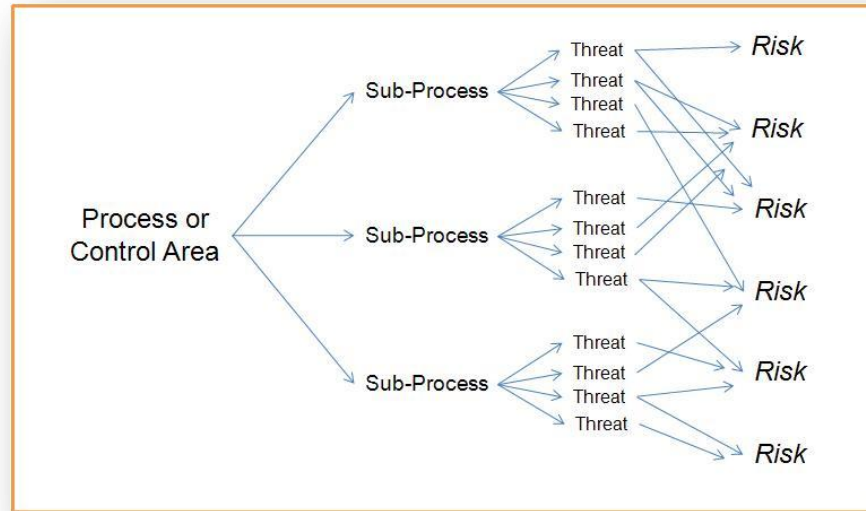


*Findings of an Independent Risk Evaluation for
XYZ Company*

July 2009

Evaluating Information Technology Risk

The risk evaluation is based on operational information collected from a representative group of Information Technology managers and executives. Using methods based on industry-standard frameworks, potential threats relating to strategy, policy and practice are examined, analyzed and classified...

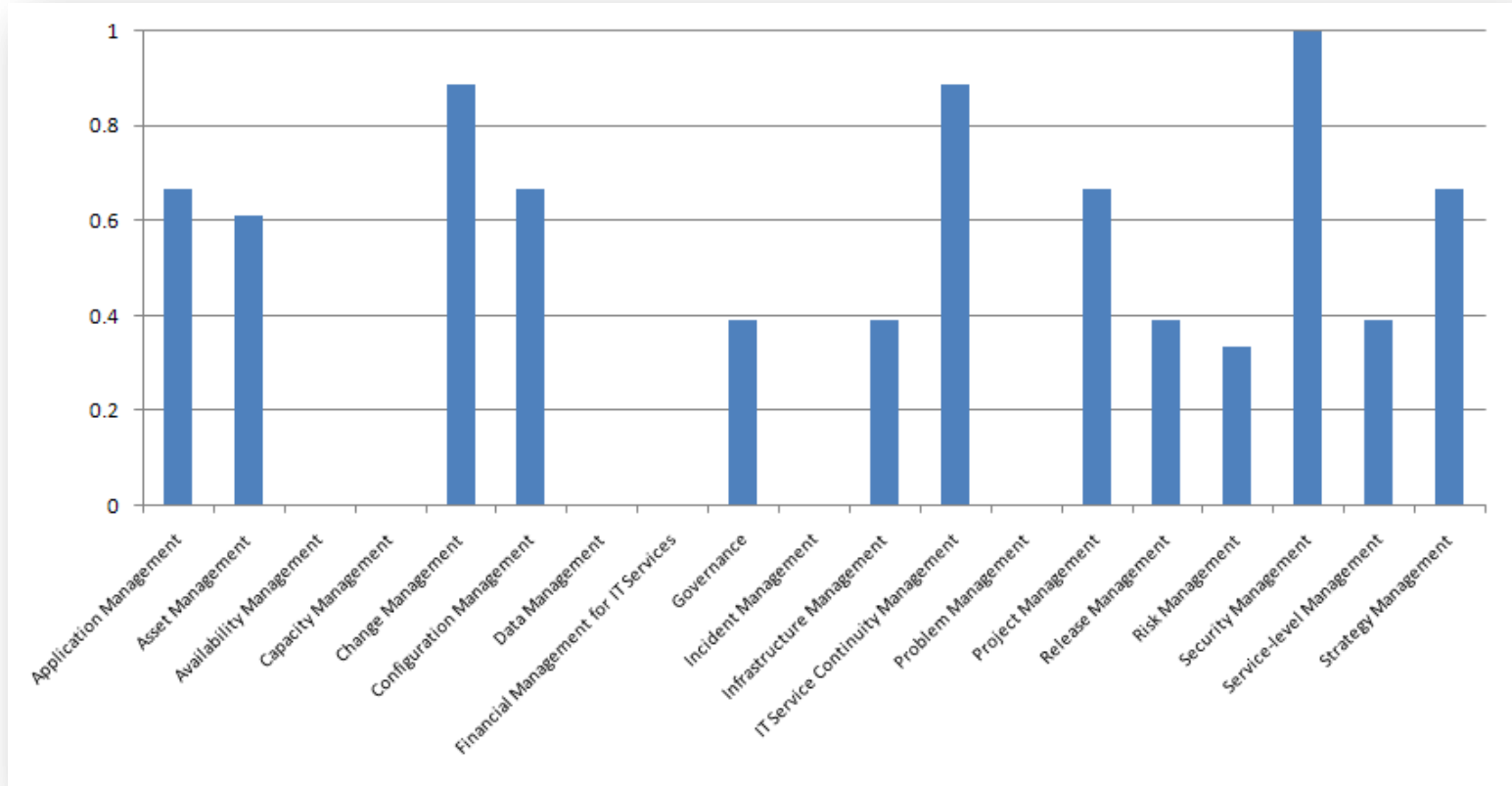


Leveraging a facilitated session, the CIO and IT management team of XYZ Company participated in a risk evaluation on June 16, 2009. The findings of that evaluation are contained in this report.

Establishing the Baseline

To better understand the operating environment, industry influences and risk tolerance, a baseline assessment is conducted prior to the formal evaluation. Respondents provide a relative priority and perceived risk level (high, medium or low) for each of 19 predefined **control areas**...

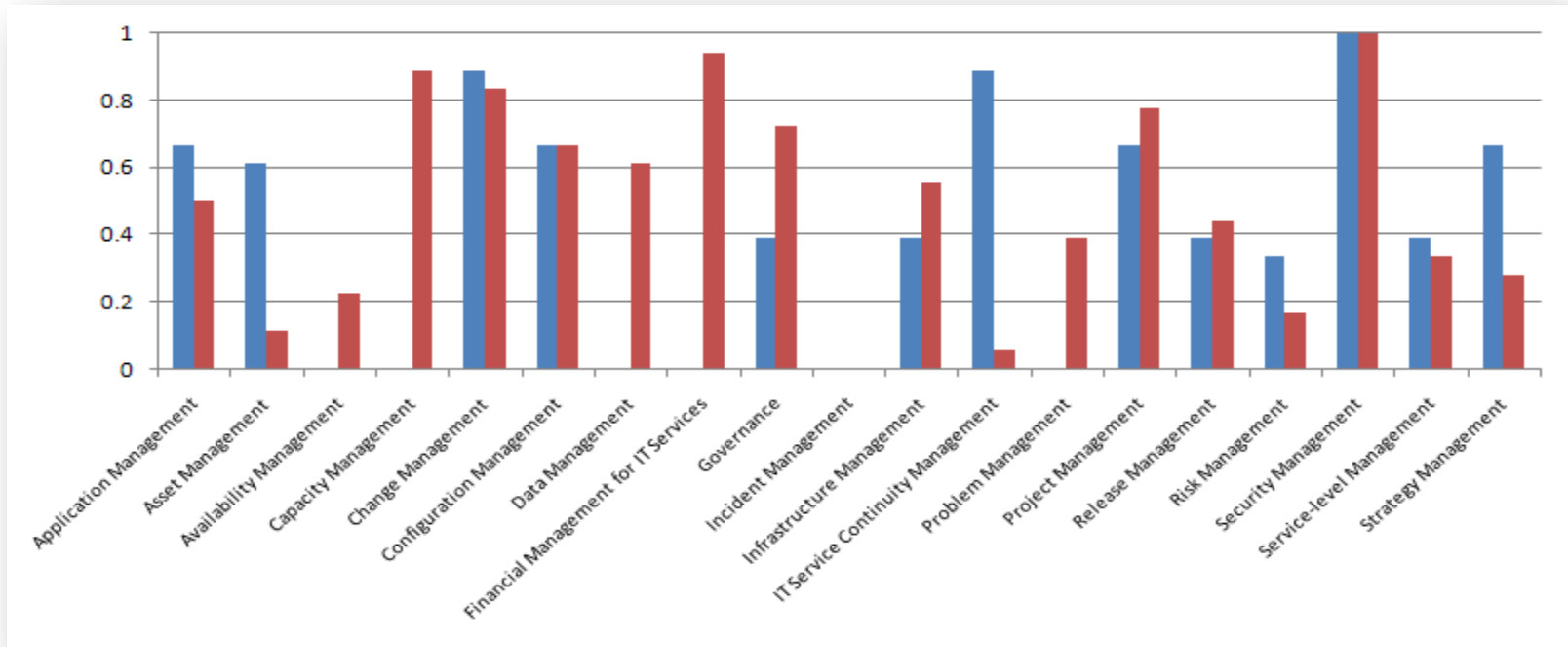
The baseline* for XYZ Company is illustrated in the chart below:



* Values normalized using Percent Rank to show relative importance and risk

Using the Evaluation Findings

Comparing the baseline to the evaluation results provides a clear picture of the differences and offers insight into what's actually going on in the department...



Evaluation responses relating to the probability of occurrence for specific threats within the 19 control areas for XYZ Company illustrate the following:

Control Areas identified as areas of potentially significant risk: **Capacity Mgmt, Change Mgmt, Configuration Mgmt, Data Mgmt, Financial Mgmt for IT Services, Governance, Project Mgmt, Security Mgmt.**

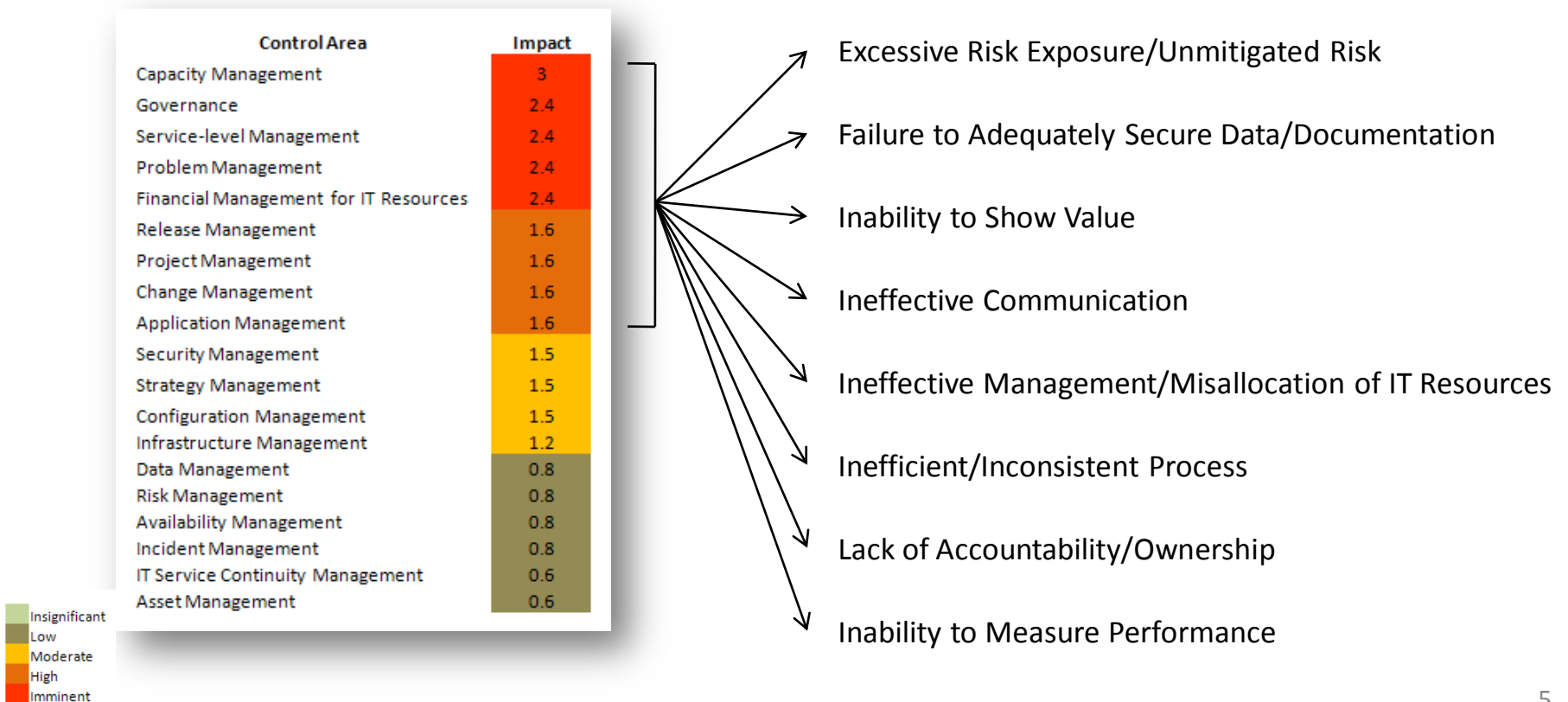
Control Areas identified as areas for which the current mitigation strategies may be effective (i.e. risk is well-mitigated): Asset Mgmt, IT Service Continuity Mgmt and Strategy Mgmt were.

Threat to Risk Mapping

Control Areas map through sub-processes to threats and, left unaddressed, can cause a number of potentially serious problems...

Using a standard scale, specific threats for each control area were classified into one of 5 categories:

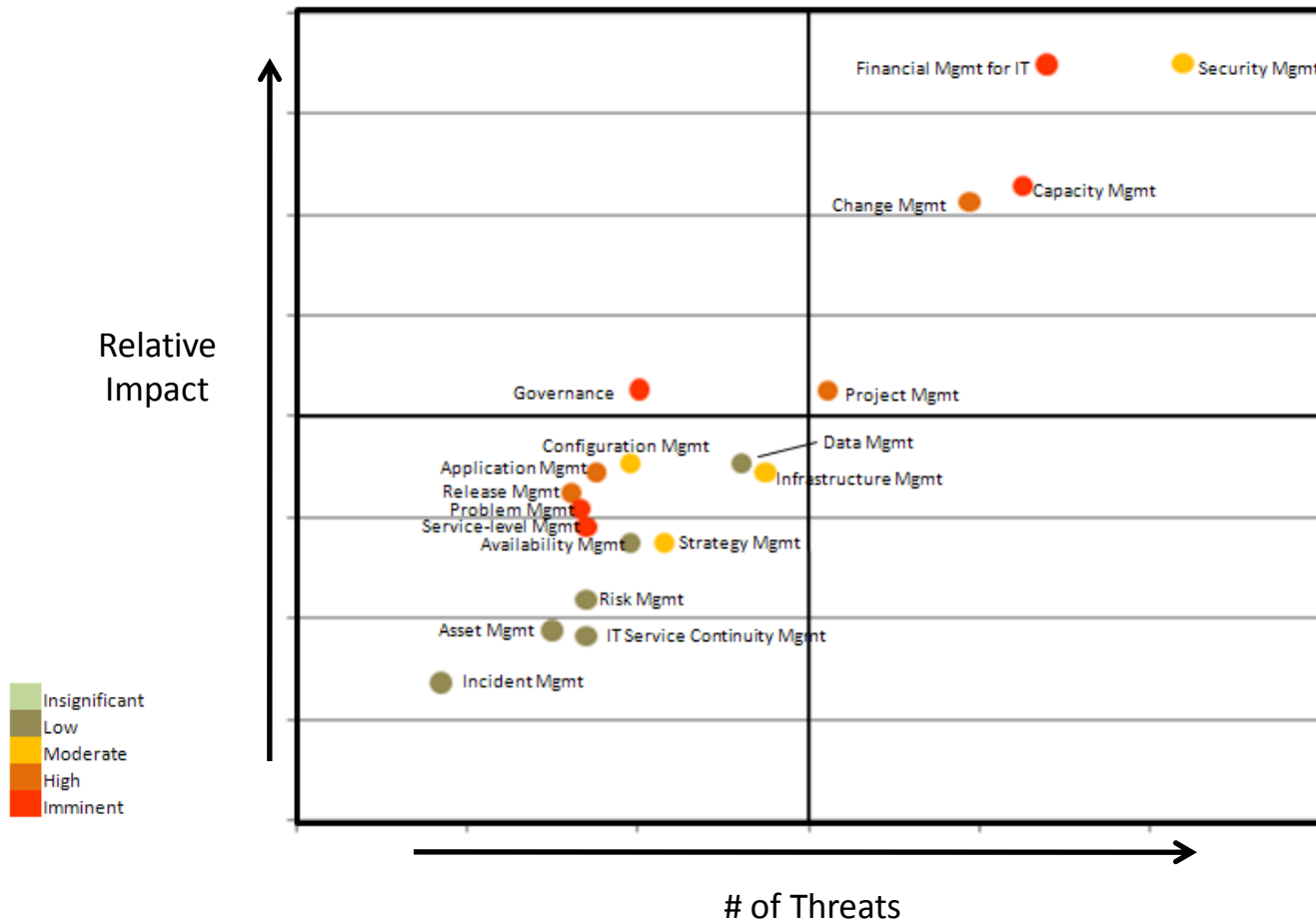
- Insignificant
- Low
- Moderate
- High
- Imminent



Focusing for Payback

This chart provides a ranking for control areas, based on the number and severity of the threats associated with them and their significance in the overall risk portfolio...

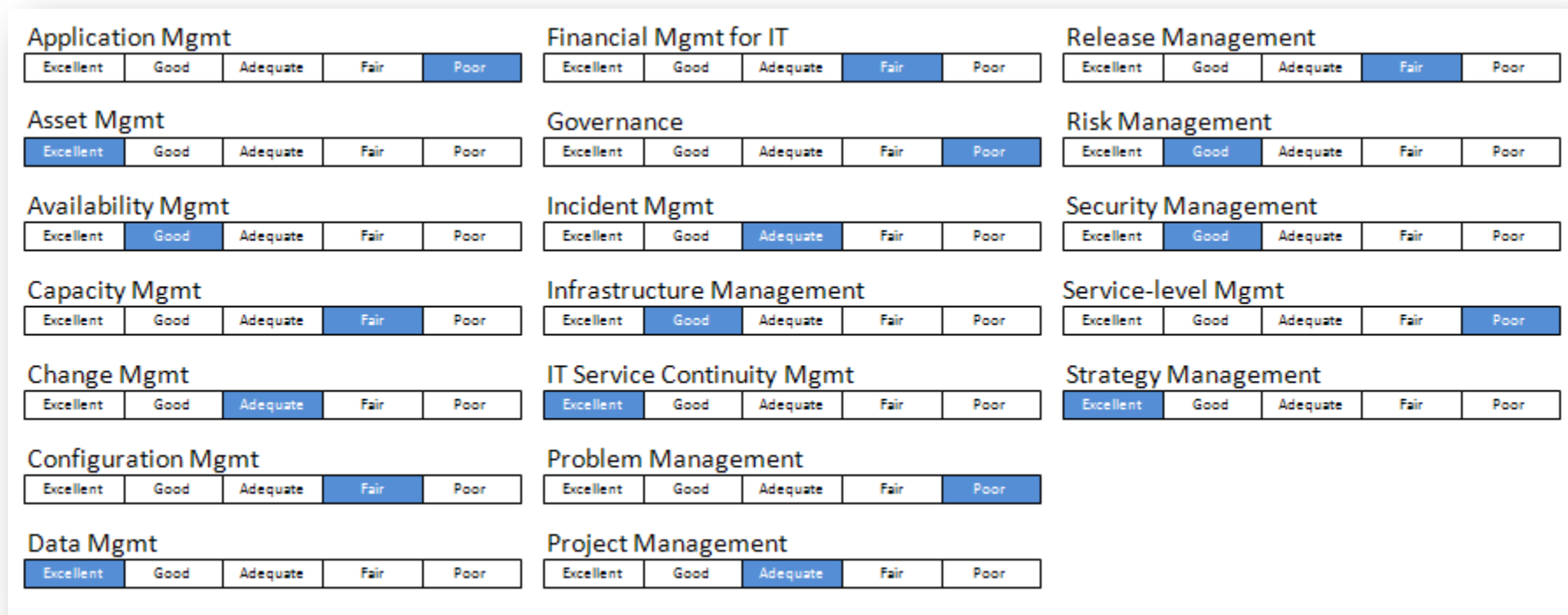
Financial Mgmt and Capacity Mgmt are high priorities with potentially severe threat levels while Security Mgmt carries risk predominantly based on its reach.



Addressing threats and mitigating risks associated with control areas in the upper right quadrant provides the most significant reduction in overall risk .

Score by Control Area

Using the relative impact and severity index for each threat, an overall score can be determined by control area. A simple average of the scores, provides a score for the portfolio...



Overall Risk Portfolio for XYZ Company:

Excellent	Good	Adequate	Fair	Poor
-----------	------	-----------------	------	------

Recommendations

Specific to the findings in this report for XYZ Company, Enterprise Risk Associates, LLC recommends focusing on the following priorities...

- Reduce the probability of occurrence for threats tied to the following control areas (identified and cataloged in Quadrant 4 of the diagram on page 6 of this report:
 - Security Management
 - Financial Management for IT
 - Capacity Management
 - Change Management
 - Project Management

- Formalize processes for areas where little or no current, documented and/or published process/policy exists (i.e. Governance)

- Reduce the severity of threats related to the following sub-processes (identified and categorized as “Imminent”):
 - Manage IT Human Resources
 - Monitor and Evaluate IT Performance

- Improve the overall risk portfolio from **Adequate** to **Good**