CENLAR FSB
CENTRAL LOAN ADMINISTRATION & REPORTING

CLIENT MEETING

April 28, 2022

Meeting Agenda

- Welcome and Introduction: Dave Miller, EVP
- Business Controls : Lynn Tarantino, SVP, Chief Control Officer
- Operational Risk Management: Kurt Kremstein, VP, Chief Operational Risk Officer
- Compliance: Jennifer Rowen, SVP, Chief Compliance Officer
- Audit: Wayne Tull, SVP, Chief Audit Executive
- Conclusion: Dave Miller, EVP

Internal Controls and Risk Management

Cenlar's Three Lines of Defense
Primary Responsibilities

STRUCTURE

- Board approval of ERM policies and risk appetite statements
- Sets guidance/ requirements for risk appetite & tolerance levels
- Enforces program and risk ownership accountability
- Weekly and monthly reoccurring reporting & meetings

1 Operations

Functional Owners:
Business Process Owners and Control Office Team

- Process, Risk and Control owners
- Manage, mitigate, report risk
- Day-to-day management of client and third-party relationships
- Control Office (Issue Management, Business Control Office and Operational Change Management)

2 Governance

Functional Owner:
Enterprise Risk Management
Independent oversight and reporting function

- Policy and program design based on industry best practices and regulation (policy and program owner)
- Portfolio risk management
- Risk management subject matter experts
- Key Functions: Compliance, Legal, RCSA, Issues Management, Third-Party Risk, IT Risk, Quality Assurance, Quality Control, Client Audit Support, P&Ps

3 Independent Oversight

Functional Owner:
Internal Audit

- Independent audit & review function
- Risk, controls & monitoring consultant resource
- Issue Validation

1 Control Office Team – Business Controls

Line 1

- Business Control Team made up of Business Control Directors, Managers and Analysts who partner and collaborate with assigned business units, but report independently to the Chief Control Officer
- The Business Control Team works with the business leaders to manage, mitigate and report risks on a daily basis.
- The team plays an active role
  - » Facilitation of ongoing risk control self assessments and,
  - » Control testing to help the business unit understand their current risk and control profile further ensuring they remain in compliance with
    - » Cenlar's risk appetite, stated business objectives, and applicable regulations and contractual obligations

RCSA
Key Process Mapping, Identification of Control Points and Gaps
Evaluate of Regulatory Requirements
Evaluate of Risks
Evaluate Control Descriptions
Assess Inherent Risk
Evaluate Control Effectiveness (Design and Operational Effectiveness Testing)
Identify Control Improvement Opportunities (GAPS, Ineffective Controls)
Manage change

1 Control Office Team – Issues Management

Issue Management - Identification and Intake, Root Cause Analysis and Evaluation, Short Term/Long Term Corrective Action, Customer Remediation, Compensating Controls, Execution, Testing, Validation, Sustainability

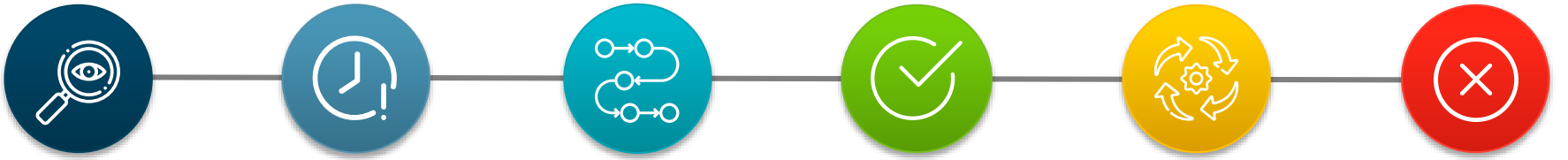
Issue Owner – Business Unit

- Ultimately accountable for timely, effective and end-to-end resolution of all issues.

Issue Manager

- Serves as Issue Owner delegate and drives day to day oversight over the issue, ensuring progress. Provides strategic direction for the improvements or remediation;
- Appraises stakeholders of all identified risks or concerns during the entire issue lifecycle and initiates escalations;
- Applies a project management discipline across the Issues Management lifecycle to coordinate across MAP owners and all relevant stakeholders, including IA as applicable;
- Ensures that they is a clear and tracked plan to progress through all MAP activities;
- Responsible for ensuring all artifacts are defined, tracked, delivered, and packaged.

1 Issue Remediation Process



Pending Root Cause

- Issue Reported
- RCA In Process
- Severity Rating Pending
- CA Activities

Pending Remediation

- RCA Complete
- Severity Rated
- CA Activities
- MAP Planning

Remediation in Process

- CA Activities
- Remediation Activities
- MAP In Process

Validation

- MAP Complete
- Validation Activities

Sustainability

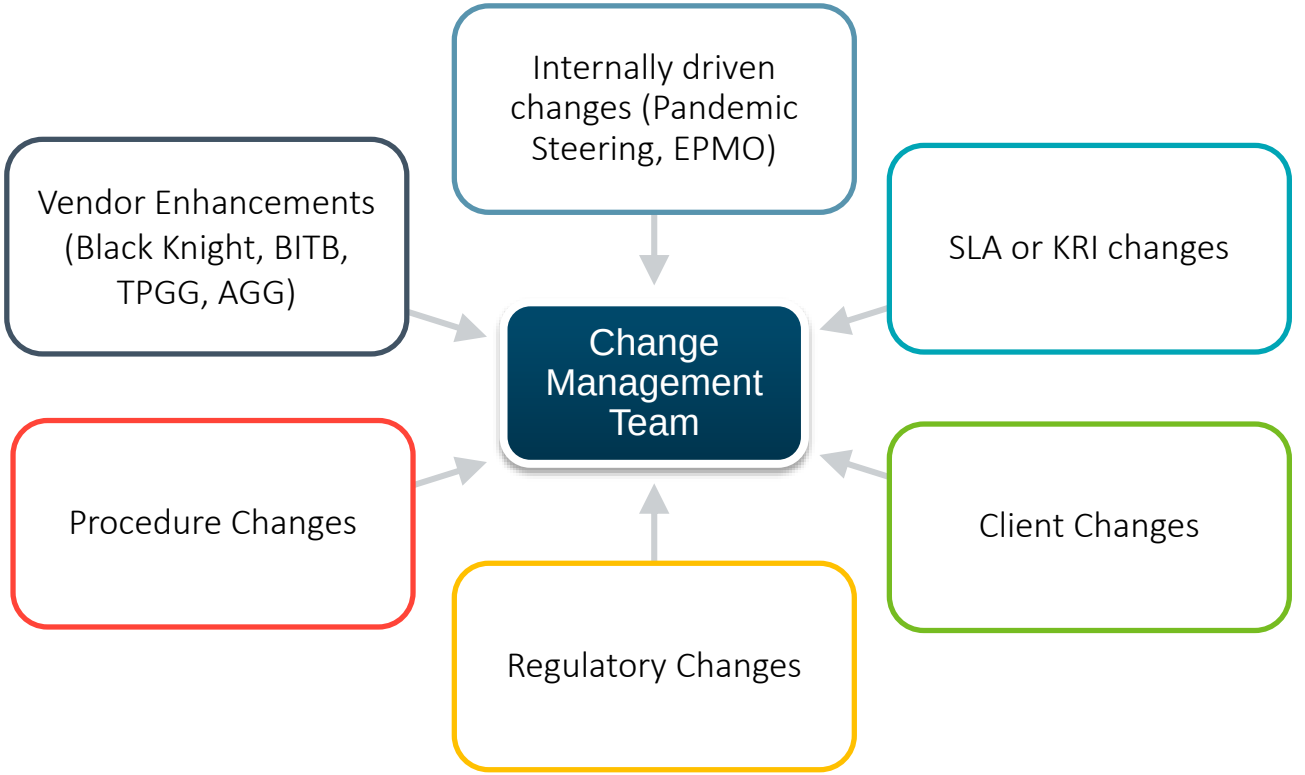
- Monitoring/ Testing
- 90 Days

Closed

- Reported
- Post-Mortem

RCA	Root Cause Analysis
CA	Corrective Action
MAP	Management Action Plan

1 Operational Change Management



2 Enterprise Risk Management (ERM)

The ERM Organization is comprised of 3 core functions:

2 Compliance

Compliance

The Compliance Team is charged with implementing processes to ensure that the company is complying with all applicable laws, rules and regulations, as well as internal codes of conduct, policies and procedures.

Key Functions

- Compliance Testing/Risk Assessment
- KRI Validation
- Compliance Advisory:
  - » Regulatory Change Management
  - » Policy Mgmt. & Training
- Financial Crimes
  - » BSA/AML/OFAC
  - » Fraud
- Fair Lending/Fair Servicing
- Examination Management

2 Compliance Testing

Testing Schedule

Driven by risks derived from audits, regulatory examinations, change management or changes in the risk ranking at the state and federal level.

Testing Methodology

- Ongoing monitoring of the Compliance Management System.
- Focusing on the effectiveness of:
  - » Adherence to regulatory change
  - » Effectiveness of preventative and detective testing

Reporting

- Formal report produced at the conclusion of each review period.
- Identified issues entered into the GRC.
- Update on the status of testing provided into the Management Operating Reviews.

2 Compliance Advisory

Issues Management

- Review issues to ascertain and validate compliance impact rating
- Review and approve MAPs for compliance related issues
- Periodically review emerging issues with BCDs and BCMs
- Provide guidance on compliance related matters and process changes related to issues

Advisory Function

- Procedure Review
- Customer Communication Review and Approval (Letters/Scripting/Email)
- Compliance Advisory Mailbox (Internal Support for Compliance Related Questions)
- Enterprise Wide Project Compliance Support
- Third-Party Risk Management Compliance Support

Regulatory Change Management

- Weekly Working Group Meetings
- At risk items tracked and escalated to the Chief Compliance Officer and the Board Risk Committee
- Seven Step Process
  1. Identification
  2. Impact Assessment
  3. Management Action Plan Approval
  4. Implementation
  5. Implementation Validation
  6. Post-Implementation Testing
  7. Closure
- Communication with Clients
  - » Category (Federal, State, GSE, Other), Change ID, Rule Signing Date, Rule Effective Date, High Level Summary of the Rule, Current Stage, Current Status, Projected Implementation Date, Servicing Function Impact

2 Financial Crimes

Specialist Team

- Watchlist Scanning
  - OFAC, SDN
  - 314(a)

Analyst Team

- 314(b) Requests
- Incident Referrals from Business Units
- Transaction Monitoring
  - Fraud Investigations
  - AML Investigations
- Suspicious Activity Reporting

Management Team

- CIP Program Management
- Enterprise Wide Training
- Client Due Diligence Program Management
- Management and Board Risk Reporting
- Wolters Kluwer Case Management System Oversight

2 Compliance Oversight

Examinations

- Team dedicated to management of the Office of the Comptroller of the Currency Examinations and Ongoing Supervision
- Manage all rating agency and agency (Fannie, Freddie, HUD, USDA, VA) onsite reviews/examinations

Key Risk Indicators (KRIs)

- Team dedicated to the governance, oversight and change management for KRIs

2 Operational Risk, Governance and Reporting

Operational Risk, Governance & Reporting

The Operational Risk, Governance and Reporting is charged with ensuring there is an appropriate Enterprise Risk Management framework to identify, analyze, assess, mitigate, monitor, report on, and govern the management of residual risk the environment

Key Functions / Mission

- Quality Testing – Independent detective testing function covering all applicable requirements
- Client Audit Support - Manage all client audits, including their state, regulatory, internal, and third-party audit requests
- ERM Data, Analytics and Reporting – Maintain GRC system and provide meaningful and actionable data from its programs implementing the ERM Policy
- ERM Governance – Develop, train and guide Cenlar for execution of ERM Policy/framework.
- Third Party Risk Management – Oversee Cenlar's Vendor Owners for appropriate management of its third party relationships.
- Model Risk Management – Own oversight and independent validation to ensure Cenlar effectively manages the risk of using models.

2 Quality Testing Process Flow

Execute test scripts & identify exceptions

- Develop test plans, including changes communicated for new, revised, or retired requirements
- Execute testing by Business Function and Requirement and analyze results

Communicate & Obtain Agreement

- Communicate and obtain Business Unit Mgmt. agreement for findings

Provide Reporting

- Provide reporting by Business Function and Requirement to Management and Executive Leadership

Submit Issue

- BCMs and Business Unit Mgmt. partner to determine root cause, develop Management Action Plan (MAP) and remediate issue

2 Third-Party Life Cycle

Planning

- Materiality Risk Assessment
- Identify nature and degree of inherent risks of proposed engagement
- Determine standards and controls required for engagement
- Obtain approval to engage/outsource

Due Diligence & Selection

- Execute NDA
- Perform Request for Proposal
- Review vendor due diligence
- Law Firm Certification
- Site Visit (if applicable)
- BCP/DRP and Exit Strategy Considerations
- Obtain necessary approvals

Contracting

- Perform contract risk and compliance structuring
- SLA, performance metrics & reporting
- Contract execution

Ongoing Monitoring

- SLAs, scorecard and performance monitoring
- BitSight Monitoring of critical relationships
- Third Party Risk Group
- Issues Management Remediation
- Recertification of due diligence & risk assessments
- Escalation of material issues or concerns

Termination

- Attorney Governance Group Review (if applicable)
- Contract considerations
- Transition, resumption or discontinuation readiness considerations
- Stakeholder impacts
- Return/retention/ destruction of data, intellectual property or other assets
- If applicable, start with planning again

2 Operational Vendor Due Diligence Requirements

	Due Diligence	Operational & Material Tier 0/ 1	Operational & Material Tier 2	Operational & Material Tier 3	Non- Material Tier 4	Consultant
	Cost Benefit Analysis	✓	✓	×	×	×
	Completed Materiality/Risk Assessment	✓	✓	✓	✓	✓
	Non Disclosure Agreement	✓	✓	✓	*If sharing Confidential Info	✓
	OFAC Scan/Proof & HR TIN Check	✓	✓	✓	✓	✓
	Copy of W-9 & ACH form	✓	✓	✓	✓	✓
	Contract Draft for Legal Review	✓	✓	✓	*Dependent on Service	✓
	Background Clause in Contract or Executed Attestation on File	Included Ops vendors contracts	Included Ops vendors contracts	Included Ops vendors contracts	*If Confidential Info is Shared	*If access to Restricted Data, Systems or Cenlar Facilities
Vendor-provided Documents	Due Diligence Questionnaire	✓	✓	✓	×	PStreamlined Questionnaire
	Three (3) years Audited Financial Statements	✓	✓	×	×	Dependent on Tier
	FFIEC Reports (from OCC if available)	Requested Annually	Requested Annually	×	×	×
	SSAE18 or Equivalent 3rd party Controls Rpt	✓	✓	×	×	×
	Third Party Information Security Reports*	*If access to NPI or Restricted Data or a Software	*If access to NPI or Restricted Data or a Software	*If access to NPI or Restricted Data or a Software	×	×
	Certificate of Insurance*	✓	✓	*If access to Restricted Data or Cenlar Facilities	*If access to Restricted Data or Cenlar Facilities	*If access to Restricted Data or Cenlar Facilities
	Disaster Recovery Plan Overview /Test Results*	✓	✓	*If Difficult to Replace in RA	×	×
	Vendor Management Policies & Procedures*	*If they use third parties for svcs	*If they use third parties for svcs	*If they use third parties for svcs	×	*If they use third parties
	Customer Interaction Policies & Procedures*	*If they have Borrower contact	*If they have Borrower contact	*If they have Borrower contact	×	×
	Compliance Policies*	*If there are applicable Laws /Regs	*If there are applicable Laws /Regs	*If there are applicable Laws /Regs	×	×
	Purchased Software /Tech Services Policy (SPP) **For Onboarding DD Assessment* ***Subsequent DD Assessments*	*If providing Software; **if Substantial change/ upgrade in Technology	*If providing Software; **if Substantial change/ upgrade in Technology	*If providing Software; **if Substantial change/ upgrade in Technology	*If providing Software; **if Substantial change/ upgrade in Technology	*If providing Software; **if Substantial change/ upgrade in Technology
	Exit Strategy	✓	*If Difficult to Replace in RA	*If Difficult to Replace in RA	×	×
	Site Visit	Determined by TPRM & TPSA	Optional	Optional	×	×
	Review Frequency	12 Months	12-18 Months	36 Months	×	Dependent on Tier

2 Information Technology Risk Management

Information Technology Risk

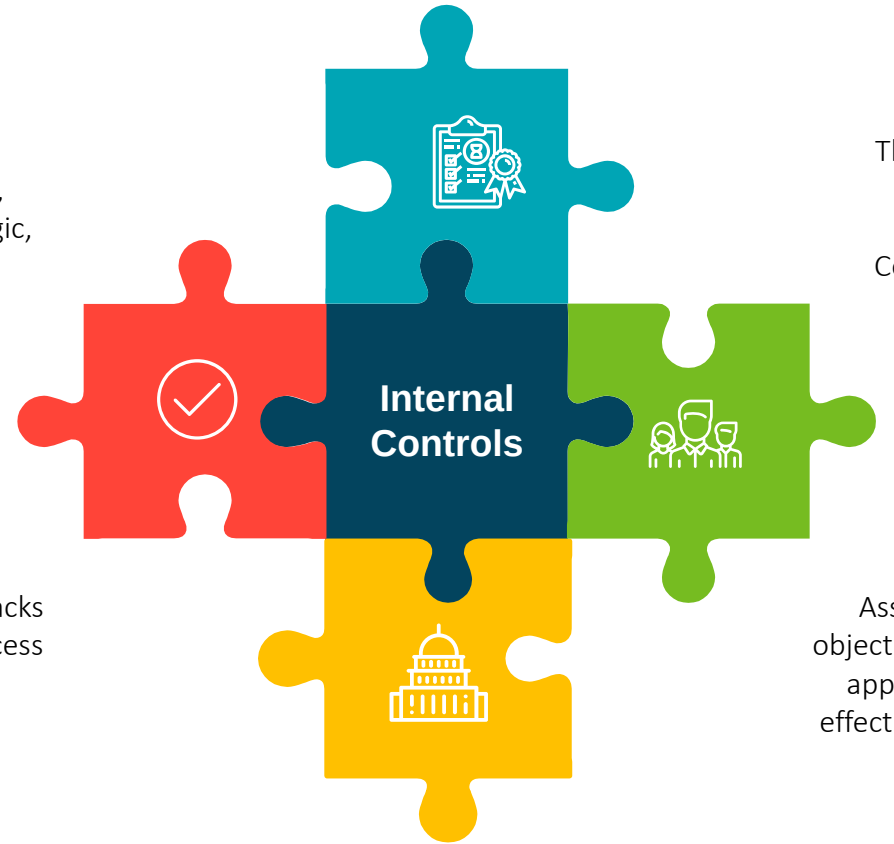
The Information Technology Risk Management Team is responsible for maintaining oversight for all areas of technology including:

- IT Governance
- Disaster Recovery
- IT Change Management
- Software Development Life Cycle (SDLC)
- Portfolio and Project Management
- Database Management
- IT Security
- Asset and Configuration Management
- IT Operations
- IT Service Delivery

3 Internal Audit

Assurance

Looks beyond financial risks and considers regulatory, operational, market, credit, reputational, strategic, technological, and fraud risks



Independent

The Internal Audit Team reports to the Chief Audit Executive who Reports to the Board Audit Committee and administratively to the Chief Executive Officer

Validation

Advocates for improvements and tracks issues through the remediation process to ensure proper closure

Governance

Assists Cenlar with accomplishing its objectives by using a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes

3 Internal Audit Cycle

3 The Annual Risk Assessment and Audit Plan

The Internal Audit Department uses the results of the Annual Risk Assessment to identify the auditable entities with the greatest risk. The following is performed during the annual risk assessment:

- Identifying auditable entities within the audit universe to complete the Risk Assessment
- Discussions with business managers for anticipated processing, technology, management/staffing, or regulatory changes impacting risk
- Identifying sub-entities, compliance regulations, vendors, and systems that are related to each auditable entity
- Assigning inherent risk for each auditable entity
- Using COSO framework - assess each risk factor
- Determine a risk rating for each risk category and an overall rating for each entity

Risk Level	Audit Frequency
High	Every 12 - 18 months
Moderate	Every 24 - 30 months
Low	Every 36 - 42 months

The overall risk rating for the auditable entity determines the audit frequency.

3 The Audit Process

All audits follow a similar sequence of activities and may be divided into four phases:

- **Planning:** Gain an understanding of business activities, risks, and control structure to establish scope of audit and build testing program. Deliverables include walkthrough documentation, flowcharts, and the Risk & Control Matrix.
- **Fieldwork:** Execution of testing program. Deliverables include workpaper documentation, exception confirmation, and root cause analysis.
- **Reporting:** Communicating audit results to management. Deliverables include Audit Report and Management Memo
- **Post Closing Activities:** Issue tracking, remediation, validation, and closure. This phase also includes the Quality Assurance Improvement Program review.

3 Assurance and Validation

Issues and control gaps identified through all sources, along with the associated corrective action plans and due dates, are captured in the GRC Issue Management application (Process Unity). The GRC tool provides an automated workflow which produces status reports for management and the Board of Directors.

- All Functional Managers with issues are able to review their issues at anytime through the GRC.
- Weekly the Executive & Management team discuss open issues.
- Open issue status and trends are discussed at every Board Risk and Board Audit Committee meetings
- All action plans completed by the business units which are associated with issues rated moderate or higher are independently validated for design and operating effectiveness by Internal Audit

THANK YOU

for your time!

CENLAR®
CENTRAL LOAN ADMINISTRATION & REPORTING

www.cenlar.com
780 TOWNSHIP LINE ROAD | YARDLEY, PA 19067