

# UNDERSTANDING THE BUSINESS PERSPECTIVE

## Practice Driver

Noting frequent resistance to adoption of new security policies and controls, the CISO at Boxwell sought a more systematic approach for measuring user preferences and risk tolerances. However, the sheer scale of the organization (Boxwell employs more than 35,000 individuals in dozens of countries) served as a major impediment.

## Risk Tolerance and Usability Indicators

Rather than measuring the preferences and tolerances of each individual employee, Boxwell created a proxy by researching senior executive opinion and surveying key middle managers throughout the business on 14 key dimensions. The process for creating these risk tolerance and usability indicators is described below.

- **Step #1: Risk Tolerance Survey Design**—Information Risk creates 14 sliding scales that measure risk tolerances and usability preferences on key dimensions.
- **Step #2: Risk Tolerance Calibration via Executive Anchors**—Information Risk anchors the indicators based on executive opinion to ensure business managers' preferences remain within acceptable boundaries.
- **Step #3: Survey Administration**—Information Risk interviews more than 20 midlevel business and IT managers to further calibrate organizational risk tolerance and usability preferences to ensure the final indicators incorporate senior executive opinion and on-the-ground realities.
- **Step #4: Business-Informed Decision Making**—Information Risk staff members use the indicators as a guide to make more prudent security architecture decisions that effectively balance information security and business needs.

# UNDERSTANDING THE BUSINESS PERSPECTIVE

**Faced with numerous business-relevant trade-offs when making changes to the security architecture...**

**...but lacking the ability to assess the tolerances and preferences of thousands of employees...**

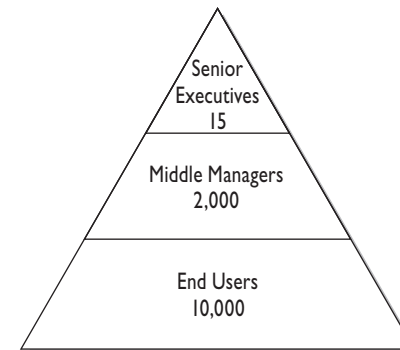
Sample Trade-Offs for Microsoft Vista Deployment

*Illustrative*

	<b>Option 1</b> Use Built-In Security Features	<b>Option 2</b> Use Best-of-Breed Security Add-On Products
1. Level of Required User Activity	High	Low
2. Capital Cost	Low	High
3. Ability to Enforce Control Adoption	Low	High

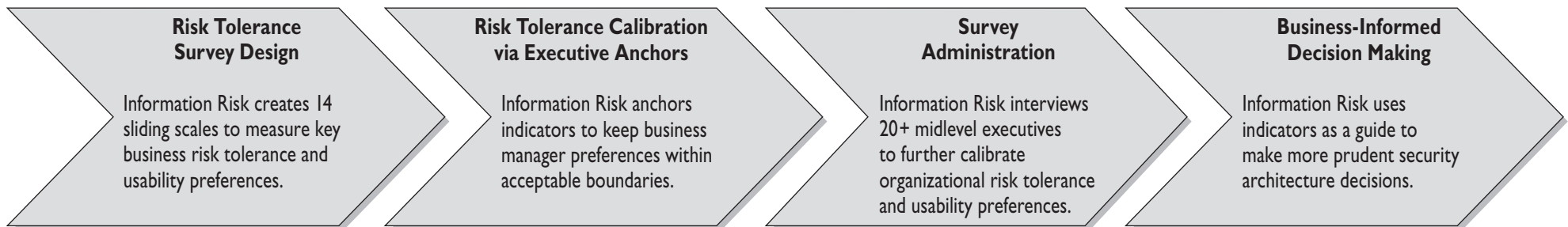
Sample Corporate Hierarchy

*Illustrative*



**...Boxwell creates risk tolerance and usability indicators to guide more business-friendly architecture decisions**

Process for Creating Risk Tolerance and Usability Indicators



\* Pseudonym.

Source: Boxwell; IREC research.

This study may not be reproduced or redistributed without the expressed permission of the Corporate Executive Board Company. The Information Risk Executive Council has worked to ensure the accuracy of the information it provides to its members. This report relies upon data obtained from many sources, however, and the Information Risk Executive Council cannot guarantee the accuracy of the information or its analysis in all cases. Furthermore, the Information Risk Executive Council is not engaged in rendering legal, accounting, or other professional services. Its reports should not be construed as professional advice on any particular set of facts or circumstances. Members requiring such services are advised to consult an appropriate professional. Neither the Corporate Executive Board nor its programs are responsible for any claims or losses that may arise from a) any errors or omissions in their reports, whether caused by the Information Risk Executive Council or its sources, or b) reliance upon any recommendation made by the Information Risk Executive Council.

# TAKING THE PULSE OF THE ENTERPRISE

## Setting the Anchors

The first step in the calibration process is to anchor the indicators around the preferences of executives. The CISO decided to set these anchors to ensure that the opinion of middle management did not stray too far from those set by the senior leadership of the company. To gauge the preferences of senior management, the CISO relied on the following:

- Established security policies
- Prior discussions with executives
- Public statements by executives
- Internal company statements by executives

## Incorporating Feedback from Middle Management

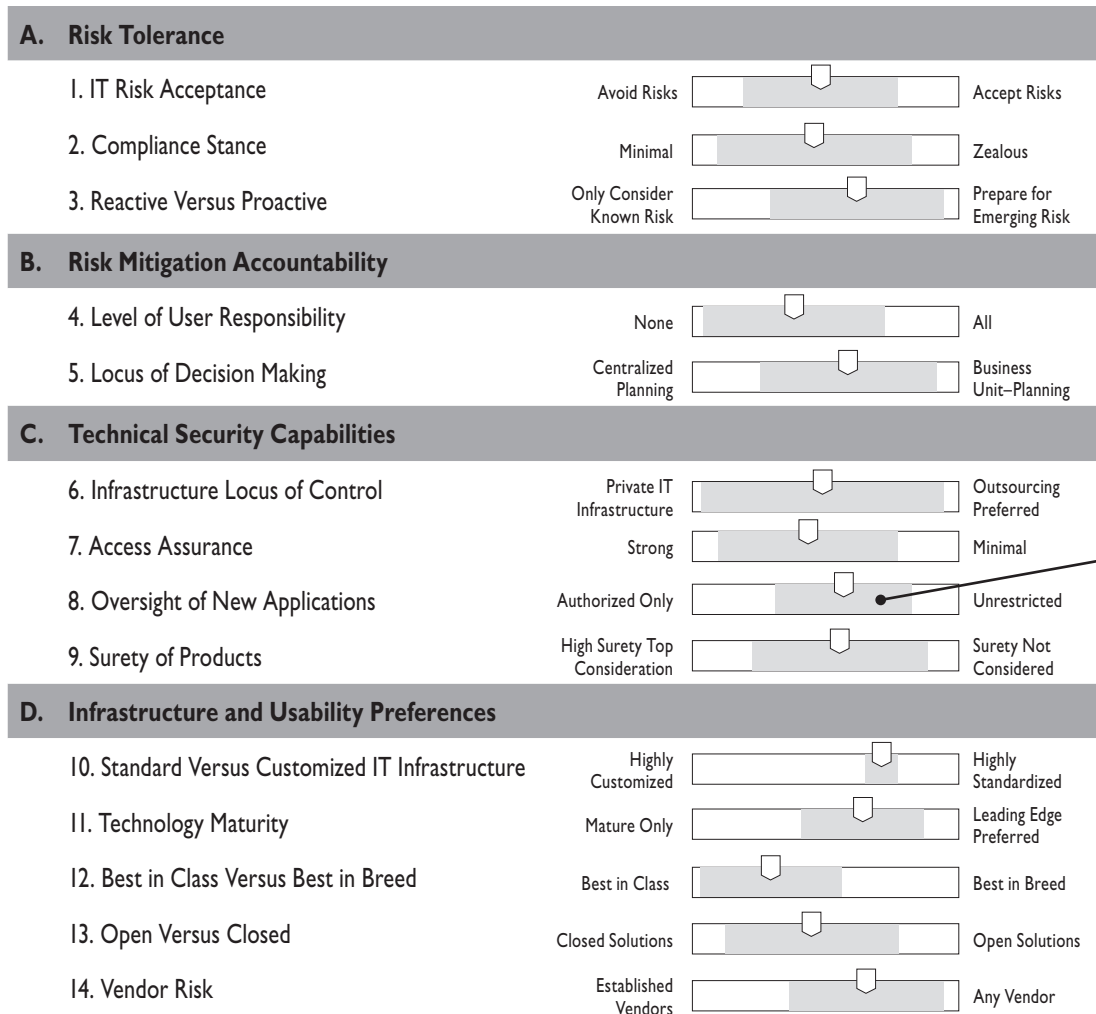
After the executive anchors were established, the CISO met with 10 IT managers and 10 general managers in several key business units throughout the company. The goal was to balance executive preferences with the preferences of people on the ground in the operational environment. The process for blending middle management preferences with those of senior executives works as follows:

- **Step #1**—CISO meets one-on-one with IT or general manager, presents an anchored copy of each of the 14 indicators, and explains the meaning of the indicator.
- **Step #2**—Business or IT manager moves the indicator to a position based on their personal preference.
- **Step #3**—After completing the process for 20 managers, the CISO averages the results and sets a final calibration for the indicator.

# TAKING THE PULSE OF THE ENTERPRISE

**CISO creates 14 sliding scales that are anchored on executive preferences and informed by middle management to capture the overall business sentiment on key drivers of security architecture decisions**

## Risk Tolerance and Usability Indicators



### Calibrating the Indicators

CISO selects a cross section of IT and general business middle managers to calibrate the right tolerances and preferences.

- Senior IT Managers (10)—Provide IT perspective on architectural preferences
- Senior Business Managers (10)—Provide business perspective on risk tolerances

### Setting the Anchors

CISO uses the following resources to set executive anchors:

- Public statements by executives
- Established security policies
- Internal company statements by executives
- Prior discussions with executives

\* Pseudonym.

Note: To protect the sensitivity of this information, the placement of indicators is hypothetical and does not reflect actual preferences at Boxwell.

Source: Boxwell; IREC research.

This study may not be reproduced or redistributed without the expressed permission of the Corporate Executive Board Company. The Information Risk Executive Council has worked to ensure the accuracy of the information it provides to its members. This report relies upon data obtained from many sources, however, and the Information Risk Executive Council cannot guarantee the accuracy of the information or its analysis in all cases. Furthermore, the Information Risk Executive Council is not engaged in rendering legal, accounting, or other professional services. Its reports should not be construed as professional advice on any particular set of facts or circumstances. Members requiring such services are advised to consult an appropriate professional. Neither the Corporate Executive Board nor its programs are responsible for any claims or losses that may arise from a) any errors or omissions in their reports, whether caused by the Information Risk Executive Council or its sources, or b) reliance upon any recommendation made by the Information Risk Executive Council.

INTERESTED IN MORE ON THIS TOPIC?

Contact Our Member Support Center at:

**E:** [EXBD\\_Support@executiveboard.com](mailto:EXBD_Support@executiveboard.com)

**P:** +1-866-913-2632