summit consulting

[XXX]
ERM AUDIT REPORT

ENGAGEMENT OBJECTIVES

Company X engaged Internal Auditor X to perform an internal audit of its ERM function. A baseline review, assessing the function's elements in relation to (Insert Standards) was conducted in the following phases:

Information gathering and project planning.

Understanding ERM's current state with regard to the following components:

- Design and Governance
  - Policies and procedures
  - Charter
  - Methodology (including definitions of risk and control, qualitative and quantitative differentiation, etc.)
- Infrastructure
  - Business processes
  - Ownership and accountability
  - Training
  - Organizational structure and coverage
  - Others
- Information Management
  - System and data
  - Information gathering
  - Information consolidation
  - Analytics
  - Information reporting
- Future Planning
  - Management's vision for further development of the ERM function

Evaluation of the ERM program in relation to (Insert Standards).

Gap analysis and summarization of findings & recommendations.

summit

SUMMARY OF KEY OBSERVATIONS (1/3)

Company X management has made significant progress with the establishment of its ERM program, especially given Company X's scale and short timeframe since inception. The program's components are in general conformance with the (Insert Standards). The below observations are not intended to mean that a correction of deficiencies is needed, but rather reflect opportunities for improvement in comparison to leading ERM practices in the financial services industry, many of which have a longer ERM history than Company X, and that management may want to consider whether such practices would be an appropriate fit for Company X:

1	**Considerable progress with development and implementation of the ERM program has been made since the program's inception in (Insert Date).**

- Various sound ERM practices and structural components have been put in place, and a satisfactory governance model has been established during the program's first stage of development.
- Recognized ERM concepts, methods and standards, namely those outlined by (Insert Guidance), have been implemented, and these serve as the program's philosophical and functional building blocks.
- Organizational strengths such as business culture, talent base and performance have not been compromised through the introduction and implementation of the ERM approach.
- Employees across the organization show a willingness and ability to contribute to ERM's current and future development.

SUMMARY OF KEY OBSERVATIONS (2/3)

2	**The Operational Risk Management component of the ERM program is in its infancy, but evolving rapidly. The next stage of development should include:**

- Establishment of an operations risk framework to facilitate a stronger link between identification, evaluation, response, monitoring and reporting activities.
- Consideration of an operations risk technology platform to coincide with the framework, to process operations risk information, and to efficiently facilitate ongoing identification, analysis and reporting.
- An expansion of the definition of “operations risk” to include impact on indirect economic value, such as credibility/brand and opportunity cost to ensure that other types of organizational risks are not overlooked.

3	**Executive management’s expectations of the ERM function, beyond the expectation of compliance with regulatory mandate, are not fully defined.**

- ERM is a conceptual approach based on the integration of value creation and value preservation activities relative to risk and its dynamics.
- Company X has invested significant resources into development of an ERM program, and we have found successful implementations to clearly outline the benefits these resources are expected to bring.
- Expectation for and communication of ERM’s value proposition to stakeholders is important to shaping an organization’s long-term risk culture and approach to its endeavors.
- We acknowledge that Company X’s history of minimal financial loss from market, operations and credit risk management makes it more challenging to find immediate economic value from an ERM program.

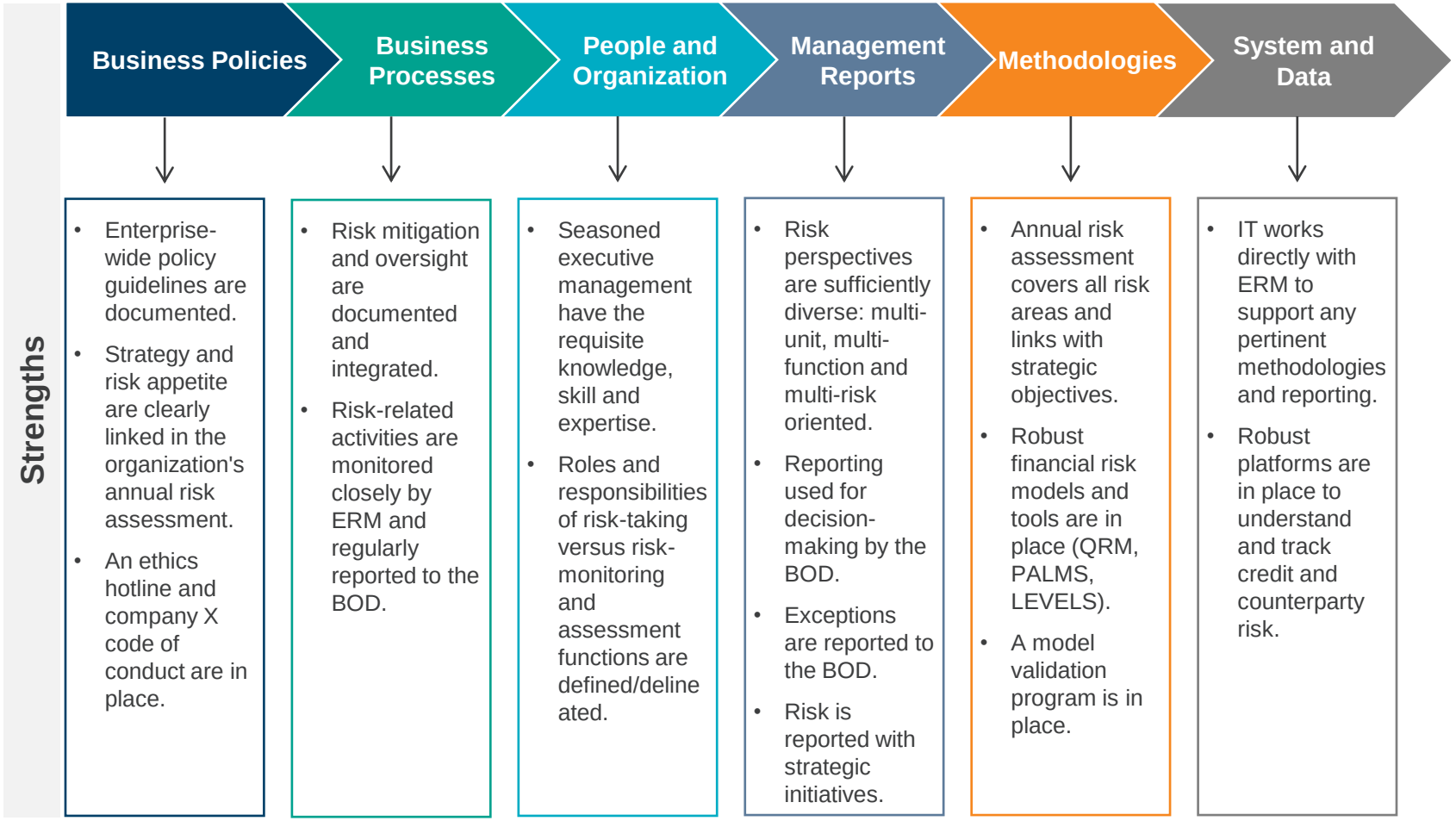
SUMMARY OF KEY OBSERVATIONS (3/3)

4	**The organizational structure is in compliance with Company X's stated objectives. Looking forward and considering future program development, there will be the opportunity to reflect on leading ERM practices of the financial services industry and consider the costs and benefits associated with such. Should management desire to incorporate such, then a cost-benefit consideration could be given to the opportunities like the following:**

- Integration with other risk-related responsibilities of the organization (e.g., Sarbanes-Oxley). One practice is to seek out greater efficiency and effectiveness by further integrating the collection, analysis and reporting of risk management-related information, if appropriate resources are available to the ERM function.
- Establishment of a relative value system for comparison of risk and relative benefit from risk management activities (e.g., an economic capital mechanism). The objective here would be to establish a uniform system for active comparison of all business risks undertaken to benefits (or costs) for the organization.
- Establishment of an IT platform for operations risk management could bring about greater efficiency and effectiveness with operations risk management by integrating a framework with policy, relevant business information and managerial controls.

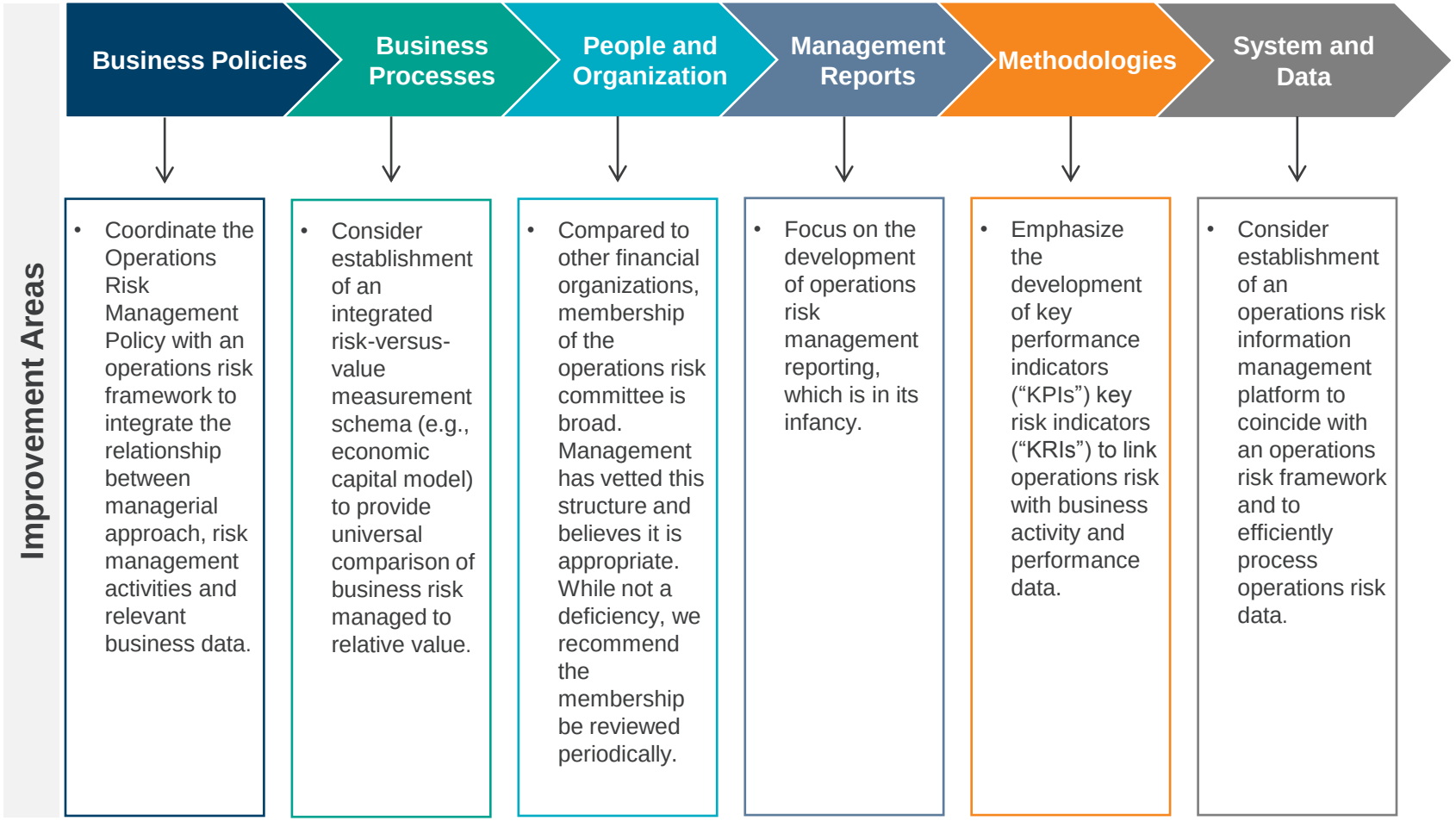
DETAILED OBSERVATIONS AND RECOMMENDATIONS: ERM INFRASTRUCTURE (1/2)

The following is a progress summary regarding development of the infrastructure needed to support the ERM program using SCL's Six Elements of Risk Framework:



DETAILED OBSERVATIONS AND RECOMMENDATIONS: ERM INFRASTRUCTURE (2/2)

The following is a progress summary regarding development of the infrastructure needed to support the ERM program using SCL's Six Elements of Risk Framework:



DETAILED OBSERVATIONS AND RECOMMENDATIONS: ERM PROGRAM

Based on the scope of work performed, we observed the following specific enhancement opportunities and compared those with both standards and leading practices in the financial services industry:

Observations	Component	Recommendations	Framework	Leading Practice
ERM Value Proposition	Internal Environment	Enterprise risk management is an integrated methodology built upon value creation and value preservation emphases. Long-term program success could be enhanced through clear expectation and communication of ERM's future value proposition.	√	√
Risk Definition	Risk Assessment	The definition of "risk" could include the addition of intangible value, such as credibility/brand equity and opportunity cost, in addition to financial loss. Realized risk often has economic consequences which are not always recognized through accounting frameworks. Best practice is to look at risk in terms of economic impact and structure value preservation and creation activities around economic value.	√	√
Long-Term Integration of Related ERM Activities	Internal Environment	As ERM programs mature, consideration should be given towards integration of other risk activities, such as financial reporting risk activities (Sarbanes-Oxley). Full integration of these risk related-activities may strengthen the enterprise risk portrait management maintains and make inter-relationships between risk types and management activities more evident.	√	√
Integrated Measurement Schema	Internal Environment	Establishment of a relative value system for comparison of risk and relative benefit from risk management activities would better allow for clear integration and relative comparison or risk and risk management activities. One example of such a schema is an economic capital model (e.g., RAROC or risk-adjusted return on capital).	√	√

Note: Check color indicates status of recommendation: Red = Expectation Not Met, Orange = Needs Improvement, Blue = Meets Expectations.

summit consulting

DETAILED OBSERVATIONS AND RECOMMENDATIONS: OPERATIONS RISK (1/3)

Observations	Component	Recommendations	Framework	Leading Practice
Establish an Operational Risk Management (ORM) Function Development Plan	Internal Environment	1. Develop, approve and implement an ORM function "roadmap" (i.e., a multi-year plan defining key milestones by quarter). This roadmap would put the organization on a path to defined benefits and should address the evolution of the following: • ORM structure (with options to increase or decrease resources depending on business strategy) • Operational loss measurement and quantification analyses • Scenario analysis • Use of external loss data • KPIs, KRIs and their use by various levels in the organization • Integration with Sarbanes-Oxley and compliance processes • ORM platform 2. Develop, approve and implement an ORM framework consistent with industry standards. An ORM framework would define the components of ORM and the activities of each component. For example, an ORM framework might be defined as building a common ORM language and culture across five stages of risk management: (1) Risk Definition, (2) Risk Measurement, (3) Risk Monitoring, (4) Risk Allocation and (5) Risk Management. 3. Key components of the ORM program are still under development. The development of a roadmap and framework would allow management to delineate which components need to be developed within which timeframes, as well as which components, are more critical to the success of the ERM program.	N/A	√

DETAILED OBSERVATIONS AND RECOMMENDATIONS: OPERATIONS RISK (2/3)

Observations	Component	Recommendations	Framework	Leading Practice
Enhance ORM Policy	Internal Environment	Develop, approve and implement an ORM policy. While the ERM charter that exists defines the responsibilities of the operations risk committee and the Risk Management Policy addresses several operational risk areas, an ORM policy would define the ORM components including the following: • Roles and responsibilities of entities and key positions as they relate to the ORM framework, e.g. business managers, internal audit, compliance and legal. • Operational functions such as information security, vendor management and business continuity. • Description of operational loss including a methodology for categorizing losses, one example being the Basel 2 categories. • Interaction and dependencies of the ORM function with other risk management and business committees. • Interaction of the ORM function with ERM, compliance, legal and business risks.	√	√
Establish an Operations Risk Platform	Information and Communication	As the framework is developed, consider establishment of an operations risk platform to facilitate processing operations risk information. Such a platform could be as simple as Excel or an Access-based database, or as sophisticated as the leading stand-alone platforms in the marketplace, such as Risk Navigator, Open Pages or Protiviti's Governance Portal. Operations risk information handling will become more important as this component of the ERM program develops. A centralized platform could more efficiently facilitate ongoing identification, analysis, and reporting of operations risk information.	√	√

DETAILED OBSERVATIONS AND RECOMMENDATIONS: OPERATIONS RISK (3/3)

Observations	Component	Recommendations	Framework	Leading Practice
Additional Stress Test Scenarios	Risk Assessment	Leading practices today include additional possible scenarios, which could be modeled with existing technology and data. One example is the “Step Scenario” used in income simulation modeling by which interest rates rise or fall by an equal amount each period over an extended number of periods (e.g., up to 100 to 200 basis point total). Another example is operational risk modeling based on management consideration of potential loss scenarios and the possible or likely loss associated with such a scenario. Modeling in this manner may be more representative of real life market behavior and provide management with a more realistic understanding of possible portfolio performance.	√	√

APPENDIX A: KEY DOCUMENTS REVIEWED

- Strategic Plan
- Risk Assessment
- Risk Assessment Appendix A – Heat Map Summary
- AB 06-02 Model Documentation and Validation
- Audit Committee Charter
- Financial Reports
- Code of Conduct
- Credit Committee Agenda and Minutes
- Credit Committee Charter
- Credit Policy
- Derivatives
- ERM Committee Charter
- ERM Division Charter
- ERM Org Chart
- ERM Staff Bios
- FHFB Final Examination Report
- Finance Committee Charter
- Financial Policy Committee Charter
- Interest Rate Risk Management Model Validations
- Investments and Hedging/ Financial Management Policy
- IT Management Status Report
- Board Meeting Agenda and Handouts
- Finance Committee Meeting Agenda and Handouts
- Market Risk Mgmt Committee Charter
- MPP Credit Structure
- Market Risk Minutes
- Market Risk Reports
- Master Company X Org Charts
- MPP Pool Aggregation Assessment
- Operations Risk Management Committee Charter
- Operations Risk Meeting Minutes
- Product Development Review Committee Charter
- Risk Management Policy
- Treasury Risk Management Monthly Report

Internal Audit Reports:		
1. Advances	2. Derivatives	3. Mortgage Purchase Program
4. Mortgage Purchase Program: S&P Levels Model	5. Investments and Hedging	6. Unsecured Credit and Liquidity

Summit Consulting Ltd / Resources for leading experts
www.summitcl.com