SIMPLIFYING BANK RISK MANAGEMENT

ENTERPRISE RISK MANAGEMENT DOESN'T HAVE TO BE COMPLICATED OR EXPENSIVE

PREPARED BY:

OLIVIA LINDSAY, EVP – CHIEF RISK OFFICER, BANC OF CALIFORNIA

&

DAN RODERICK, CEO, STRUNK

DATE: OCTOBER 9, 2025

OPENING CONTEXT

Why banks overcomplicate ERM:

- Fear of regulators

- Complex frameworks borrowed from large institutions

- Overreliance on consultants/software

Reality: Most banks need clarity, not complexity

WHAT ERM REALLY IS

Simple definition: Identifying, assessing, managing, and monitoring risks across the institution

ERM is a framework, not a bureaucracy

Core bank risks: credit, liquidity, operational, compliance, reputation

MYTH VS. REALITY

- Myth: ERM requires massive investment
- Reality: Effective ERM relies on culture, communication, and accountability
- Examples of low-cost risk practices that work

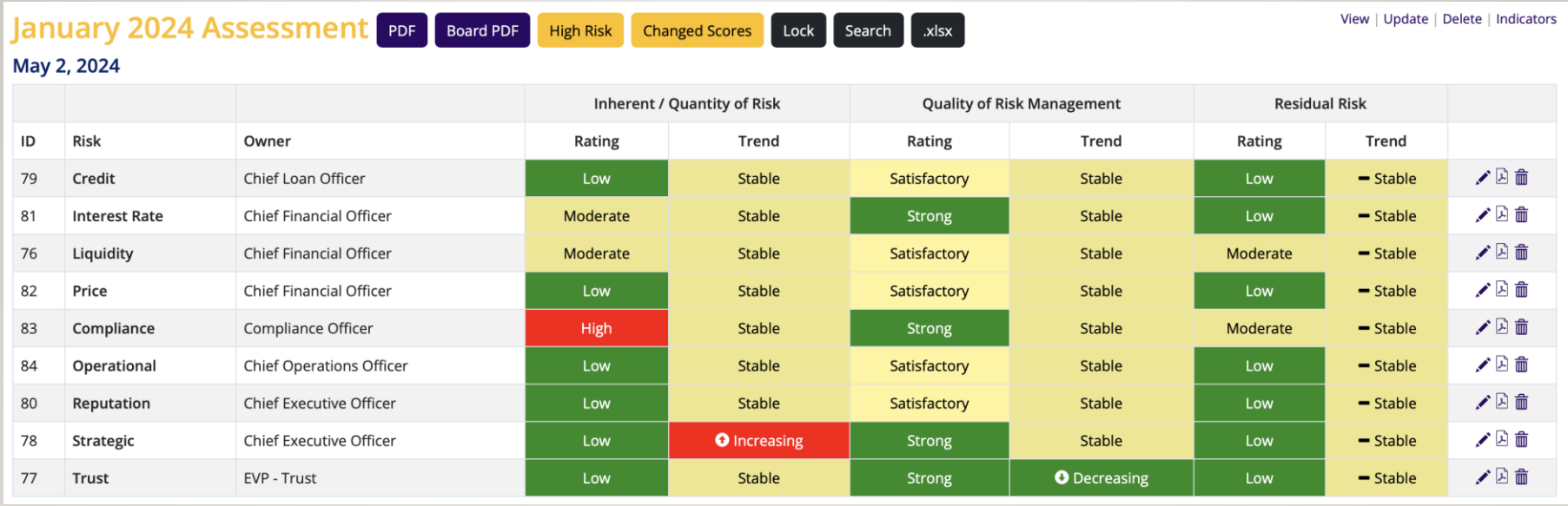
THE 5 PILLARS OF SIMPLE ERM

- 1. Governance & Tone at the Top – Leadership support
- 2. Risk Identification – Use existing committee discussions
- 3. Risk Assessment & Prioritization – Simple heat map/scoring
- 4. Controls & Mitigation – Leverage existing policies/procedures
- 5. Monitoring & Reporting – Dashboards, not 200-page reports

TOOLS THAT DON'T COST MUCH

- Excel-based risk register
- Simple heat maps
- Quarterly risk review meetings
- Plain-language risk appetite statements

SAMPLE RISK HEAT MAP



January 2024 Assessment

PDF | Board PDF | High Risk | Changed Scores | Lock | Search | .xlsx

View | Update | Delete | Indicators

May 2, 2024

			Inherent / Quantity of Risk		Quality of Risk Management		Residual Risk		
ID	Risk	Owner	Rating	Trend	Rating	Trend	Rating	Trend	
79	Credit	Chief Loan Officer	Low	Stable	Satisfactory	Stable	Low	– Stable	
81	Interest Rate	Chief Financial Officer	Moderate	Stable	Strong	Stable	Low	– Stable	
76	Liquidity	Chief Financial Officer	Moderate	Stable	Satisfactory	Stable	Moderate	– Stable	
82	Price	Chief Financial Officer	Low	Stable	Satisfactory	Stable	Low	– Stable	
83	Compliance	Compliance Officer	High	Stable	Strong	Stable	Moderate	– Stable	
84	Operational	Chief Operations Officer	Low	Stable	Satisfactory	Stable	Low	– Stable	
80	Reputation	Chief Executive Officer	Low	Stable	Satisfactory	Stable	Low	– Stable	
78	Strategic	Chief Executive Officer	Low	↑ Increasing	Strong	Stable	Low	– Stable	
77	Trust	EVP - Trust	Low	Stable	Strong	↓ Decreasing	Low	– Stable	

SAMPLE RISK DASHBOARD

Top 5 Risks Overview
- Credit Risk: High
- Liquidity Risk: Medium
- Operational Risk: Medium
- Compliance Risk: High
- Reputation Risk: Medium

Key Metrics
- Loan Delinquencies ↑
- Liquidity Ratios Stable
- Audit Findings ↓
- Compliance Issues ↑
- Customer Complaints Stable

INTEGRATING WITH DAILY OPERATIONS

- ERM shouldn't be a side project
- Embed into:
- - New product approvals
- - Vendor management
- - Compliance testing
- - Strategic planning

CASE STUDY EXAMPLE

- Mid-sized bank ERM implementation:
- - One risk committee
- - Quarterly reporting
- - Simple dashboards
- Results: better exam results, lower costs, improved awareness

ESTABLISHING A RISK CONTROL SELF ASSESSMENT (RCSA) PROGRAM – A BOTTOMS UP APPROACH

PEOPLE

- Establish a Strong Tone at the Top - Board and CEO
- Create Shared Ownership Amongst the Executive Team – We Win Together (or We Lose Together)
- Empower a dedicated and experienced risk leader with process design experience
- Identify Business Unit Champions – We Win Together (or We Lose Together)
- Share plans and progress with your Regulators

PROCESS

- Develop a project plan with timebound commitments
- Create comprehensive Governance Documents (Standards, Methodology, Procedures, Training Material)
- Identify the "in-scope" universe of business units
- Create a risk-based schedule with quarterly progress checks to promote accountability
- Start with a Pilot Group of "friendlies"
- Calendar meetings and working sessions to drive deliverables forward
- Focus on understanding and documenting key business processes and controls
- Map controls back to Risk Statements
- Test control designs with worst case scenarios to facilitate credible challenge discussions

SYSTEMS

- Standardize Key Program Elements
- Risk Impact Statements and Linkage to Risk Pillars
- Rating Definitions: (Inherent Risk; Control Maturity; Control Operating Effectiveness; Residual Risk; Control Design Descriptions)
- Collect Evidence/Test Effectiveness
- RCSA Summary Results
- Memorialize Credible Challenge
- Report & Monitor
  - Schedule Progress
  - Self Identified Findings
  - Aggregated RCSA Results
  - Thematic Opportunities

COMMON PITFALLS TO AVOID

- Overengineering the framework
- Focusing only on regulatory compliance
- Creating 'binder ERM' with no practical use

REGULATOR EXPECTATIONS

- Regulators want:
  - Demonstrated oversight
  - Clear documentation
  - Evidence of board involvement
  - They don’t require expensive software

QUICK WINS

- Create a risk register in Excel
- Assign owners for top risks
- Do a quarterly risk dashboard for the board
- Use existing audits/exams as inputs

CONCLUSION

- ERM is about discipline, not dollars
- Keep it simple, practical, and effective
- Questions & Discussion