San Francisco State University
Audit, Risk and Compliance (ARC)

Working Session
June 22nd, 2016
Agenda

• Introductions and Vision – Ron Cortez
• Finance Risk Assessment – Jay Orendorff
• 2016 Information Security Audit Update – Julianne Tolson
• Risk Dashboards – Michael Beatty
  – College of Liberal & Creative Arts
  – Student Affairs and Enrollment Management
• Evaluation Methods – Grace Crickette
  – Accountability – Risk Appetite and Tolerance
• Audit and Advisory Services – Helen Storrs
  – MARS 2012 – 2014 Update
• Wrap Up
Finance Risk Assessment

San Francisco State University
We Make Great Things Happen
The Role of Enterprise Risk Management in Achieving Financial Health
Introduction

The higher education sector confronts potential financial dislocation driven by:

- Business model/revenue transition
- Expense management limitations
- Significant on-going capital demands

The form and magnitude of stress will vary across the sector; but the changing environment drives three imperatives:

1. Define and test “Financial Health”
2. Understand the sources and characteristics of potential stressors to financial health
3. Establish a decision-support framework that promotes balance between pursuing financial health and managing risk

© 2016 Kaufman, Hall & Associates, LLC. All rights reserved.
Finance Risk Assessment

1 Defining Financial Health
Realizing Financial Health

Financial health is realized when the institution performs at a level where operating needs are met and sufficient capital is generated from internal or external sources to fund the investments needed to support its mission and remain competitive.

The corridor of control is the balancing point between two opposing goals:

1. Compete as effectively as you can, which requires aggressive investment of capital and commitment of operating dollars, but
2. Respect the fiduciary role of management and the board to maintain the long-term financial integrity of the institution.
Developing the Roadmap to Financial Health Requires Rigorous Multiyear Strategic, Financial and Capital Planning

The financial plan defines the institution’s financial health “glide path.”
Finance Risk Assessment

Step 1: Comprehensive Understanding of Credit Position

- Market Strength: Student Demand & Donor Support
- Capital Needs, Debt and Other Liabilities
- Operating Performance
- Financial Resources & Liquidity
- Legal Structure Convenants of Debt

Source: Moody’s Investors Service
Step 2: Balance Capital Sources and Uses

How much cash?

How much debt?

How should these tradeoffs be optimized within an appropriate credit and risk context?
Step 3: Develop a Realistic Plan That Supports the Execution of the Institution’s Strategy

Finance Risk Assessment

Base Case (Conservative)

Consolidated Results

Initiative #1

Initiative #2

Initiative #3

Initiative #4
To put the Financial Plan into action, Year 1 must be the Institution’s budget, and updates to the Plan must occur annually or more frequently, if needed.
2 Moving from Financial Health to Risk Management
Context: Risk Management Corridor of Control

• Corridors of Control are ultimately about the vertical and horizontal management of Operations, Capital, Liabilities and Invested Assets

• **Financial Health** Corridor of Control:
  – Continuously balance capital investment commitments against financial resources
  – Driven by a series of performance “targets”

• **Risk** Corridor of Control:
  – Continuously balance the role of financial resources in generating return versus offsetting risk
  – Driven by a series of performance “floors”
A Framework for Integrated Risk Management

- The Treasury model that best responds to prevailing needs is a corporate framework that has four defining characteristics:
  1. Is built on a comprehensive point-in-time catalogue of the organization's risks
  2. Maps the risk management contribution available from financial resources
  3. Defines risk-based asset allocation; and tests the impact of deploying invested assets to risk management first and then to the pursuit of returns
  4. Becomes part of the organization's on-going Treasury decision-support and management efforts
1. Cataloguing the Corporate Risk Portfolio

<table>
<thead>
<tr>
<th>Operating Profile</th>
<th>Less</th>
<th>Established Hedges</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cash Flow Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Factor Sensitivities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Discreet Event Exposures</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Liability Profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Tender/Put Events</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Swap Valuations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Market Access Exposure</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capital Profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Baseline Capital Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Discretionary / Strategic Options</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Funding Capacity</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invested Asset Profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Policy, Reporting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Rebalancing, Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Exposures Less Established Hedges</th>
<th>Embedded Risk Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partnership Strategies</td>
<td>Discretionary Spending Options</td>
</tr>
<tr>
<td>Leases</td>
<td>Staggered Events</td>
</tr>
<tr>
<td>Bank Facilities</td>
<td>Diversification</td>
</tr>
<tr>
<td>Collateral Agreements Options</td>
<td>Disciplined</td>
</tr>
<tr>
<td>Strategy</td>
<td>Allocations</td>
</tr>
<tr>
<td></td>
<td>Flex-Planning</td>
</tr>
</tbody>
</table>

Finance Risk Assessment
1. Cataloguing the Corporate Risk Portfolio (continued)

The heart of a corporate framework is a comprehensive catalogue of risks across operations, capital, and liabilities.

For each identified risk the cataloguing process:

- Quantifies the risk over an agreed-upon measurement horizon
- Determines whether a risk can be hedged
- Assesses whether unhedged risks can be offset by management intervention and how this impacts net risk exposure
- Defines a residual risk pool that is either carried by the institution or is offset in whole or in part by available risk resources
2. Defining The Available Corporate Risk Resources

- Risk Capacity is derived from two key sources
  - Credit and Debt Capacity – ability to access external funds (questionable reliability)
  - Cash and Invested Assets – currently available funds
- Once resources are identified, defining the role of and restrictions on cash becomes the key to risk tolerance (capacity)
3. Risk Framework That Integrates Operations and Balance Sheet

- Can connect operations and the balance sheet by aligning invested assets allocated to risk management against tiered risk pools (tiered by liquidity characteristics)
- Remaining resources are free to pursue return, subject to defined risk tolerance and Investment Policy Statement constraints
3. Risk Framework That Integrates Operations and Balance Sheet

- Result is risk-based asset allocation that can be compared to existing allocation to gauge net risk and the cost of hedging.
4. The Framework as a Core Decision Support Tool

**Integrated Framework Value:**
- Responds to the prevailing environment by allocating risk resources across operations, liabilities and invested assets
- Identifies and tests different risk positions and the corresponding impact on risk-adjusted returns
- Enables the assessment of different risk and hedging combinations

**Risk Framework In Practice:**
- Clarifies the connection between operations-capital-liabilities-invested assets in generating and managing risk
- Defines a single, global risk map under one analytical umbrella
- Assesses response options; whether and how to hedge, manage, and otherwise mitigate identified risks
- Defines the overall cost of benefit of a risk-based approach to resource deployment
- Operationalizes so that it becomes part of ongoing review and decision support; potential inclusion in IPS
Operationalizing establishes a decision-support framework that offers management and governance access to the wide-angle perspective they need to navigate periods of change and stress.

**Evaluation**
- **Concept:**
  - Assess risk catalog contribution
  - Determine key risk initiating factors (e.g. rates, third-parties, etc.)
  - Quantify; understand cash flow and fair value impact
- **Analysis:**
  - Cash flow variability
  - Event risks
  - Counterparty exposures

**Impact**
- **Concept:**
  - Determine risk responses and mitigates
  - Understand quality of any natural hedges
  - Assess impact to tiers
- **Analysis:**
  - Risk Response
  - Risk Map
  - Tiered Liquidity

**Rebalancing**
- **Concept:**
  - Determine impact to investment risk and allocations
  - Determine if sizing requires full analysis refresh
  - Explore methods for refining exposure
- **Analysis:**
  - Asset Allocation Strategy
  - Heuristics and linear adjustments
  - Group Discussion
Finance Risk Assessment

3 Conclusion and Questions
Conclusion

• Higher educational institutions are complex operating companies with varied and transitioning return and risk characteristics

• The prevailing environment dictates two imperatives that apply to all types of institutions
  1. Establish and maintain a financial planning infrastructure that supports the definition and pursuit of Financial Health
  2. Use that same planning infrastructure as part of a corporate risk framework that integrates operations-capital-liabilities-invested assets under a single decision-support umbrella

• Treasury should sit in the wheelhouse of these initiatives – using them to help test and inform how balance sheet resources dynamically relate to operations and how they should best be deployed

• Best practice application makes this a powerful multi-disciplinary process that creates a way to organize and direct strategic, operating and financial thinking across the organization both today and on an ongoing basis
Information Security Audit Update

Overview

• Audit had nine observations / recommendations
• Some observations map to the same response
• Work on most challenging responses prioritized
Network Access Control (NAC)

Addresses observations 7, 8, & 9

• Infrastructure project to authenticate users of devices connecting to wired network
• First phase to secure the network ports in public locations
• Equipment ordered communication startles, deployment planned
• Discovery scans have identified devices with obsolete operating systems

For more information see: http://tech.sfsu.edu/guides/network-access-control-nac
Multi-Factor Authentication (MFA)

Addresses observation 3

• Infrastructure project to first update the campus Virtual Private Network (VPN)
• Updated VPN with Duo two-factor authentication completed
• Updated VPN with Duo deployed in an ITS pilot
• Communication with users under development

For more information see:
https://duo.com/ & https://vpn.sfsu.edu
Information Security Audit Update

Survey of decentralized compliance with Information Security Policy

Addresses observations 1, 2, 4, 7 & 9

- Infrastructure project to first update the Virtual Private Network (VPN)
- Updated VPN with Duo two-factor authentication completed
- Updated VPN with Duo deployed in an ITS pilot
- Communication with users under development
Vulnerability Management

Addresses observations 5, 7 & 9

- Reviewed campus subnets to identify subnets dedicated to a unit and those shared access units
- Created business areas to map dedicated and shared subnets
- Will reorganize the monthly scan to use revised business areas for improved accountability
Information Security Audit Update

Incident Reporting

Addresses observations 1, 4 & 9

• Existing incident process reviewed and compared to industry best practices
• Revised incident procedure deployed for high risk incidents
• Missing DMCA complaint procedure drafted
Firewall Settings

Addresses observation 6

• Campus firewall rules were reviewed and any security deficiencies re-meditated

• Campus firewall rules have been reviewed and changes proposed to streamline rule processing
<table>
<thead>
<tr>
<th></th>
<th>CUSTOMER</th>
<th>FINANCIAL</th>
<th>PROCESS</th>
<th>PEOPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Training mitigates risk</td>
<td>Property Claims 1 claim; $77,000</td>
<td>Audit Observations 0</td>
<td>Worker’s Comp Claims 4,327 EEs; 1 Claim; $1,046</td>
</tr>
<tr>
<td></td>
<td>Claims can be an indicator of a need for</td>
<td></td>
<td>Harassment Prevention Training Completion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>improved management and controls</td>
<td></td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Weak Controls + Lack of Accountability lead</td>
<td></td>
<td>Data Security Training Completion 56.18%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>to inefficiency and financial loss and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>compliance risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Training mitigates risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Risk Dashboard

### Student Affairs & Enrollment Management

<table>
<thead>
<tr>
<th>CUSTOMER</th>
<th>PROPERTY CLAIMS</th>
<th>0 claims</th>
</tr>
</thead>
<tbody>
<tr>
<td>FINANCIAL</td>
<td>CONFlict of Interest Compliance Training Completion</td>
<td>100%</td>
</tr>
<tr>
<td>PROCESS</td>
<td>Harassment Prevention Training Completion</td>
<td>100%</td>
</tr>
<tr>
<td>PEOPLE</td>
<td>EPL Claims</td>
<td>1 claim; $62,210</td>
</tr>
</tbody>
</table>

**Training mitigates risk**

**Claims can be an indicator of a need for improved management and controls**

**Weak Controls + Lack of Accountability lead to inefficiency and financial loss and compliance risk**

- **Unfound Inventory**: 21.17%
- **Data Security Training Completion**: 56.18%
- **Audit Observations**: 4
- **Worker’s Comp Claims**: 404 EEs; 15 Claims; $121,028
- **Ergo Evaluations**: 14 of 404 EEs
- **Compromised E-mail Account Incidents**: 20 (9% of Univ. EEs; 9% of Incidents)

Training mitigates risk.

Claims can be an indicator of a need for improved management and controls.

Weak Controls + Lack of Accountability lead to inefficiency and financial loss and compliance risk.
Which colleges/departments are next?

Any Volunteers?
### Data / Systems Security:

Ability to safeguard data and critical operational data.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Target</th>
<th>Actual</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PCI Compliance</strong></td>
<td>% of Compliance</td>
<td>100%</td>
</tr>
<tr>
<td><strong>Security Risk Management Program</strong></td>
<td>% of Completion</td>
<td>100%</td>
</tr>
<tr>
<td><strong>ISO Compliance</strong></td>
<td>% of compliance with ISO 27001 / 27002</td>
<td>95%</td>
</tr>
</tbody>
</table>

**Score**: 63%

**Management Mitigation Plan**: The execution of a 27-point plan to lock down intrusion detection and protection is underway; The Security Risk Management Framework is underway and will be updated quarterly; Assess systems against ISO 27001/27002.

**Accountable Executive**: CIO
Audit and Advisory Services
Management Agreed Upon Responses Status

• For reports issued in 2012-2014, A&AS has verified actions for 85 out of 109 responses. Completion dates have been obtained for the remaining 24 responses.

• A&AS has begun meetings for reports issued from January to June 2015.
2016 ARC Meeting Schedule

• June 22, 2016
• August 10, 2016
• October 12, 2016
• December 4, 2016
Wrap Up