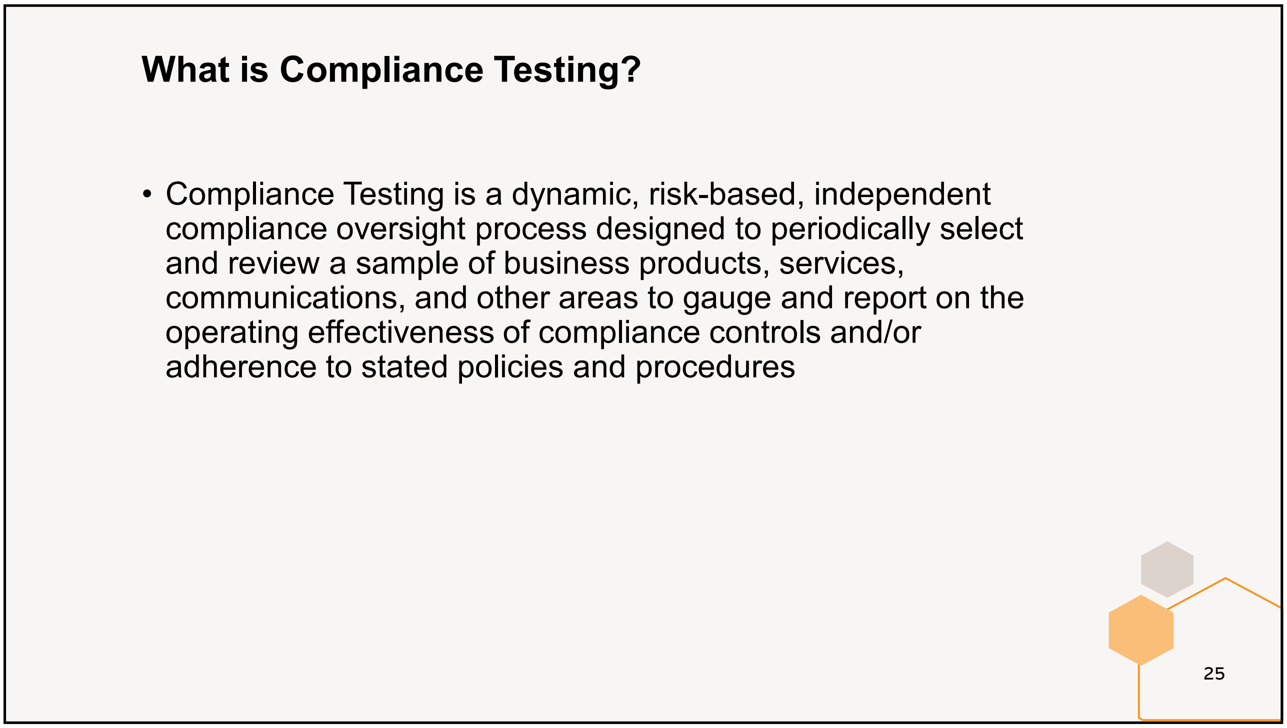
Oversight / Self-Assurance Activities

- In some banks, the business units have some assigned responsibility for monitoring and testing.
- Be sure to establish timing and deadlines for reporting to Compliance
- Have an escalation path to keep the line accountable
- Have an agreed plan for handling issues



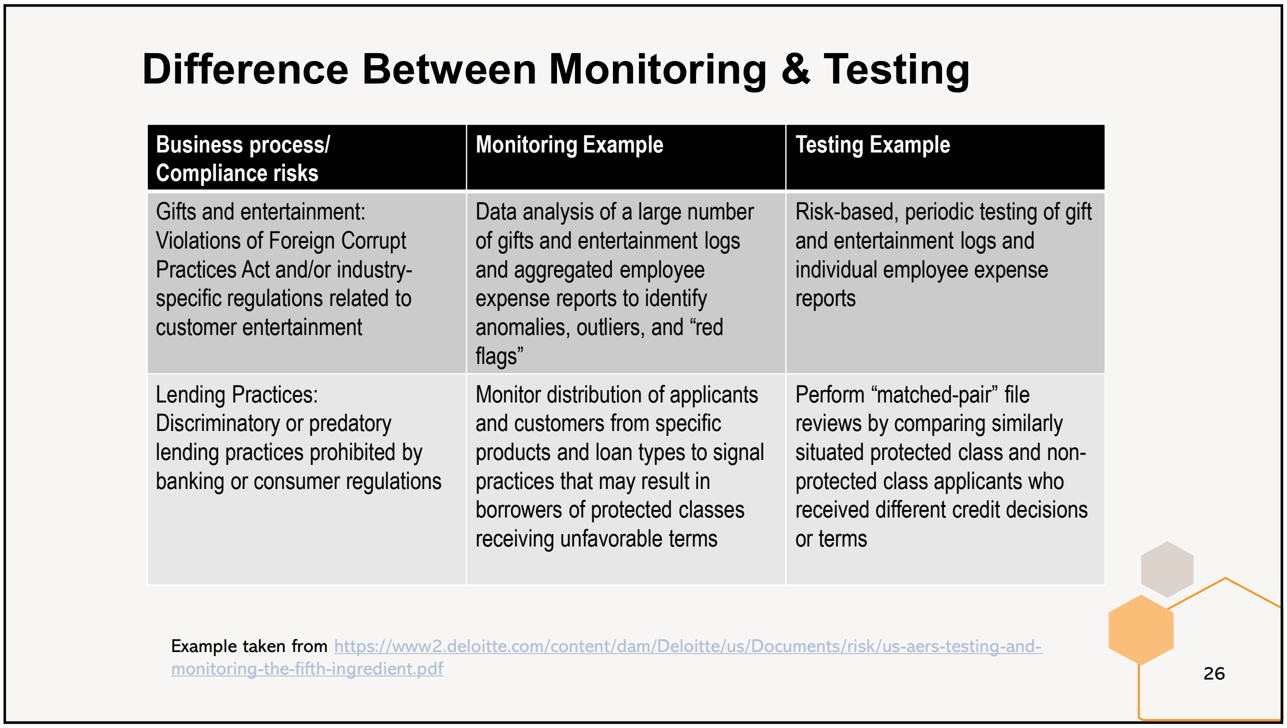
Compliance Monitoring Activities

- Complaints volume and trends
- Business Line Reporting
- Pipeline report
- Notices provided
- Overdrafts
- Third-party service provider operations
- Internal compliance communication systems that update and revise the applicable laws and regulations to management and staff.
- Emerging compliance trends based on regulatory guidance or enforcement actions



What is Compliance Testing?

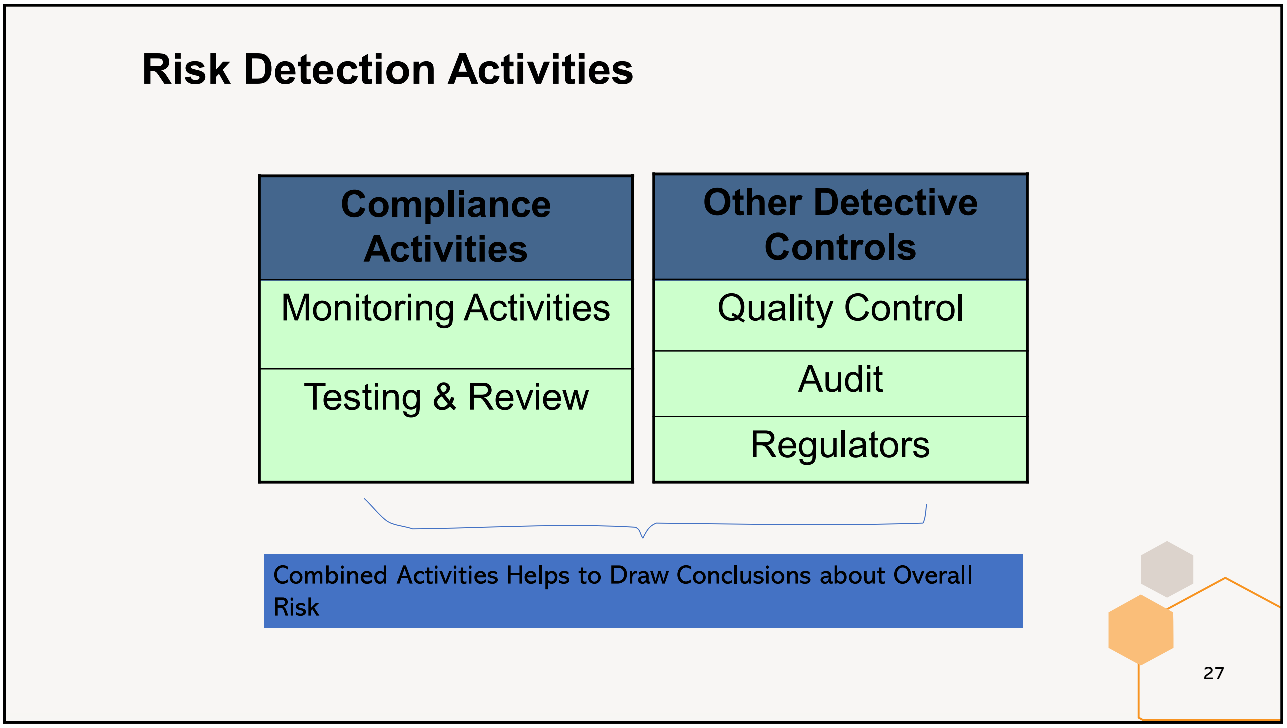
- Compliance Testing is a dynamic, risk-based, independent compliance oversight process designed to periodically select and review a sample of business products, services, communications, and other areas to gauge and report on the operating effectiveness of compliance controls and/or adherence to stated policies and procedures



Difference Between Monitoring & Testing

Business process/ Compliance risks	Monitoring Example	Testing Example
Gifts and entertainment: Violations of Foreign Corrupt Practices Act and/or industry-specific regulations related to customer entertainment	Data analysis of a large number of gifts and entertainment logs and aggregated employee expense reports to identify anomalies, outliers, and "red flags"	Risk-based, periodic testing of gift and entertainment logs and individual employee expense reports
Lending Practices: Discriminatory or predatory lending practices prohibited by banking or consumer regulations	Monitor distribution of applicants and customers from specific products and loan types to signal practices that may result in borrowers of protected classes receiving unfavorable terms	Perform "matched-pair" file reviews by comparing similarly situated protected class and non-protected class applicants who received different credit decisions or terms

Example taken from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-testing-and-monitoring-the-fifth-ingredient.pdf



Risk Detection Activities

Compliance Activities

Monitoring Activities

Testing & Review

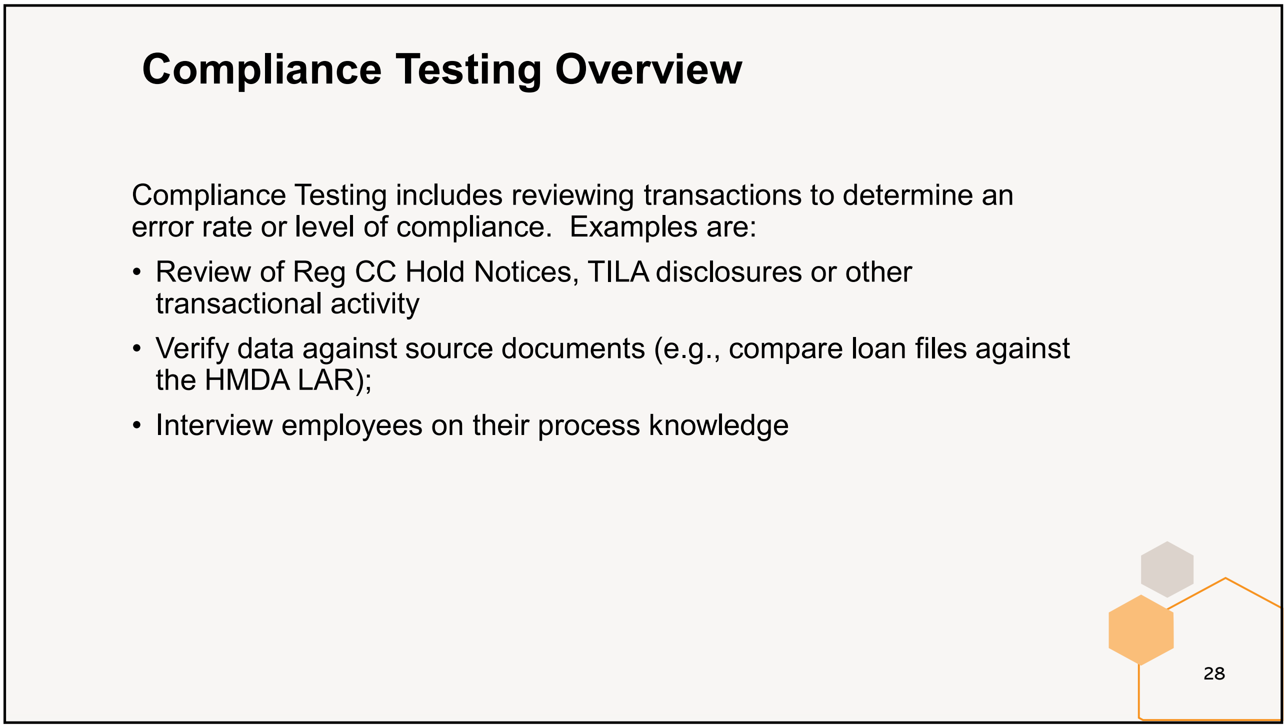
Other Detective Controls

Quality Control

Audit

Regulators

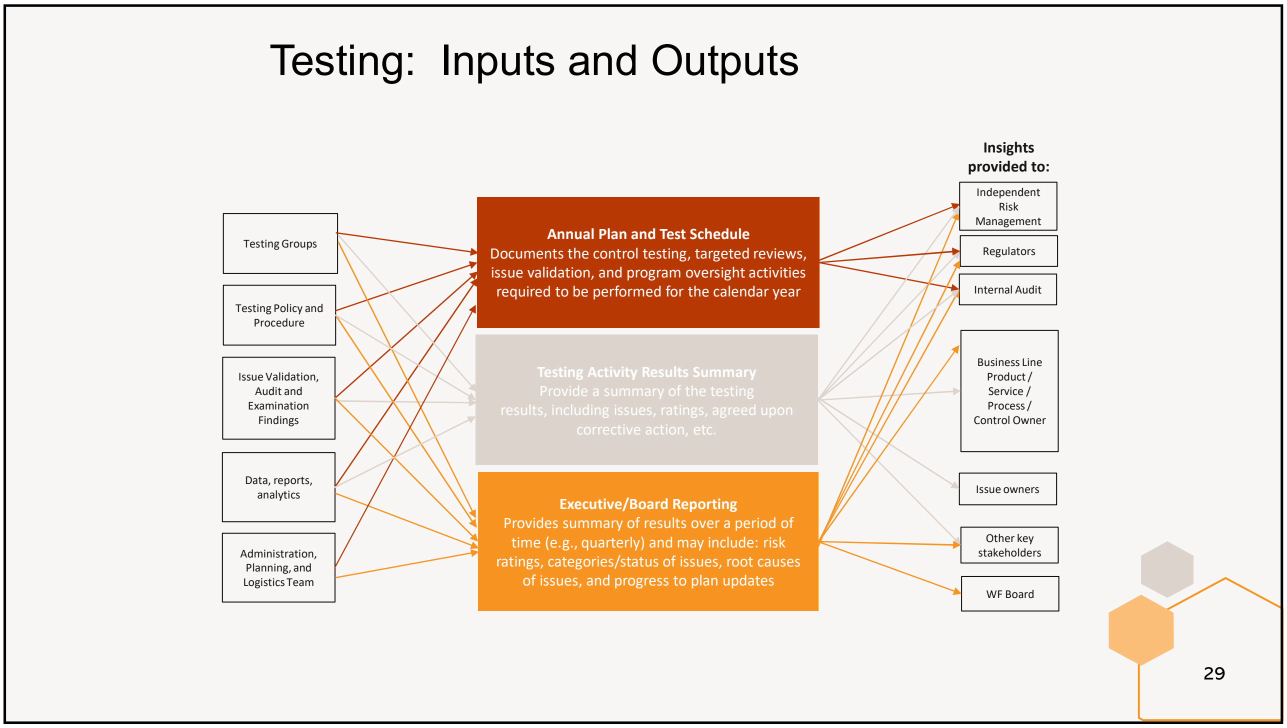
Combined Activities Helps to Draw Conclusions about Overall Risk



Compliance Testing Overview

Compliance Testing includes reviewing transactions to determine an error rate or level of compliance. Examples are:

- Review of Reg CC Hold Notices, TILA disclosures or other transactional activity
- Verify data against source documents (e.g., compare loan files against the HMDA LAR);
- Interview employees on their process knowledge



Testing: Inputs and Outputs

Testing Groups

Testing Policy and Procedure

Issue Validation, Audit and Examination Findings

Data, reports, analytics

Administration, Planning, and Logistics Team

Annual Plan and Test Schedule
Documents the control testing, targeted reviews, issue validation, and program oversight activities required to be performed for the calendar year

Testing Activity Results Summary
Provide a summary of the testing results, including issues, ratings, agreed upon corrective action, etc.

Executive/Board Reporting
Provides summary of results over a period of time (e.g., quarterly) and may include: risk ratings, categories/status of issues, root causes of issues, and progress to plan updates

Insights provided to:

Independent Risk Management

Regulators

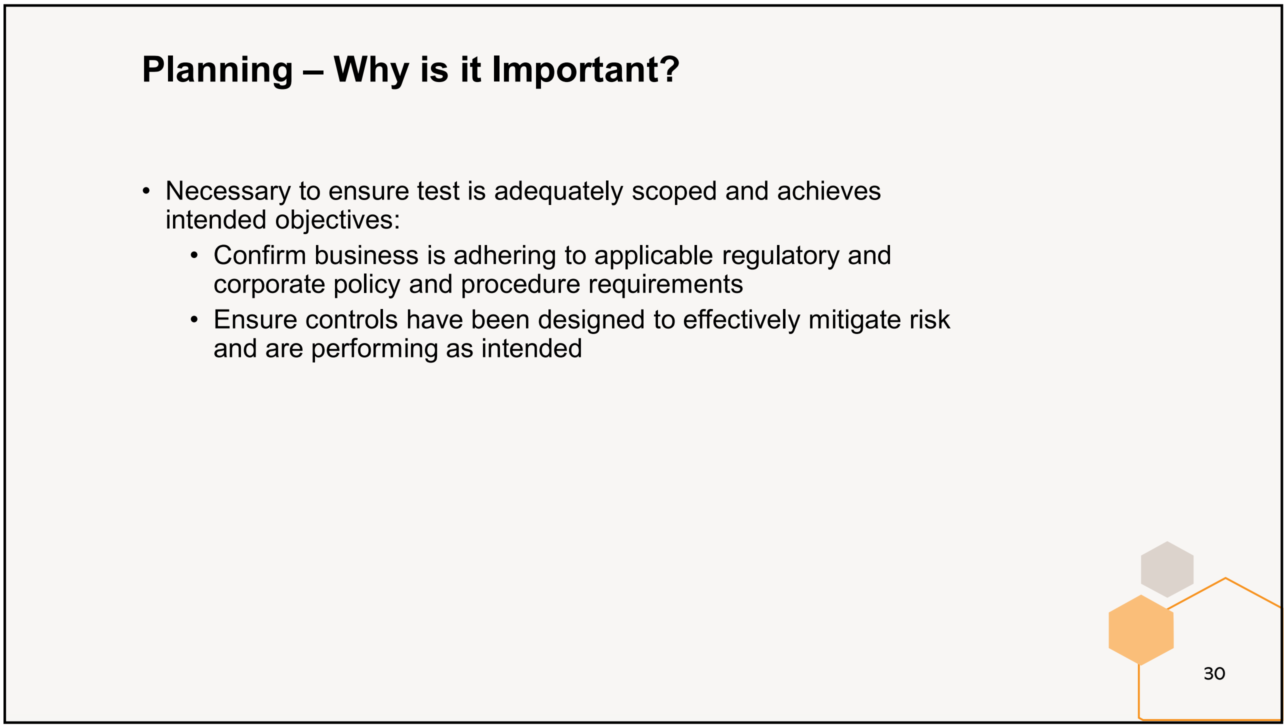
Internal Audit

Business Line Product / Service / Process / Control Owner

Issue owners

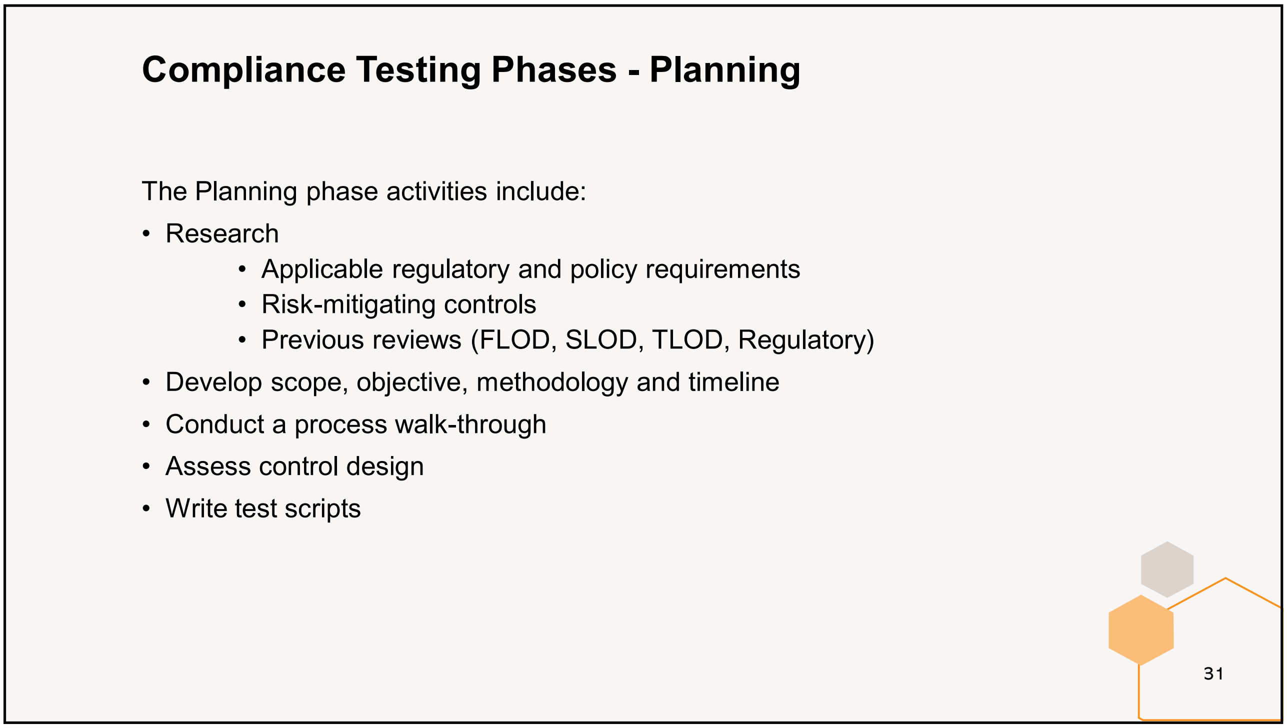
Other key stakeholders

WF Board



Planning – Why is it Important?

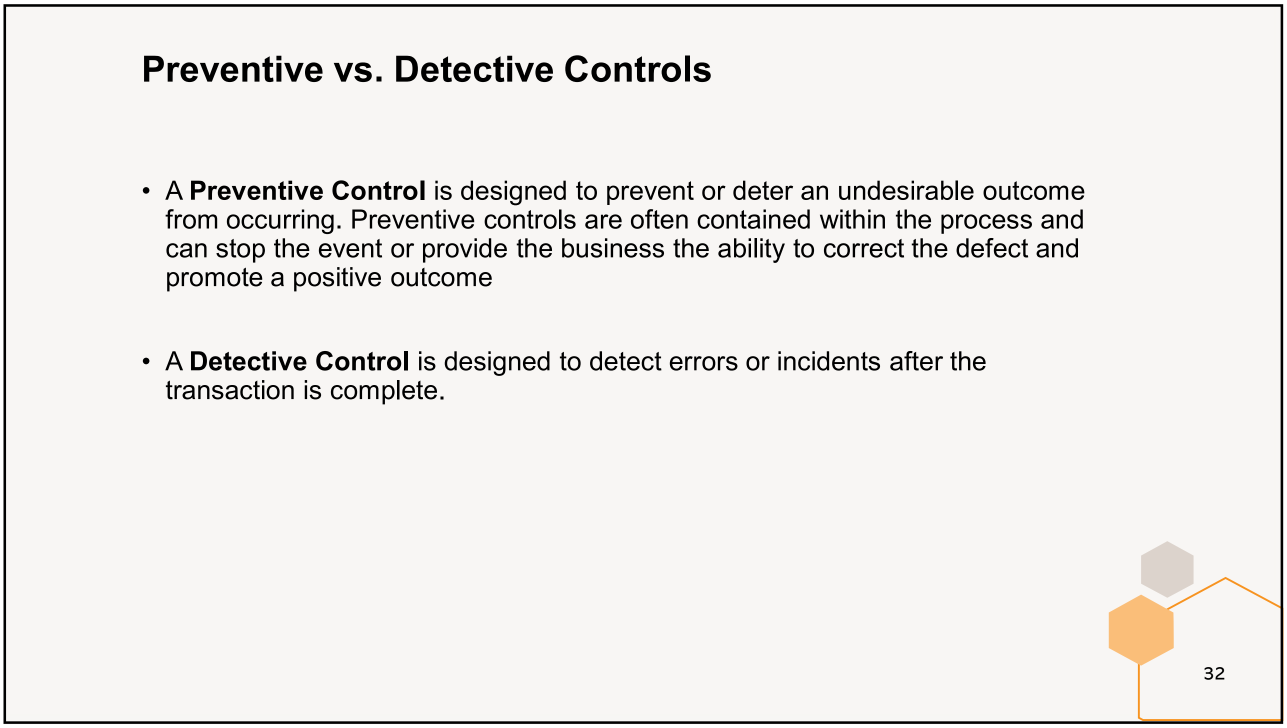
- Necessary to ensure test is adequately scoped and achieves intended objectives:
  - Confirm business is adhering to applicable regulatory and corporate policy and procedure requirements
  - Ensure controls have been designed to effectively mitigate risk and are performing as intended



Compliance Testing Phases - Planning

The Planning phase activities include:

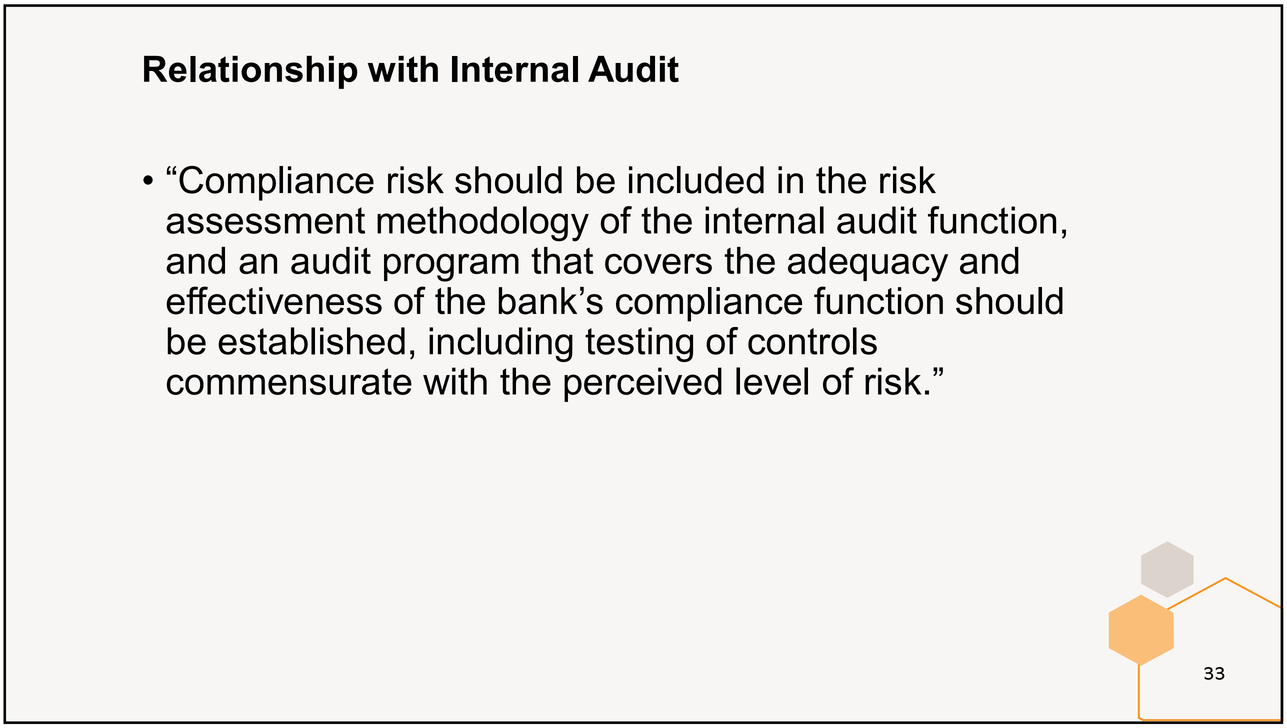
- Research
  - Applicable regulatory and policy requirements
  - Risk-mitigating controls
  - Previous reviews (FLOD, SLOD, TLOD, Regulatory)
- Develop scope, objective, methodology and timeline
- Conduct a process walk-through
- Assess control design
- Write test scripts



Preventive vs. Detective Controls

- A **Preventive Control** is designed to prevent or deter an undesirable outcome from occurring. Preventive controls are often contained within the process and can stop the event or provide the business the ability to correct the defect and promote a positive outcome

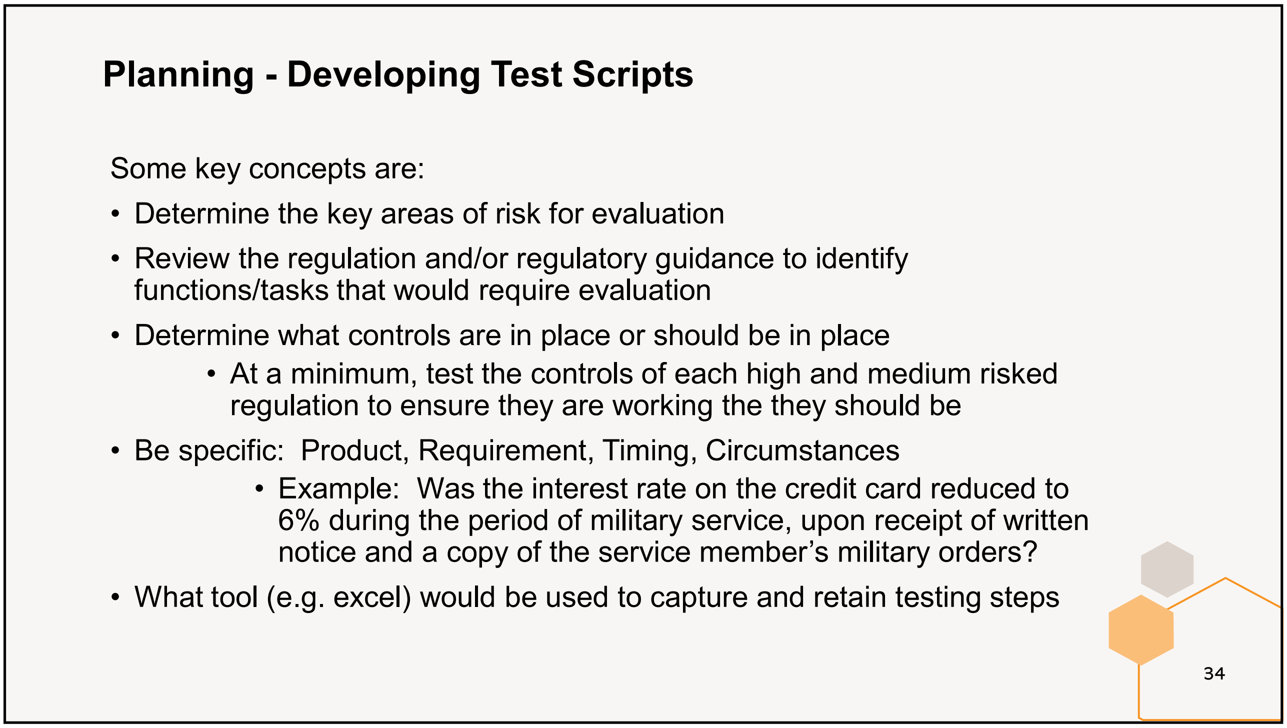
- A **Detective Control** is designed to detect errors or incidents after the transaction is complete.



Relationship with Internal Audit

- “Compliance risk should be included in the risk assessment methodology of the internal audit function, and an audit program that covers the adequacy and effectiveness of the bank’s compliance function should be established, including testing of controls commensurate with the perceived level of risk.”

33

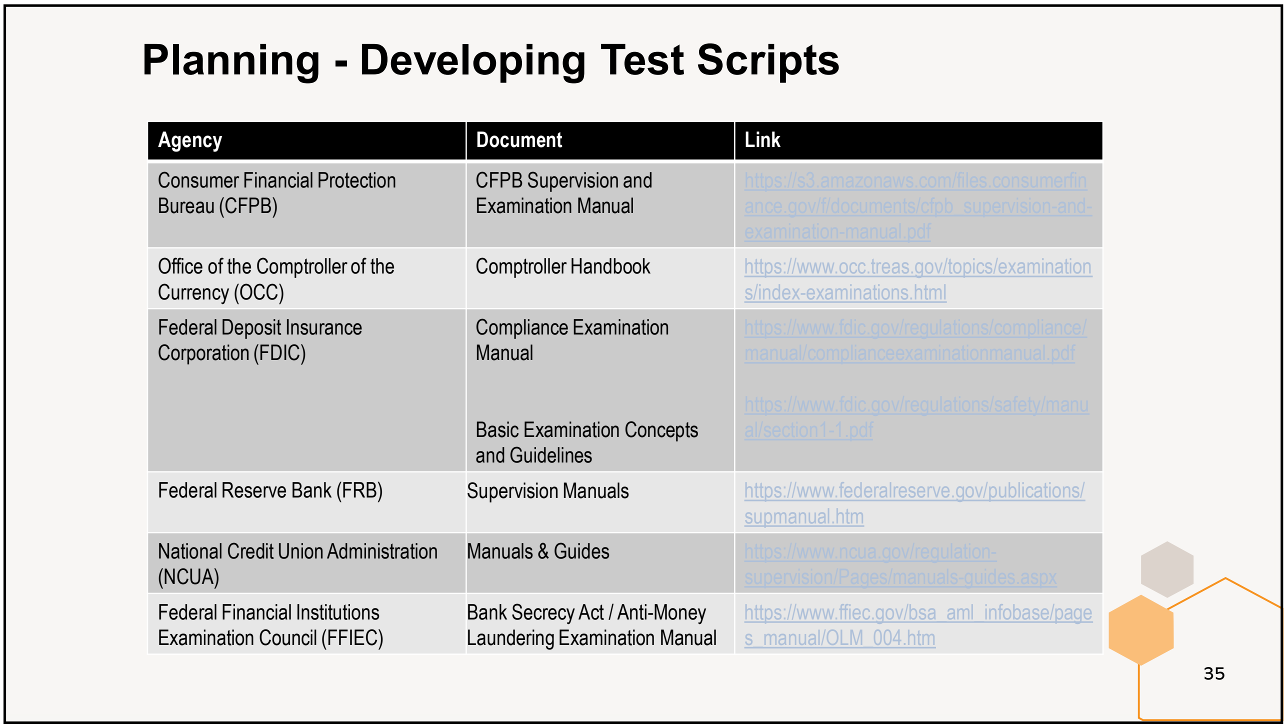


Planning - Developing Test Scripts

Some key concepts are:

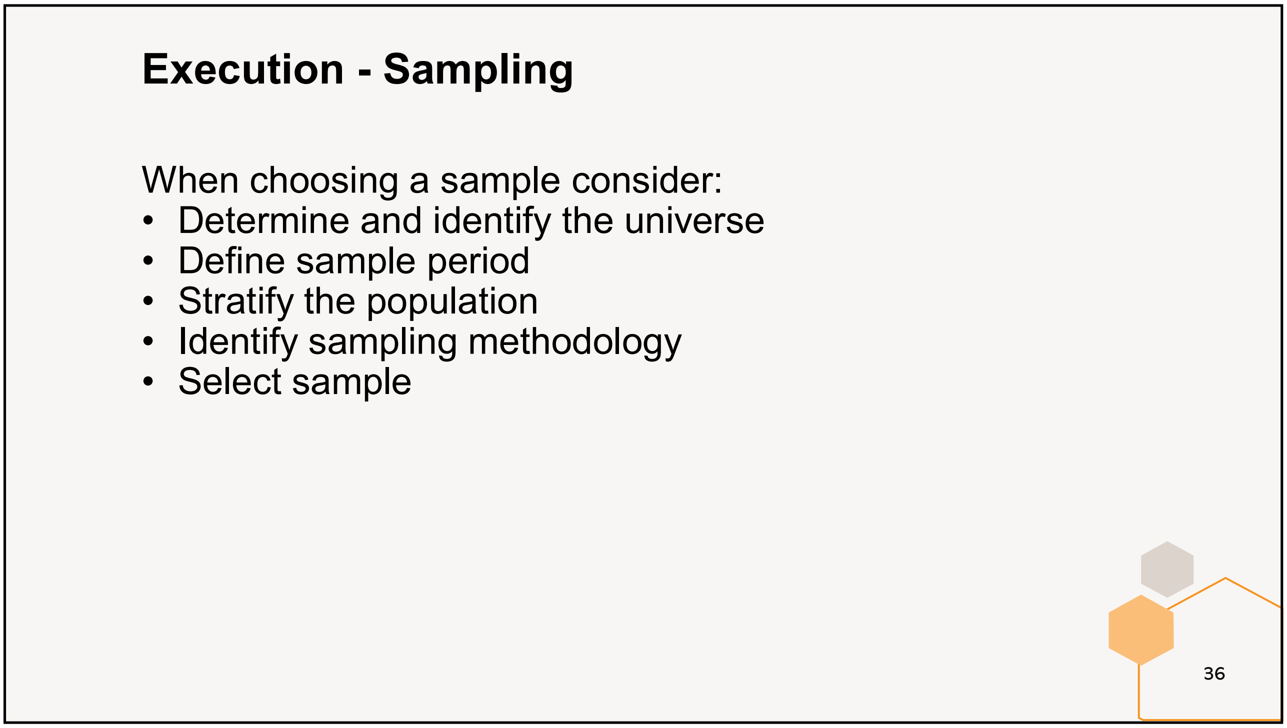
- Determine the key areas of risk for evaluation
- Review the regulation and/or regulatory guidance to identify functions/tasks that would require evaluation
- Determine what controls are in place or should be in place
  - At a minimum, test the controls of each high and medium risked regulation to ensure they are working the they should be
- Be specific: Product, Requirement, Timing, Circumstances
  - Example: Was the interest rate on the credit card reduced to 6% during the period of military service, upon receipt of written notice and a copy of the service member’s military orders?
- What tool (e.g. excel) would be used to capture and retain testing steps

34



Planning - Developing Test Scripts

Agency	Document	Link
Consumer Financial Protection Bureau (CFPB)	CFPB Supervision and Examination Manual	https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb_supervision-and-examination-manual.pdf
Office of the Comptroller of the Currency (OCC)	Comptroller Handbook	https://www.occ.treas.gov/topics/examinations/index-examinations.html
Federal Deposit Insurance Corporation (FDIC)	Compliance Examination Manual Basic Examination Concepts and Guidelines	https://www.fdic.gov/regulations/compliance/manual/complianceexaminationmanual.pdf https://www.fdic.gov/regulations/safety/manual/section1-1.pdf
Federal Reserve Bank (FRB)	Supervision Manuals	https://www.federalreserve.gov/publications/supmanual.htm
National Credit Union Administration (NCUA)	Manuals & Guides	https://www.ncua.gov/regulation-supervision/Pages/manuals-guides.aspx
Federal Financial Institutions Examination Council (FFIEC)	Bank Secrecy Act / Anti-Money Laundering Examination Manual	https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_004.htm



Execution - Sampling

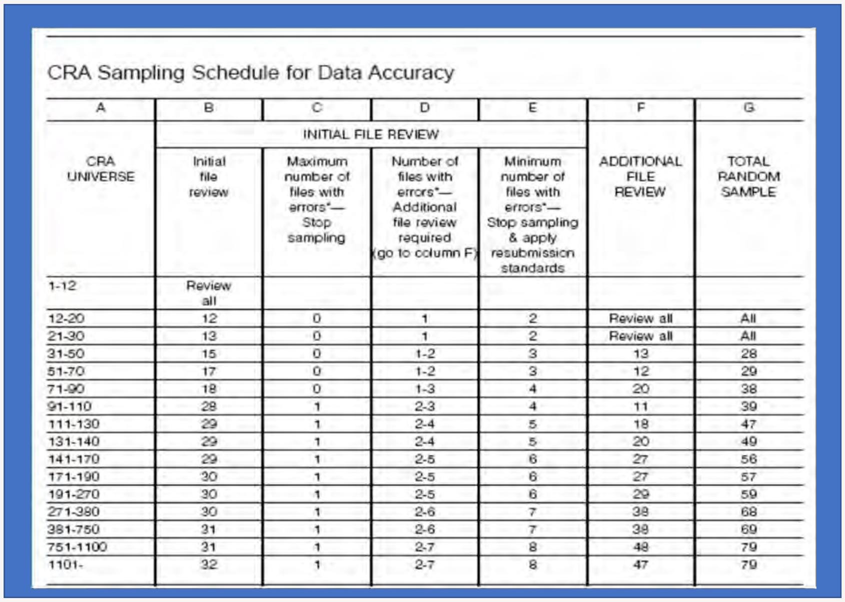
When choosing a sample consider:

- Determine and identify the universe
- Define sample period
- Stratify the population
- Identify sampling methodology
- Select sample

Execution – Sampling Methodologies

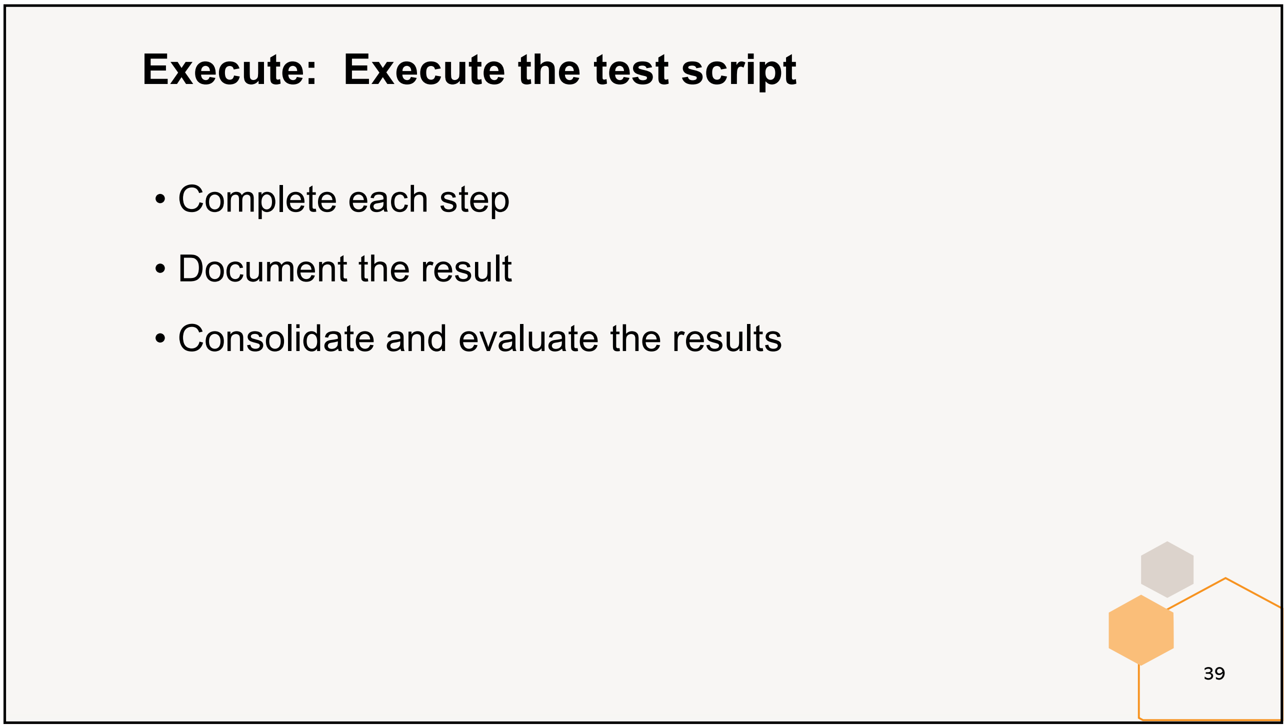
- Statistical
  - Equal chance of being selected
  - Allows for statistically valid conclusions regarding population
  - Uses assumptions for precision, confidence level and error rate
- Non-Statistical –
  - Uses sound judgement without statistical measurement
  - Relies on knowledge of policies, controls and systems to identify areas of risk exposure to select subjectively
  - Sample size must be sufficient to make an assessment of effectiveness

Statistically Valid Sampling (example)



CRA Sampling Schedule for Data Accuracy

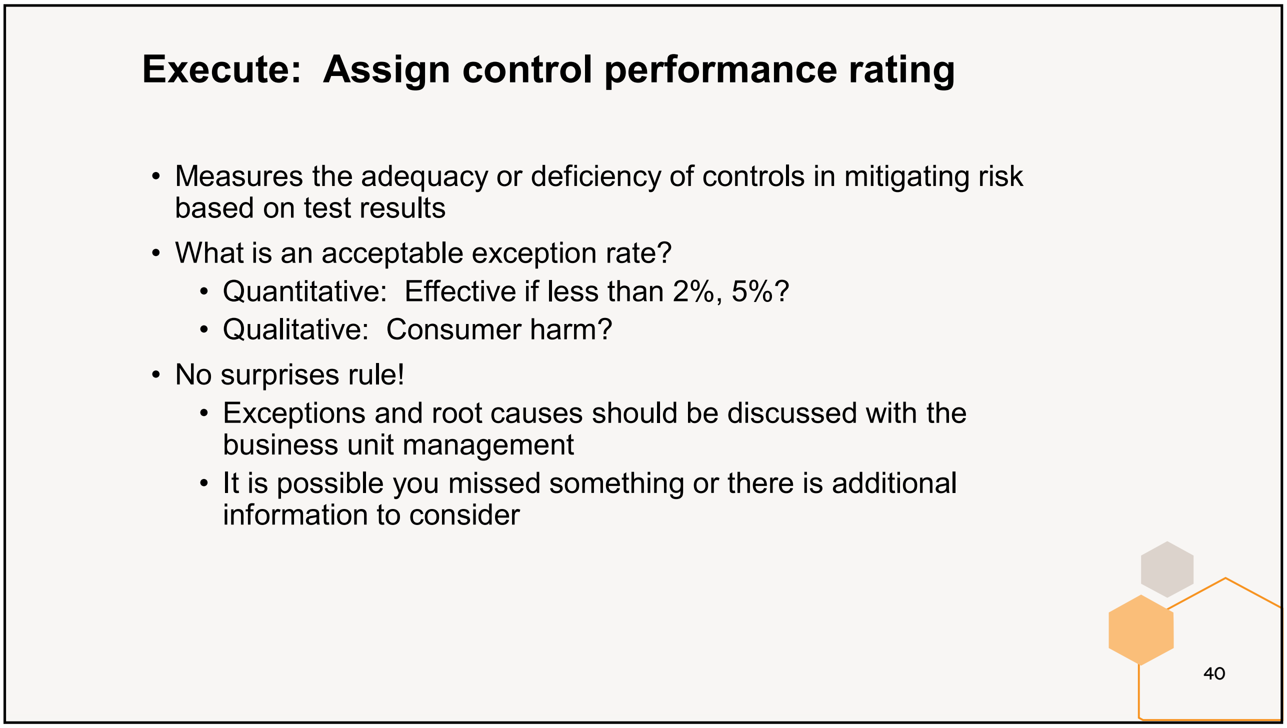
A	B	C	D	E	F	G
	INITIAL FILE REVIEW					
CRA UNIVERSE	Initial file review	Maximum number of files with errors*—Stop sampling	Number of files with errors*—Additional file review required (go to column F)	Minimum number of files with errors*—Stop sampling & apply resubmission standards	ADDITIONAL FILE REVIEW	TOTAL RANDOM SAMPLE
1-12	Review all					
12-20	12	0	1	2	Review all	All
21-30	13	0	1	2	Review all	All
31-50	15	0	1-2	3	13	28
51-70	17	0	1-2	3	12	29
71-90	18	0	1-3	4	20	38
91-110	28	1	2-3	4	11	39
111-130	29	1	2-4	5	18	47
131-140	29	1	2-4	5	20	49
141-170	29	1	2-5	6	27	56
171-190	30	1	2-5	6	27	57
191-270	30	1	2-5	6	29	59
271-380	30	1	2-6	7	38	68
381-750	31	1	2-6	7	38	69
751-1100	31	1	2-7	8	48	79
1101-	32	1	2-7	8	47	79



Execute: Execute the test script

- Complete each step
- Document the result
- Consolidate and evaluate the results

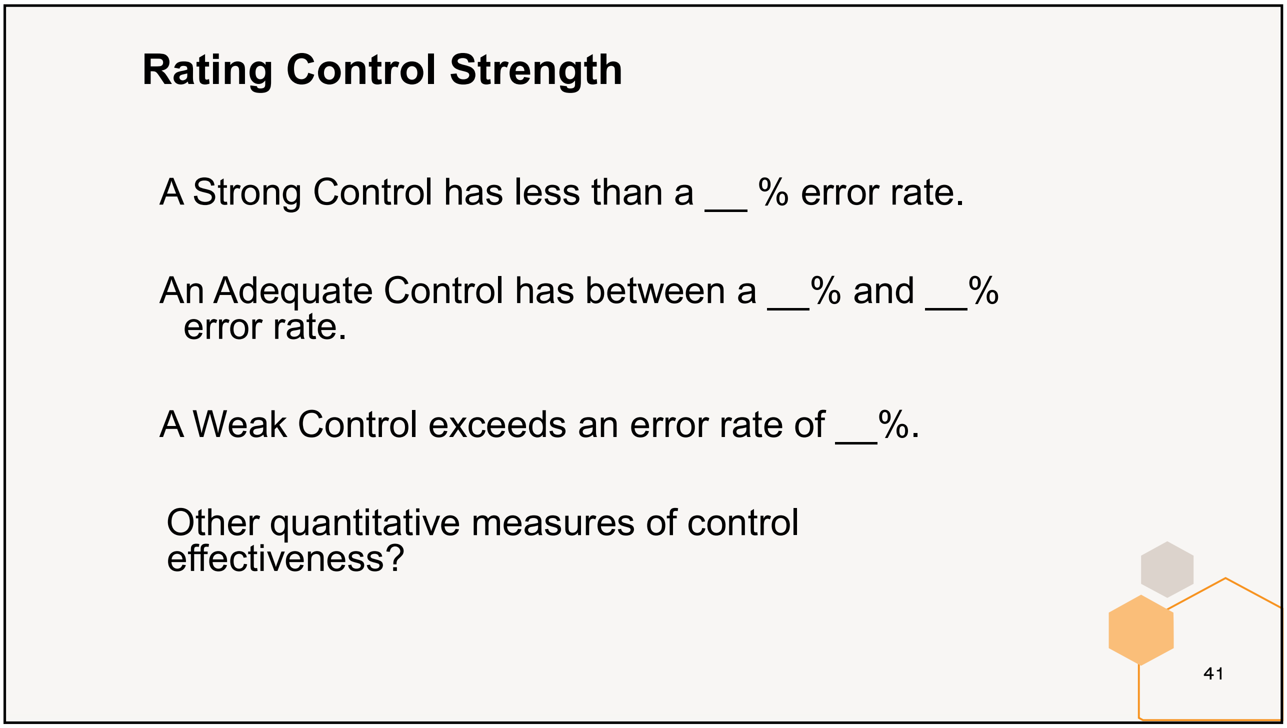
39



Execute: Assign control performance rating

- Measures the adequacy or deficiency of controls in mitigating risk based on test results
- What is an acceptable exception rate?
  - Quantitative: Effective if less than 2%, 5%?
  - Qualitative: Consumer harm?
- No surprises rule!
  - Exceptions and root causes should be discussed with the business unit management
  - It is possible you missed something or there is additional information to consider

40



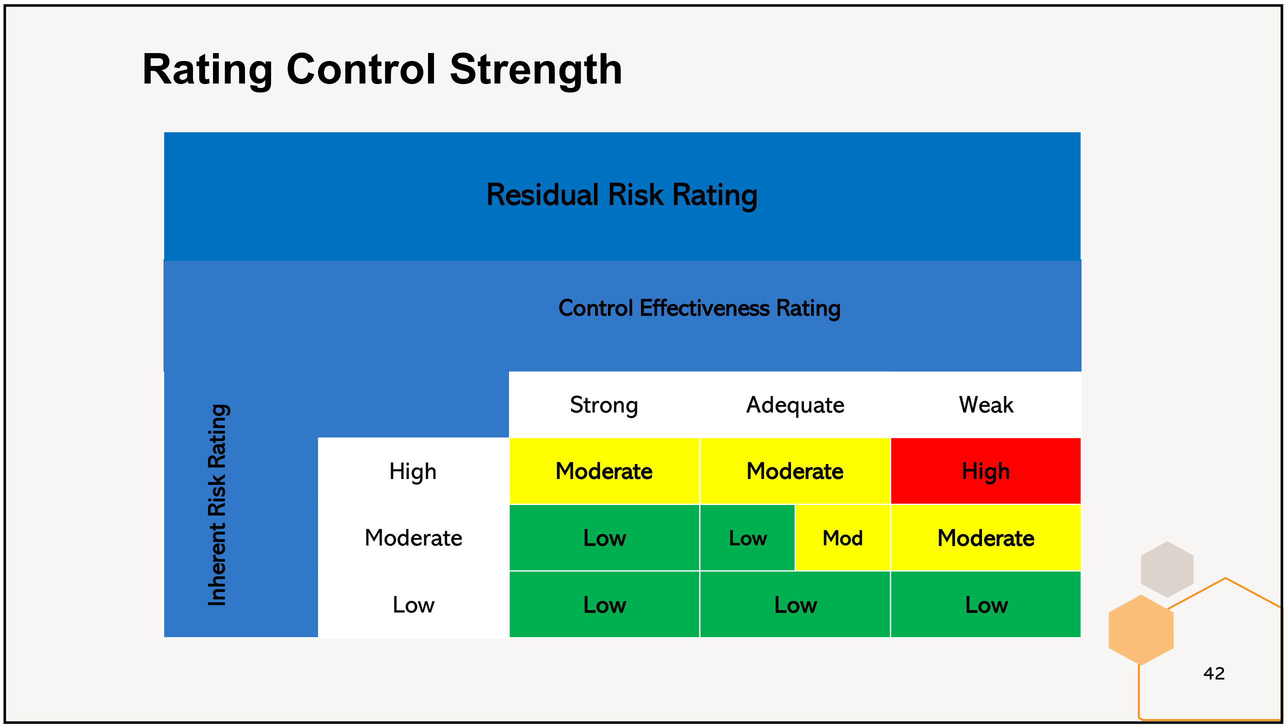
Rating Control Strength

A Strong Control has less than a __ % error rate.

An Adequate Control has between a __% and __% error rate.

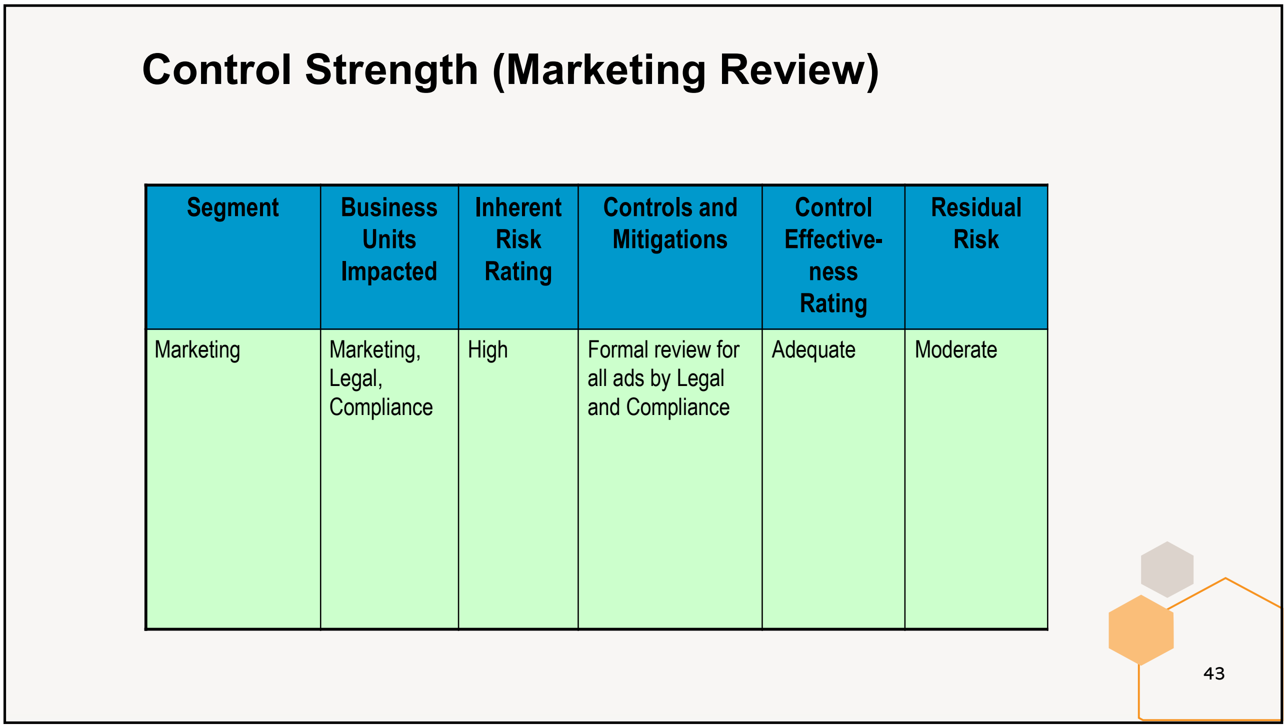
A Weak Control exceeds an error rate of __%.

Other quantitative measures of control effectiveness?



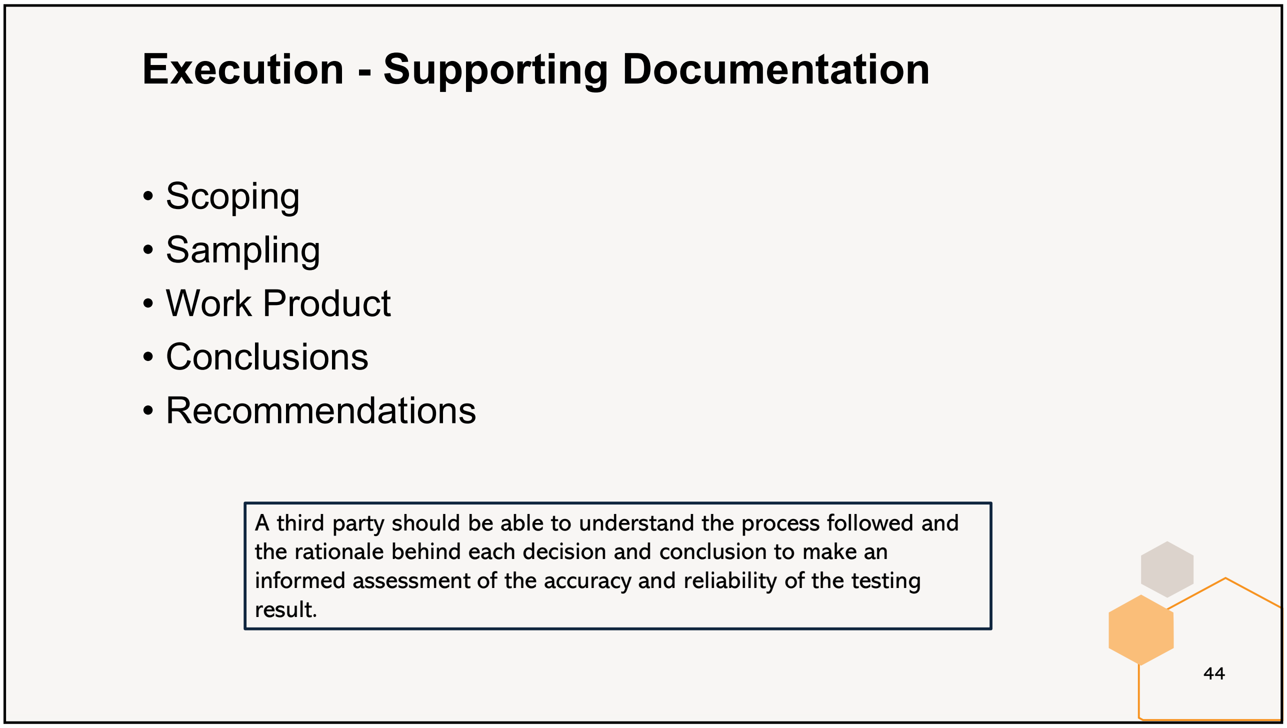
Rating Control Strength

Residual Risk Rating				
		Control Effectiveness Rating		
		Strong	Adequate	Weak
Inherent Risk Rating	High	Moderate	Moderate	High
	Moderate	Low	Low Mod	Moderate
	Low	Low	Low	Low



Control Strength (Marketing Review)

Segment	Business Units Impacted	Inherent Risk Rating	Controls and Mitigations	Control Effective-ness Rating	Residual Risk
Marketing	Marketing, Legal, Compliance	High	Formal review for all ads by Legal and Compliance	Adequate	Moderate



Execution - Supporting Documentation

- Scoping
- Sampling
- Work Product
- Conclusions
- Recommendations

A third party should be able to understand the process followed and the rationale behind each decision and conclusion to make an informed assessment of the accuracy and reliability of the testing result.

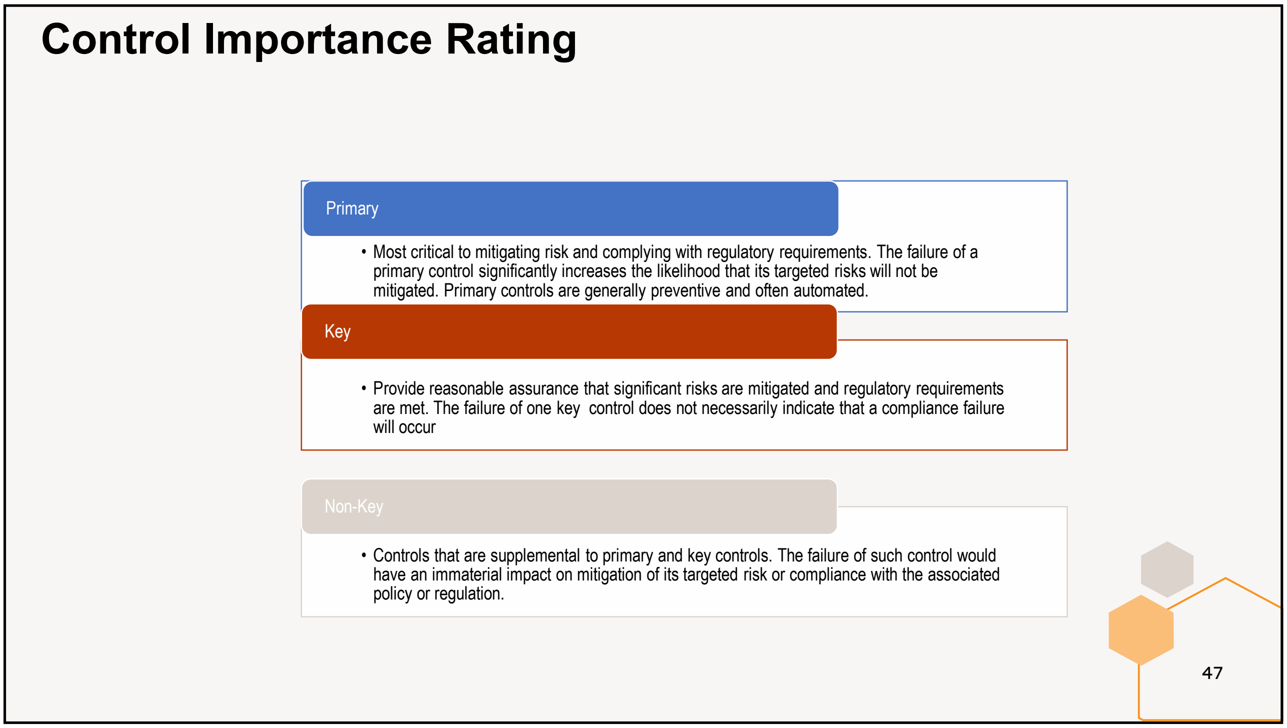
The Importance of Controls

- Control Importance Rating
- Control Placement
- Control Design
- Control Frequency

What is a control?

Defining a control

Specific activities and tools that serve to avoid, manage, and mitigate risks, reducing their impact to the company and its operation



Control Importance Rating

Primary

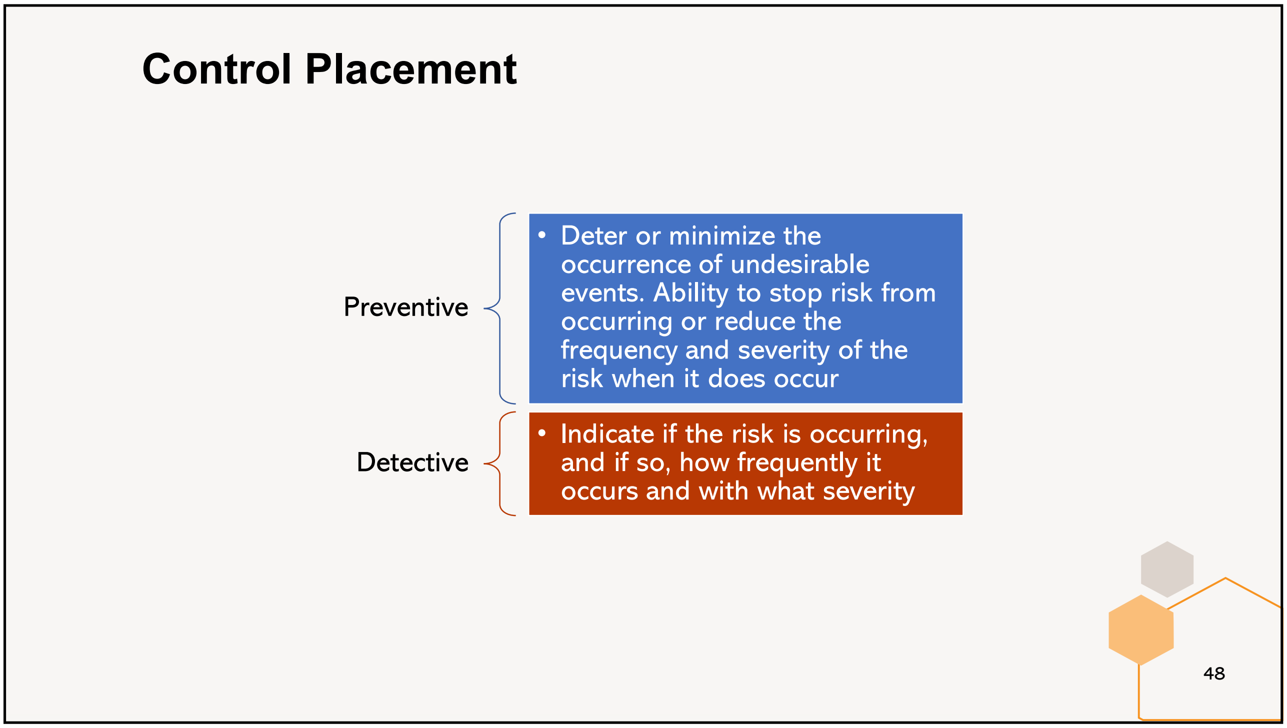
- Most critical to mitigating risk and complying with regulatory requirements. The failure of a primary control significantly increases the likelihood that its targeted risks will not be mitigated. Primary controls are generally preventive and often automated.

Key

- Provide reasonable assurance that significant risks are mitigated and regulatory requirements are met. The failure of one key control does not necessarily indicate that a compliance failure will occur

Non-Key

- Controls that are supplemental to primary and key controls. The failure of such control would have an immaterial impact on mitigation of its targeted risk or compliance with the associated policy or regulation.



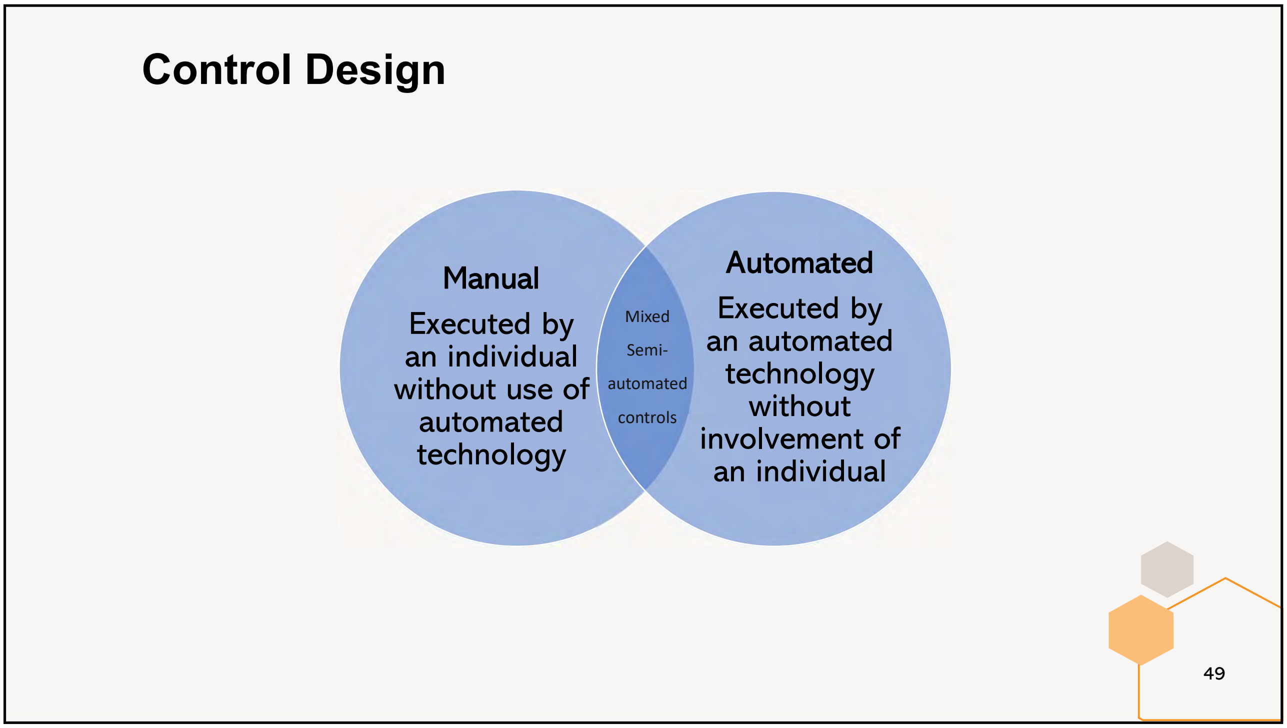
Control Placement

Preventive

- Deter or minimize the occurrence of undesirable events. Ability to stop risk from occurring or reduce the frequency and severity of the risk when it does occur

Detective

- Indicate if the risk is occurring, and if so, how frequently it occurs and with what severity



Control Design

Manual

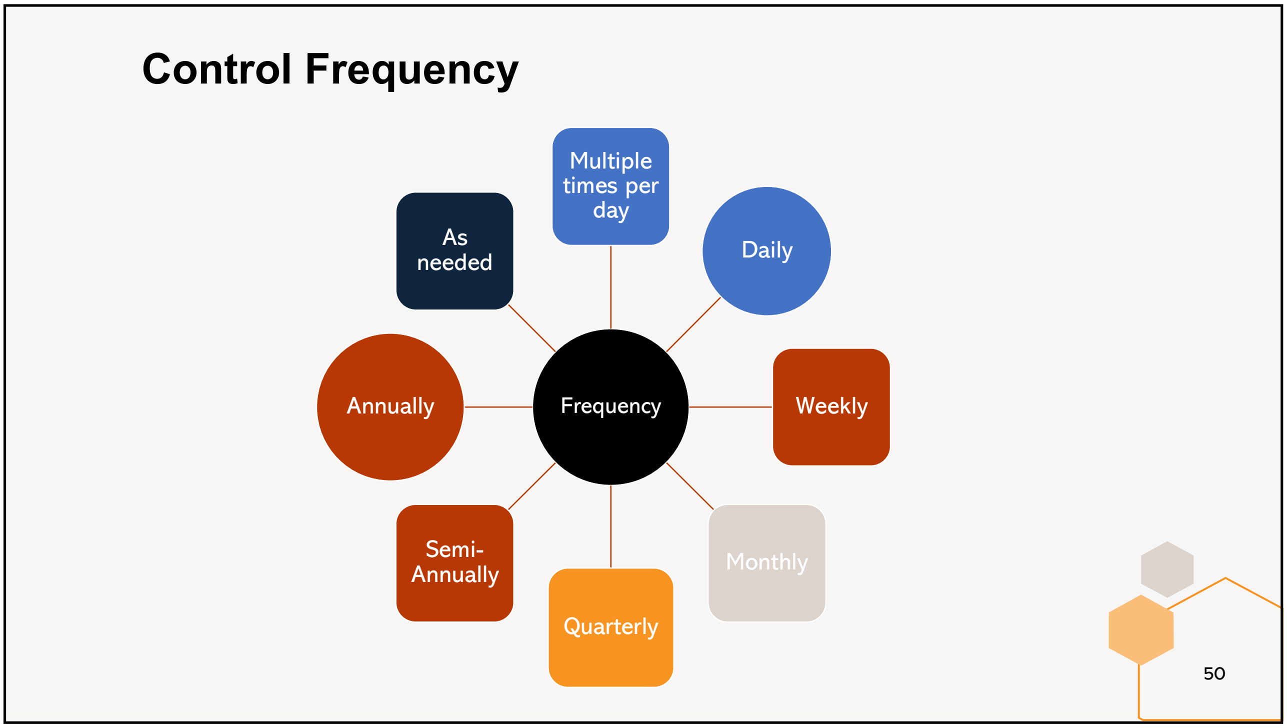
Executed by an individual without use of automated technology

Mixed

Semi-automated controls

Automated

Executed by an automated technology without involvement of an individual



Control Frequency

Frequency

Multiple times per day

Daily

Weekly

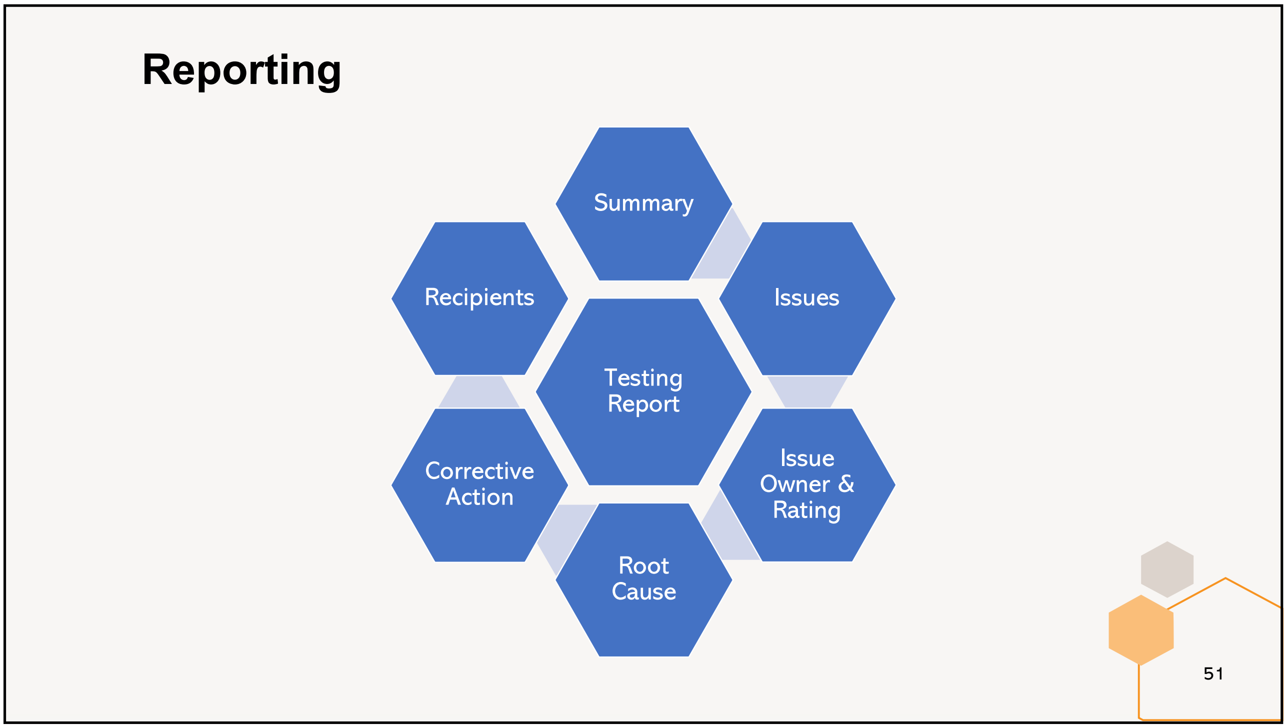
Monthly

Quarterly

Semi-Annually

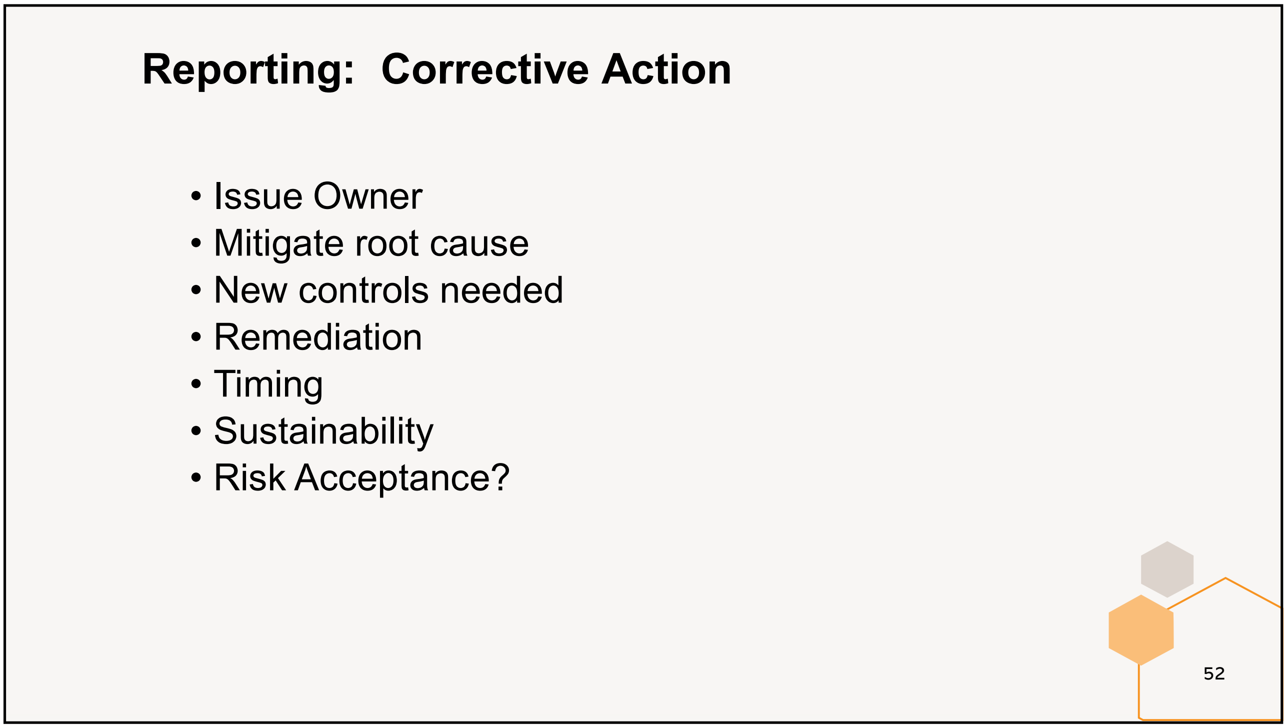
Annually

As needed



Reporting

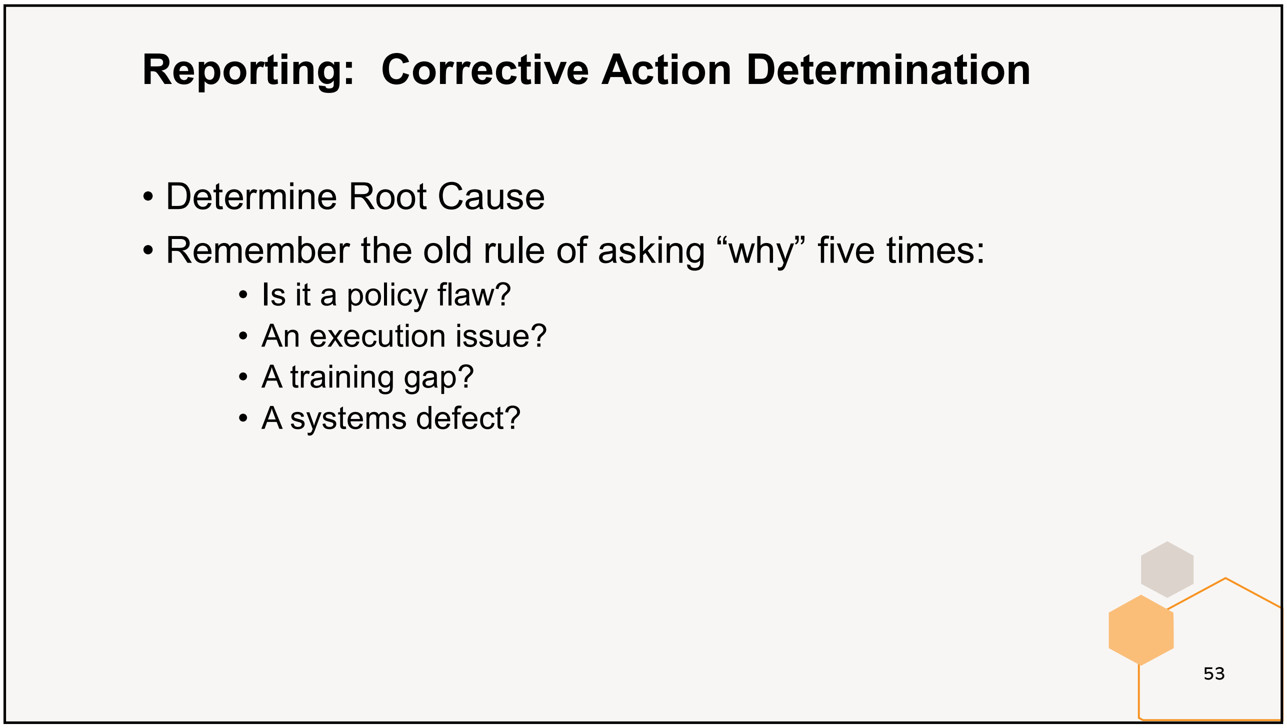
51



Reporting: Corrective Action

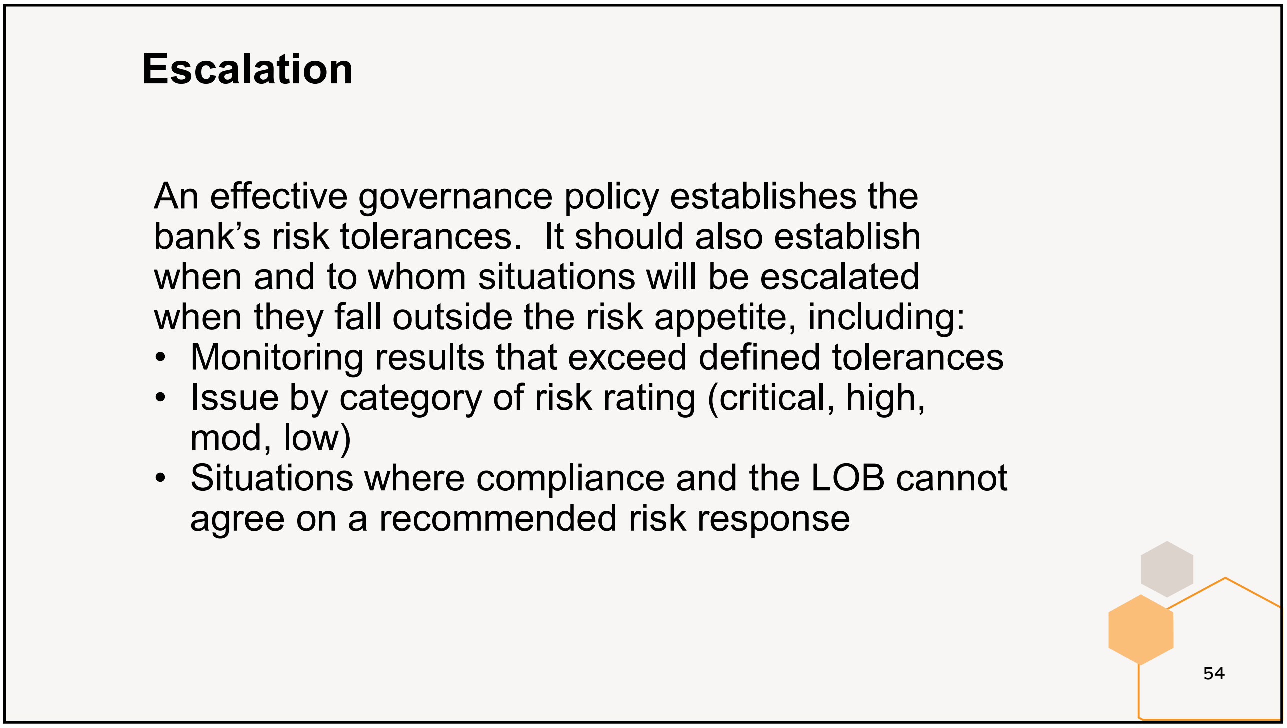
- Issue Owner
- Mitigate root cause
- New controls needed
- Remediation
- Timing
- Sustainability
- Risk Acceptance?

52



Reporting: Corrective Action Determination

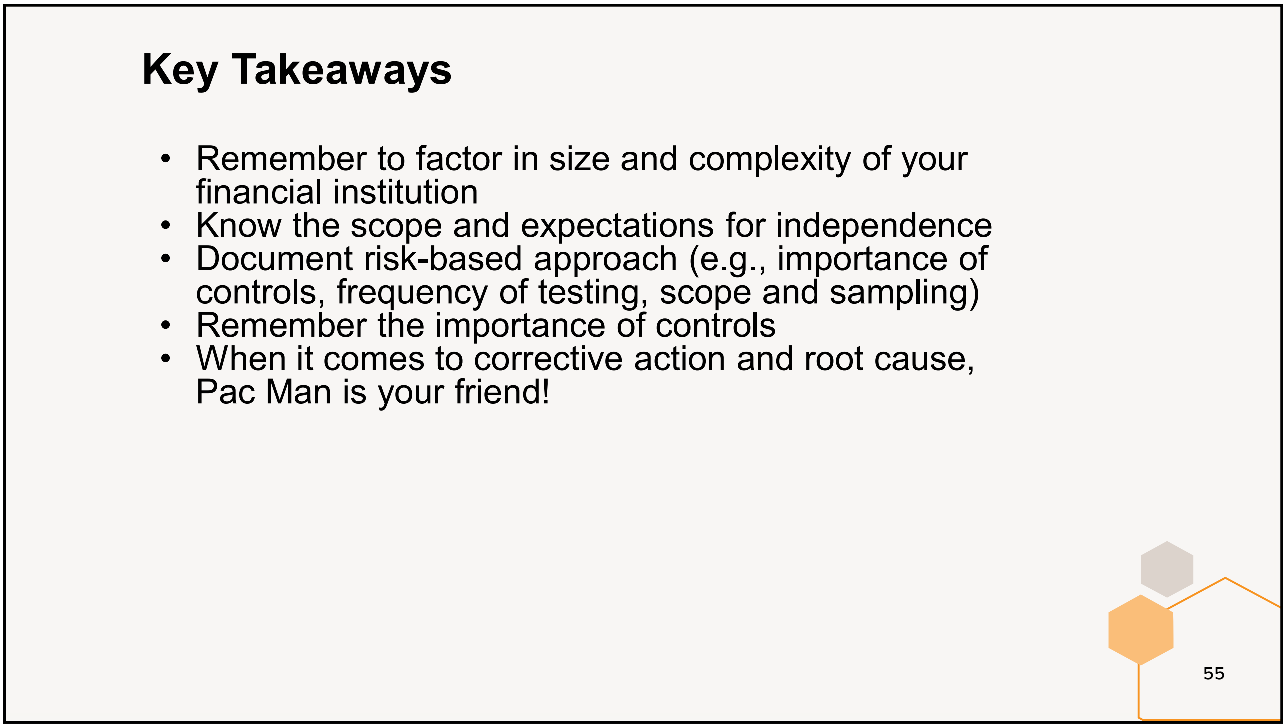
- Determine Root Cause
- Remember the old rule of asking “why” five times:
  - Is it a policy flaw?
  - An execution issue?
  - A training gap?
  - A systems defect?



Escalation

An effective governance policy establishes the bank’s risk tolerances. It should also establish when and to whom situations will be escalated when they fall outside the risk appetite, including:

- Monitoring results that exceed defined tolerances
- Issue by category of risk rating (critical, high, mod, low)
- Situations where compliance and the LOB cannot agree on a recommended risk response



Key Takeaways

- Remember to factor in size and complexity of your financial institution
- Know the scope and expectations for independence
- Document risk-based approach (e.g., importance of controls, frequency of testing, scope and sampling)
- Remember the importance of controls
- When it comes to corrective action and root cause, Pac Man is your friend!

Financial Solutions

Patti D. Joyner, CRCM

www.finsolinc.com

Patti.Joyner@finsolinc.com

Many thanks to Thomas Healy!!

The Best Compliance KPIs to Track: Benchmarking and Metrics

PLANERGY™
The Best Compliance KPIs To Track: Benchmarking And Metrics
Monitor And Manage Risk More Effectively

Digital disruption has shifted global economic priorities and fundamentally altered the ways in which companies approach everything from strategic decision-making to business process optimization to risk management.

The need to capture, organize, and analyze Big Data in order to obtain actionable insights has made the use of tools such as key performance indicators (KPIs) an essential part of every proactive and successful business management plan.

One of the most important areas where KPIs are used is compliance management.

Compliance KPIs help companies develop effective compliance programs supported by intelligent risk assessment.

By carefully monitoring these KPIs, compliance officers can avoid the costly headaches that come with non-compliance, identify the root causes of compliance issues, and better insulate their organizations against potential risks.

Compliance KPIs and Why They Matter

Doing business in the modern global economy isn't exactly a walk in the park. Internal and external stakeholders expect (and demand) optimal performance, profitability, and compliance—all backed by absolute transparency.

Companies regularly find themselves adapting to unpredictable changes in government and industry regulations related to risk and compliance.

New risks to profitability, reputation, and compliance appear with frequent (and frightening) regularity, and the costs that come with assessing and managing these risks can be daunting.

Data-driven, forward-minded, and dedicated to optimization across all business processes using continuous improvement, today's business leaders need effective risk assessment and risk management tools if they want to stay ahead of the competition.

A specific set of metrics designed to measure how well an organization's compliance department is maintaining that same organization's compliance with internal and external policies, along with industry and government regulations, compliance KPIs are essential to protecting your business *and* helping it expand beyond its current capabilities.

Tracking these KPIs and adjusting compliance policies and workflows accordingly helps compliance officers manage risk more effectively through the use of internal audits, policy enforcement, and compliance training at all levels of their organizations.

Compliance KPIs can be used to measure:

- Governance, Risk Management, and Compliance (GRC) standards for operational excellence.
- Financial compliance, including internal and external audit management.
- Data storage and management compliance.
- Purchasing compliance.

Compliance KPIs can be considered “watchdogs” or “early warning systems” for potential risk exposure. The term *key risk indicators* (KRIs) is also used for some compliance metrics.

No two organizations will share identical priorities with regard to risk mitigation, but businesses of all sizes can benefit from a compliance program built around measuring, evaluating, and adjusting workflows and policies with the help of compliance KPIs.

> *A specific set of metrics designed to measure how well an organization’s compliance department is maintaining that same organization’s compliance with internal and external policies, along with industry and government regulations, compliance KPIs are essential to protecting your business and helping it expand beyond its current capabilities.*

Benefits of Monitoring Compliance KPIs

Much like their counterparts in the procurement and accounts payable (AP) functions, compliance professionals rely on clear, accurate, and complete data to perform their jobs effectively.

They rely on this same data to evaluate the overall success of their efforts, and to guide the organization away from potential problems before they become actual disasters.

In procurement, rogue spend, lack of training, and non-compliance with procurement policies can obscure the data essential to effective spend management and financial planning, making it difficult to maintain adequate cash flow, capture value and savings through strategic spend, or build a resilient supply chain to protect business continuity.

The same is true for compliance, where a poorly executed compliance program can leave organizations at risk of reputational damage, costly fines and fees, or potential litigation and regulatory intervention.

Toward that goal, best-in-class companies are increasingly choosing to implement digital tools designed to streamline and optimize compliance management—including tracking compliance KPIs.

A compliance management solution such as Planergy, for example, provides intuitive and flexible tools that support the creation, monitoring, and refinement of your most important compliance KPIs through:

- Comprehensive, audit-friendly budgeting tools.
- Guided buying and flexible approval controls for transparent control over spend.
- Automatic three-way matching and contract compliance tools.
- GRC-friendly automation and workflow management.
- Centralized, cloud-based data collection and management.
- Best-in-class data security compliance to minimize cybersecurity-related risks.
- Vendor relationship management tools to track and evaluate vendor performance and compliance.

When companies track and refine their compliance KPIs effectively, they can expect:

- Lower costs and greater value.

- Greater operational efficiency and productivity.
- Complete, high quality information on business processes, gathered more quickly.
- Greater consistency and compliance across the entire organization.
- Stronger competitive performance through reduced risk and optimized workflows.

Best Practices for Using Compliance KPIs

To address compliance issues effectively, senior management needs a compliance program that not only identifies potential risks, but helps ferret out and correct their root causes.

Following a few best practices will strengthen your compliance policies and ensure you're making optimal use of the compliance metrics you're tracking.

1. Develop and Implement a Performance Rating System Using Needs Analysis.

Before you can get your compliance program up and running, you need to know where your organization currently stands with regard to compliance.

Using needs analysis and risk assessment, you can identify your current compliance program effectiveness and then build your program based on the business objectives you'd like to achieve.

When evaluating your current compliance ecosystem, your ranking system might look something like this:

1. **Needs Improvement:** Risk assessment reveals excess risk that is inadequately mitigated or completely uncontrolled. Internal controls and compliance policies are inconsistently applied, inefficient, or subject to

frequent failure.

2. **Functional:** Compliance protocols are effectively and consistently mitigating identified risks.
3. **Uses Best Practices:** Compliance policies and protocols effectively and consistently mitigate identified risks and provide tools for identifying, assessing, and mitigating potential risks.
4. **Transformational:** Protocols and policies require modification/refresh due to changes to the company's risk profile or as part of a continuous improvement effort to mitigate stagnation.

2. Formalize Your Compliance Program in Writing.

Having everything in black and white not only makes it easier to train your team to follow your new compliance policies and protocols, but also provides a concrete, audit-friendly record for internal and external review.

3. Invest in Compliance Education and Training.

Compliance performance superstars are made, not born. Ensure everyone across your organization has access to thorough training in your compliance programs, with updates and refreshers as needed.

When everyone's on the same page (so to speak), financial, operational, and regulatory compliance are greatly improved. This compliance ensures senior management has the complete and accurate data needed to harvest insights effectively when reviewing compliance KPIs.

4. Start with Broad Compliance KPIs and Narrow

Your Focus.

When you're using key performance indicators to manage risk, it's important to have measurability, consistency, *and* adaptability built into your compliance program.

Start with tracking and evaluating your most business-critical compliance KPIs, and then adapt your workflows to develop a more nuanced approach as needed.

Essential Compliance KPIs You Should Be Tracking

Depending on your industry and the type of business you're operating, you could conceivably build hundreds or even thousands of KPIs to track the myriad compliance issues that affect every organization.

From avoiding corruption to ensuring food safety, government agencies offer their own sets of often complex compliance requirements companies must follow to stay on the right side of the law.

Add in industry regulations, internal controls and compliance policies, and the need to comply with third-party requirements such as green business certifications or Energy Star regulations, and the average compliance team can find itself lost in wave after wave of data pouring in from countless sources.

But an effective compliance program isn't built from minutiae. It starts with establishing, measuring, and refining the compliance-related key performance indicators with the biggest impact on operational performance.

Identifying and codifying these KPIs provides a compliance paradigm that guides all subsequent controls and policies.

Ideally, your compliance team will use KPIs that are:

- Drawn from practices and benchmarks informed by needs analysis.
- Developed and implemented consistently across the organization.
- Clear and concise with regard to related risks and their mitigation.
- Readily measurable across within a given period and across business units.
- Designed to assess accountability and performance for risk owners.
- Designed to consume resources with maximum efficiency.

Every business is different, but most organizations can begin to improve their general compliance (and create a paradigm for monitoring more granular KPIs moving forward) by tracking some core compliance KPIs such as:

General Compliance

- Total Number of Compliance Issues Currently Open
- Total Number of Open Employee Relations/Human Resources Issues
- Percentage of Post-Audit Issues Outstanding: Total issues still outstanding after completion of an audit, expressed as a percentage.
- Average Compliance Investigation Cycle Time by Type
- Percentage of Internal Audits Completed On Time

Operational and Systems Compliance

- Mean Time between Failure (MTBF): The total number of minutes (or hours, or days, etc.) since a system or equipment failure.
- Percentage Difference in MBTF: Comparison of failure rates across different systems or units of equipment, expressed as a percentage.
- Mean Time to Repair (MTTR): Average time required to repair issues and return equipment or systems to normal operations. May be referred to as "downtime."

- Percentage Difference in MTTR: A measure of changes to MTTR as an indicator of relative efficiency, expressed as a percentage.
- System Availability: The total number of minutes (or days, hours, etc.) systems or equipment were actually available divided by the total number of minutes they should have been available.

Procurement Compliance

- Ratio of Disputed Invoices to Total Invoices
- Percentage of Invoices Automatically Matched
- Average Invoice Cycle Time
- Average Purchase Order Cycle Time
- Supplier Defect and Compliance Rates: Ratios of accurate and contract-compliant orders completed, respectively.

Effective Compliance Management Reduces Risk Exposure

An ounce of proactive prevention is worth a pound of compliance cure.

Invest in the tools and techniques you need to build a robust, flexible compliance program using targeted KPIs, and your organization will gain competitive strength through more effective risk management and business strategies.

What’s your goal today?

1. Use Planergy to manage purchasing and accounts payable

We’ve helped save billions of dollars for our clients through better spend management, process automation in purchasing and finance, and reducing financial risks. To discover how we can help grow your business:

- Read our case studies, client success stories, and testimonials.
- Visit our “Solutions” page to see the areas of your business we can help improve to see if we’re a good fit for each other.
- Learn about us, and our long history of helping companies just like yours.

Book a Live Demo

2. Download our guide “Preparing Your AP Department For The Future”

Download a free copy of our guide to future proofing your accounts payable department. You’ll also be subscribed to our email newsletter and notified about new articles or if have something interesting to share.

download a free copy of our guide

3. Learn best practices for purchasing, finance, and more

Browse hundreds of articles, containing an amazing number of useful tools, techniques, and best practices. Many readers tell us they would have paid consultants for the advice in these articles.

Related Posts

COMPLYLOG
A EURONEXT COMPANY

11 Key Compliance KPIs + Examples (And Why You Should Track Them)

7 minutes 14 December 2022

If there ever was a time when people accepted that companies were justified in behaving as they liked as long as they made money, those days are long gone. In the wake of events such as the global financial crash and the Libor scandal, as well as the climate crisis, Me Too and Black Lives Matter movements, regulators have sought to continually hone their legislation to reduce wrongdoing. This article discusses compliance KPI examples to help your business remain on the right side of the law.

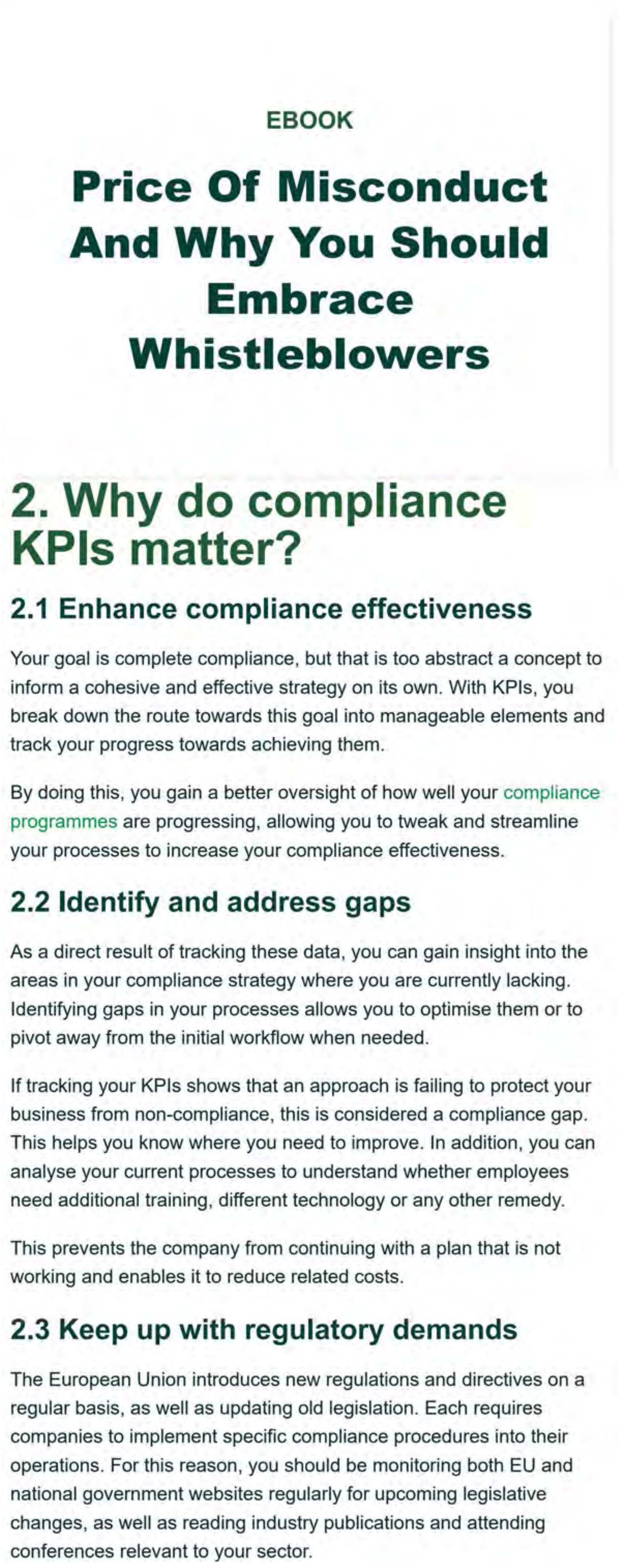
You will find why compliance KPIs are important, what makes a useful KPI and which KPIs you should track for your compliance efforts.

1. What are compliance KPIs?

Compliance key performance indicators, or KPIs, are metrics that help you measure how successful your compliance performance is in relation to your strategic goals. These include how compliant your organisation is in its internal and external policies as well as in terms of the regulatory landscape in which you work.

You can measure the effectiveness of your compliance programmes with KPIs, as well as using them as a monitoring tool to spot and remedy the early signs of non-compliance.

In a data-driven business world, KPIs offer the information you need to quantify how you are progressing towards the strategic aims of the business.



EBOOK

Price Of Misconduct And Why You Should Embrace Whistleblowers

2. Why do compliance KPIs matter?

2.1 Enhance compliance effectiveness

Your goal is complete compliance, but that is too abstract a concept to inform a cohesive and effective strategy on its own. With KPIs, you break down the route towards this goal into manageable elements and track your progress towards achieving them.

By doing this, you gain a better oversight of how well your compliance programmes are progressing, allowing you to tweak and streamline your processes to increase your compliance effectiveness.

2.2 Identify and address gaps

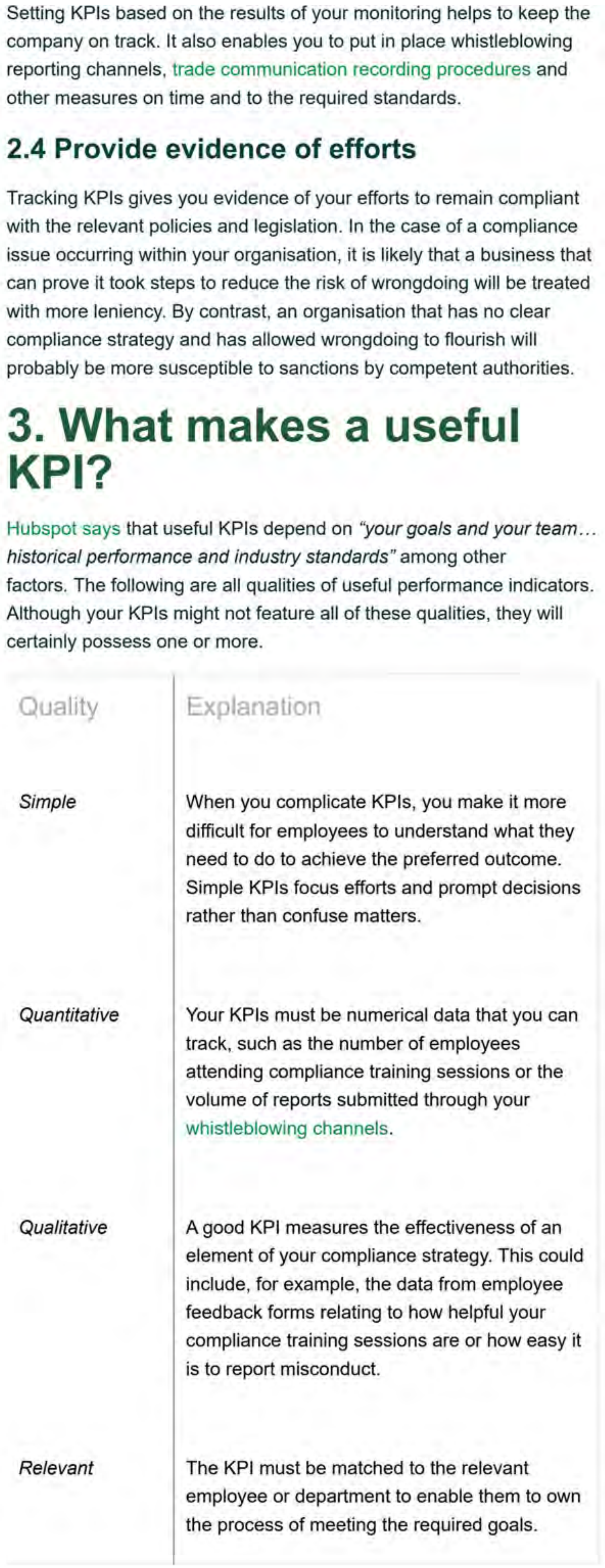
As a direct result of tracking these data, you can gain insight into the areas in your compliance strategy where you are currently lacking. Identifying gaps in your processes allows you to optimise them or to pivot away from the initial workflow when needed.

If tracking your KPIs shows that an approach is failing to protect your business from non-compliance, this is considered a compliance gap. This helps you know where you need to improve. In addition, you can analyse your current processes to understand whether employees need additional training, different technology or any other remedy.

This prevents the company from continuing with a plan that is not working and enables it to reduce related costs.

2.3 Keep up with regulatory demands

The European Union introduces new regulations and directives on a regular basis, as well as updating old legislation. Each requires companies to implement specific compliance procedures into their operations. For this reason, you should be monitoring both EU and national government websites regularly for upcoming legislative changes, as well as reading industry publications and attending conferences relevant to your sector.



Setting KPIs based on the results of your monitoring helps to keep the company on track. It also enables you to put in place whistleblowing reporting channels, trade communication recording procedures and other measures on time and to the required standards.

2.4 Provide evidence of efforts

Tracking KPIs gives you evidence of your efforts to remain compliant with the relevant policies and legislation. In the case of a compliance issue occurring within your organisation, it is likely that a business that can prove it took steps to reduce the risk of wrongdoing will be treated with more leniency. By contrast, an organisation that has no clear compliance strategy and has allowed wrongdoing to flourish will probably be more susceptible to sanctions by competent authorities.

3. What makes a useful KPI?

Hubspot says that useful KPIs depend on *"your goals and your team… historical performance and industry standards"* among other factors. The following are all qualities of useful performance indicators. Although your KPIs might not feature all of these qualities, they will certainly possess one or more.

Quality	Explanation
Simple	When you complicate KPIs, you make it more difficult for employees to understand what they need to do to achieve the preferred outcome. Simple KPIs focus efforts and prompt decisions rather than confuse matters.
Quantitative	Your KPIs must be numerical data that you can track, such as the number of employees attending compliance training sessions or the volume of reports submitted through your whistleblowing channels.
Qualitative	A good KPI measures the effectiveness of an element of your compliance strategy. This could include, for example, the data from employee feedback forms relating to how helpful your compliance training sessions are or how easy it is to report misconduct.
Relevant	The KPI must be matched to the relevant employee or department to enable them to own the process of meeting the required goals.

	Rather than simply utilising generic KPIs for compliance, it's a good practice to make them specific to the role of the people involved. It is also important to understand that different industries and sectors will require a variety of KPIs, depending on the level of regulation applicable.
Directional	The metric should show you whether your business is improving in certain elements of your compliance efforts. Understanding the direction of travel of your processes helps you decide when you need to rethink and adjust your procedures.
Specific	The more specific the KPI, the more likely it is to be achieved. Rather than setting a goal to "improve compliance," think about a concrete goal, such as asking your team to increase the number of internal audits completed on time by 10%. This allows for a more effective response.

4. The most important compliance KPIs to track + examples

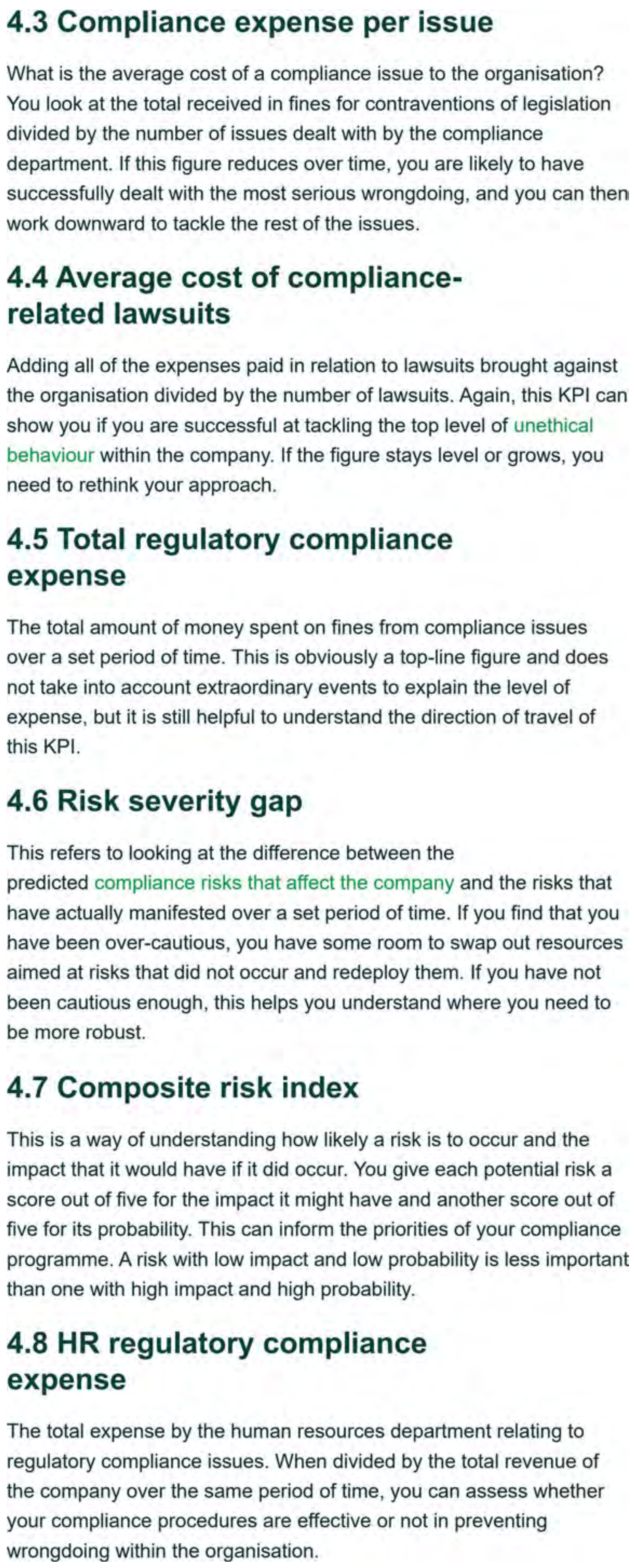
Here are some of the most important compliance key performance indicators that you should track to ensure your compliance policies are pushing the company in the right direction.

4.1 Mean time to issue discovery

The time it takes to discover a compliance issue is obviously critical for investigating and resolving problems within a reasonable timeframe. By calculating this number, you can understand whether the company is improving at uncovering violations or if they are being allowed to fester for longer. The shorter the mean time to issue discovery, the more effective your compliance efforts will be.

4.2 Mean time to issue resolution

This KPI can be analysed on its own and in relation to the mean time to issue discovery. You want to see that you are resolving issues more quickly, and that is the headline figure. However, if you are getting quicker at discovery but resolution is stagnant or even taking longer, you have a better idea of where the blocks are in the pipeline.



4.3 Compliance expense per issue

What is the average cost of a compliance issue to the organisation? You look at the total received in fines for contraventions of legislation divided by the number of issues dealt with by the compliance department. If this figure reduces over time, you are likely to have successfully dealt with the most serious wrongdoing, and you can then work downward to tackle the rest of the issues.

4.4 Average cost of compliance-related lawsuits

Adding all of the expenses paid in relation to lawsuits brought against the organisation divided by the number of lawsuits. Again, this KPI can show you if you are successful at tackling the top level of unethical behaviour within the company. If the figure stays level or grows, you need to rethink your approach.

4.5 Total regulatory compliance expense

The total amount of money spent on fines from compliance issues over a set period of time. This is obviously a top-line figure and does not take into account extraordinary events to explain the level of expense, but it is still helpful to understand the direction of travel of this KPI.

4.6 Risk severity gap

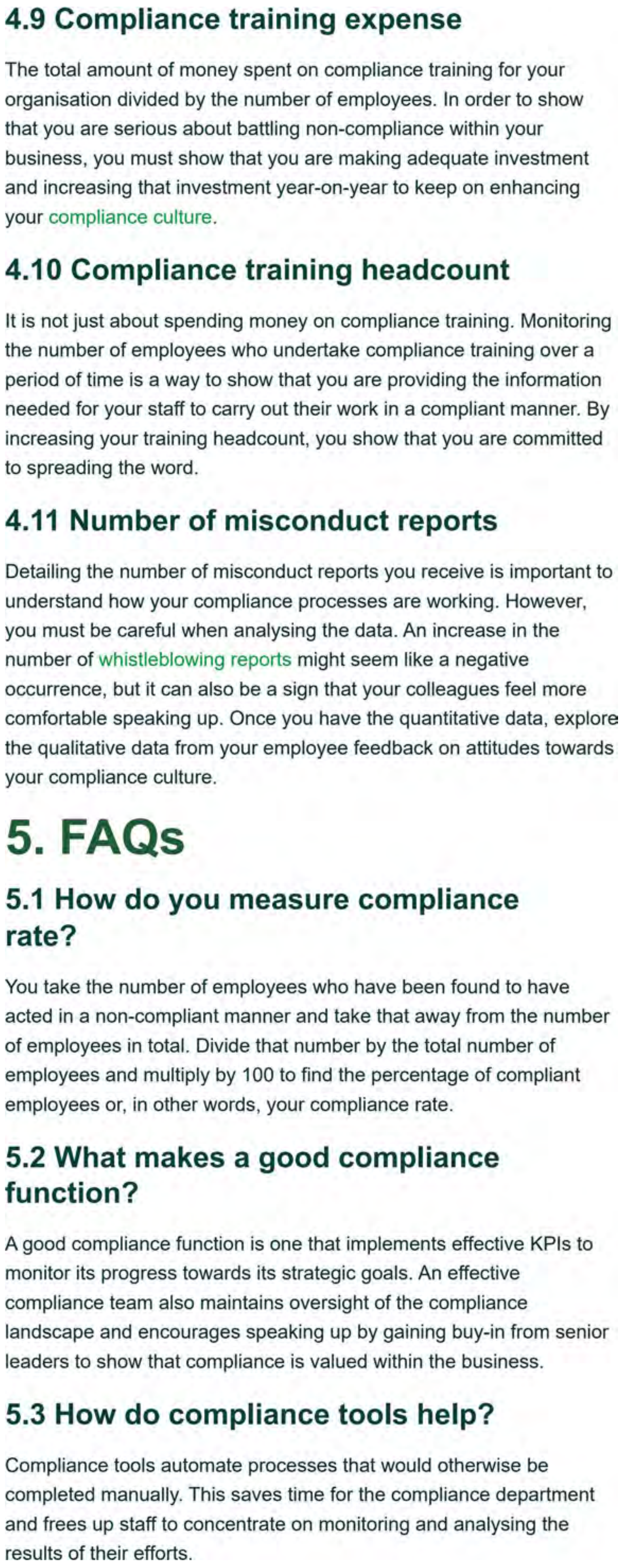
This refers to looking at the difference between the predicted compliance risks that affect the company and the risks that have actually manifested over a set period of time. If you find that you have been over-cautious, you have some room to swap out resources aimed at risks that did not occur and redeploy them. If you have not been cautious enough, this helps you understand where you need to be more robust.

4.7 Composite risk index

This is a way of understanding how likely a risk is to occur and the impact that it would have if it did occur. You give each potential risk a score out of five for the impact it might have and another score out of five for its probability. This can inform the priorities of your compliance programme. A risk with low impact and low probability is less important than one with high impact and high probability.

4.8 HR regulatory compliance expense

The total expense by the human resources department relating to regulatory compliance issues. When divided by the total revenue of the company over the same period of time, you can assess whether your compliance procedures are effective or not in preventing wrongdoing within the organisation.



4.9 Compliance training expense

The total amount of money spent on compliance training for your organisation divided by the number of employees. In order to show that you are serious about battling non-compliance within your business, you must show that you are making adequate investment and increasing that investment year-on-year to keep on enhancing your compliance culture.

4.10 Compliance training headcount

It is not just about spending money on compliance training. Monitoring the number of employees who undertake compliance training over a period of time is a way to show that you are providing the information needed for your staff to carry out their work in a compliant manner. By increasing your training headcount, you show that you are committed to spreading the word.

4.11 Number of misconduct reports

Detailing the number of misconduct reports you receive is important to understand how your compliance processes are working. However, you must be careful when analysing the data. An increase in the number of whistleblowing reports might seem like a negative occurrence, but it can also be a sign that your colleagues feel more comfortable speaking up. Once you have the quantitative data, explore the qualitative data from your employee feedback on attitudes towards your compliance culture.

5. FAQs

5.1 How do you measure compliance rate?

You take the number of employees who have been found to have acted in a non-compliant manner and take that away from the number of employees in total. Divide that number by the total number of employees and multiply by 100 to find the percentage of compliant employees or, in other words, your compliance rate.

5.2 What makes a good compliance function?

A good compliance function is one that implements effective KPIs to monitor its progress towards its strategic goals. An effective compliance team also maintains oversight of the compliance landscape and encourages speaking up by gaining buy-in from senior leaders to show that compliance is valued within the business.

5.3 How do compliance tools help?

Compliance tools automate processes that would otherwise be completed manually. This saves time for the compliance department and frees up staff to concentrate on monitoring and analysing the results of their efforts.

6. Conclusion

These compliance KPI examples show the kinds of indicators that you should track to ensure that your compliance strategy is working in an effective manner. The consequences of failing to instil a compliance culture, such as financial loss, reputational damage and reduced staff morale, can be impactful on a business. So, making sure you are continually improving your efforts to eliminate wrongdoing is in the best interests of the business.

ComplyLog offers a suite of tools to help you stay compliant with key pieces of legislation and streamline your processes:

- IntegrityLog enables you to fulfil the requirements of the EU Whistleblowing Directive.
- InsiderLog helps you automate your insider list management as per MAR.
- TradeLog makes managing employee personal trading easier and faster.

You can request a free demo of each of these tools by clicking on the links above.

7. References and further reading

- Company code of conduct examples
- Benefits of a code of ethics
- How to create a compliance communication strategy
- How to measure the effectiveness of whistleblowing
- How to write a conflict of interest policy + template

Share this post