

The Bank of Bolsa Chica

Bank of Bolsa Chica

Risk Assessment

FFIEC Case Summary Report

June 1, 2007

**Mr. Jean Smith, President
Ms. Andrea Watson, Analyst**

The Bank of Bolsa Chica

Risk Assessment Case Summary Report

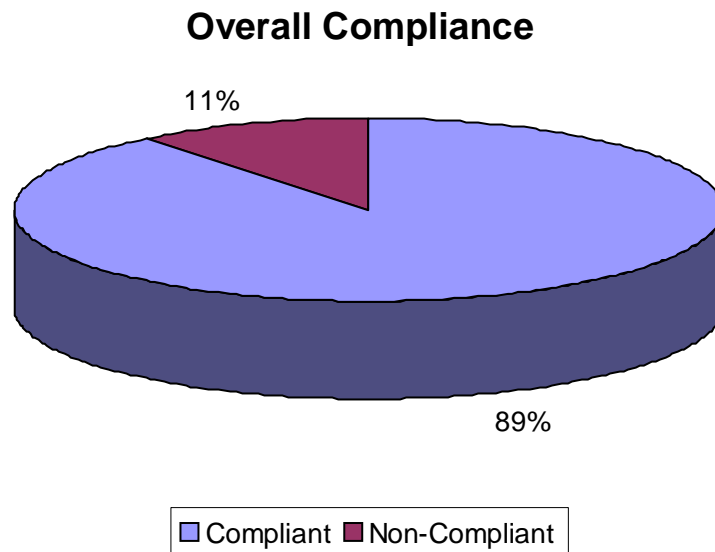
Background

The Bank of Bolsa Chica performed a self-assessment of internal IT systems and systems run by technical service providers to meet the FFIEC Risk Assessment Guideline. Information was provided by the user with input (if selected) by the third party providers under review.

The increasing alignment between the information technology infrastructures with the business units within the Financial Institution now includes looking at Return On Investment for security controls, corporate governance and reputation risk. Enterprise risk management compliance should be the primary driver for IT spending and should contribute to the budgetary processes.

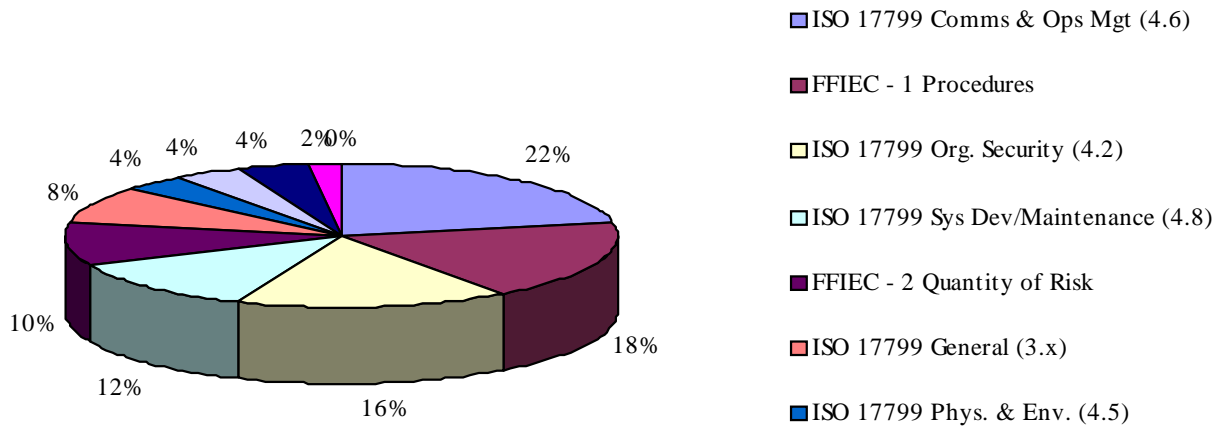
Vulnerability Analysis

The Bank created web questionnaires designed to measure the level of the organizational vulnerabilities according to the **FFIEC Guidelines and ISO standards**. There were 20 vulnerabilities discovered. Completed responses were received from **8 respondents**. In total, there were **170 different questions answered** and of those **18 had non compliant answers**.

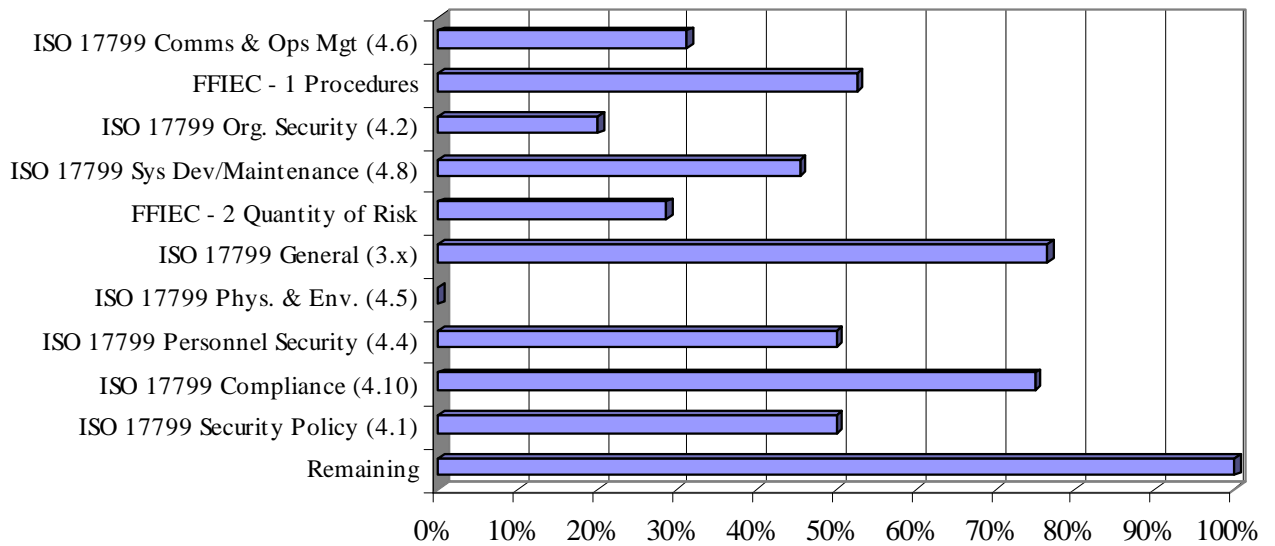


The analysis of the non-compliant responses is provided below. The pie charts show the percentage of answers that were answered as non-compliant, that is received a score below the 80 % threshold. The bar charts show the percentage of the answers that were at or above the threshold compared to the total number of answers in each category presented.

Non Compliant Answers by Question Category

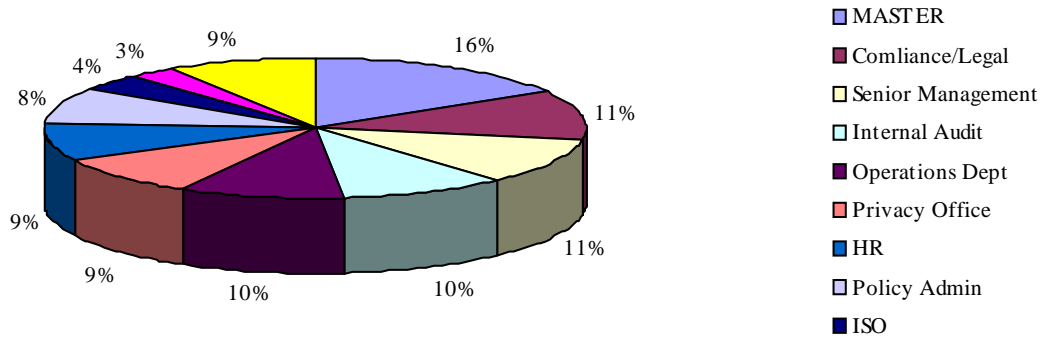


Question Category Compliance



QUESTION_CATEGORY	NC	Comp	NotApp	Unk	NoAns	Average Score	Compliance
FFIEC - 1 Procedures	136	121	38	119	2	65.2%	47%
FFIEC Tier II Procedures - A. Access Rights Administration	134	130	7	48	0	71.4%	49%
FFIEC Tier II Procedures - J. Intrusion Detection and Response	130	211	9	117	1	70.1%	62%
FFIEC Tier II Procedures - A. Authentication	129	218	51	188	1	73.0%	63%
FFIEC - 4 Adequacy Policies	126	186	18	66	1	75.9%	60%
FFIEC - 2 Quantity of Risk	70	101	5	31	1	72.7%	59%
FFIEC Tier II Procedures - B. Network Security	68	219	12	45	0	82.0%	76%

The process of risk analysis was also used to measure compliance with existing requirements. The categories of compliance are listed on the left in the graph above. Questions measuring compliance are linked to each of these vulnerability categories. The graph illustrates how well respondents in different job categories reported they complied with the various parts of the standard. Percentages of compliance are listed along the bottom of the graph. It is possible to see the results of the surveys both by individual and by job title.



RESPONDENT	NC	Comp	NotApp	Unk	NoAns	Average Score	Compliance
MASTER (Analyst)	207	113	10	4	0	55%	35%
Sherry Smith	133	70	6	9	0	59%	34%
Sam Nicholls	10	179	0	61	1	87%	95%

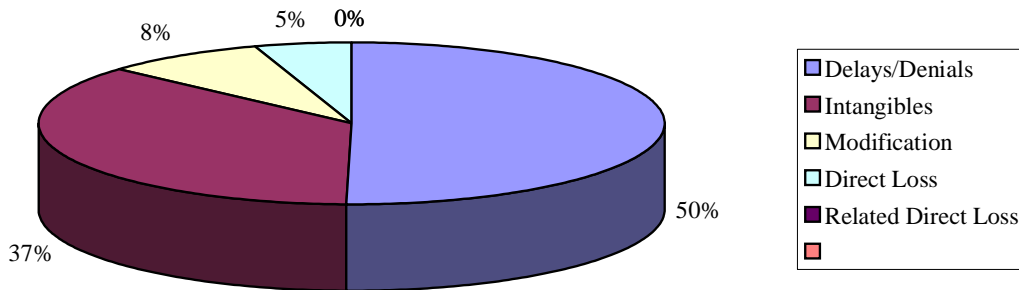
Fred Powell	0	4	0	0	0	100%	100%
Gina Davis	0	7	0	2	0	93%	100%

RESPONDENT	NC	Comp	NotApp	Unk	NoAns	Average Score	Compliance
Bill Smith	124	49	9	36	0	75%	28%
Ron Lee	110	12	1	24	0	45%	10%
Deb White	97	24	12	22	0	65%	20%
Dave Hall	49	70	1	74	0	85%	59%
Mark Smith	47	137	8	22	0	84%	74%
Jane Gibbs	43	37	0	46	3	80%	46%
Barb White	43	78	102	10	0	86%	64%

Annual Loss Expectancy (ALE)

The report analyzed the Bank of Bolsa, Online Banking Systems including **27 assets** in **10 asset categories**, **6 loss categories** and **37 separate threats**. Each asset and threat pair was linked to different types of losses including direct losses, indirect losses, losses due to delays or denial of service, disclosure losses, modification losses, and intangible losses; and each combination can have a degree of severity associated with it, based on the potential impact. . The following charts show the distribution of potential losses for the asset categories, threats and loss categories selected for use in this case. The ALE (Annual Loss Expectancy) was modeled by Asset Category, Threat Category and by Type of Loss.

Annual Loss Expectancy by Loss Type
--

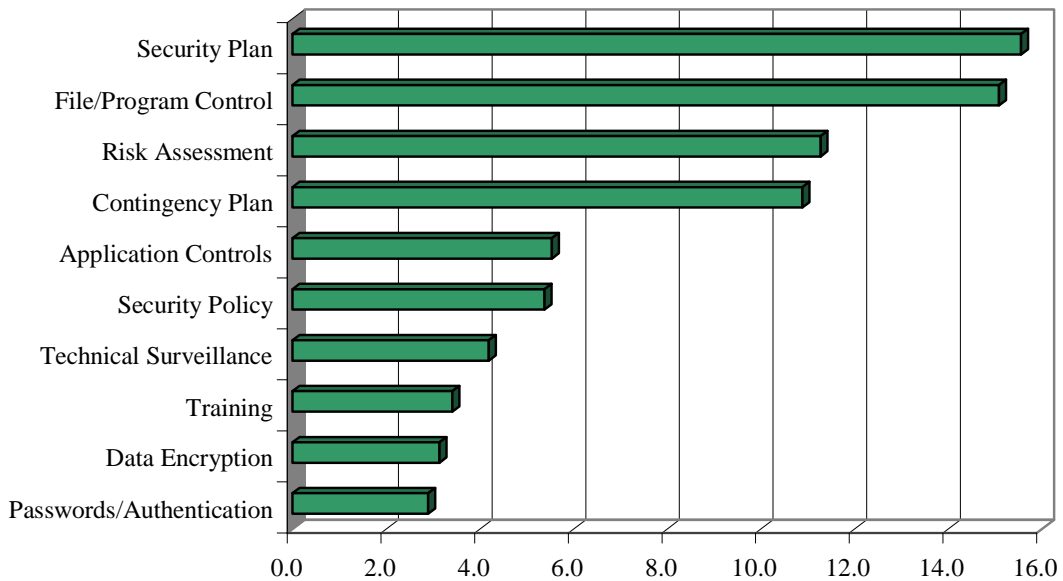


The risk assessment produced incident ratings for the highest threats, the organizational vulnerability level, and recommendations on cost-effective controls to mitigate the risk.

Return on Investment (ROI)

The objective of the ROI analysis is to evaluate prospective safeguards to test what reduction if any would occur with the implementation of that specific Safeguard. The reduction in ALE, called the Benefit, is then compared with the cost of implementation and operation of each Safeguard to produce a single value which is the return on investment (ROI). The ROI is the annual benefit of the recommended safeguard, divided by the total annual cost.

Return on Investment (0% Discount)



SAFEGUARD	% In Place	Life Cycle	Cost/yr	Savings/yr	ROI
File/Program Control	20	3	\$46,667	\$2,105,669	97.8
Encryption	25	3	\$132,235	\$4,557,790	34.5
Documentation	75	3	\$25,833	\$873,855	33.8
Property Management	0	3	\$36,667	\$1,147,454	31.3
Visitor Control	0	2	\$150,000	\$3,946,505	26.3
Training	0	3	\$83,333	\$1,735,281	20.8
Application Controls	20	3	\$210,987	\$3,512,764	16.6
Audit Trails	30	3	\$90,745	\$1,490,828	16.4
Passwords/Authentication	50	3	\$203,333	\$3,071,075	15.1

The results of the risk analysis can be used to create a protection strategy for the Bank that includes the following strategies.

Risk acceptance: A managerial decision to **accept** a certain degree of **risk**, usually for technical or cost reasons. For example, a bank has to maintain an open physical environment because customers must come into the bank. The bank accepts the risk associated with customers entering the bank.

Risk mitigation: Mitigation solutions are point product solutions or services designed to **reduce the impact or prevent the occurrence of a specific incident**. Examples of mitigation solutions include guard services, alarm systems, firewalls and intrusion detection software.

Risk transfer: Risk transfer solutions are designed to **share risk** and the attendant financial burdens across multiple organizations when an incident does occur. Examples of such solutions include insurance policies, contract terms and reciprocal agreements.

Event recovery/business continuity: Event recovery services enable the **resumption or continuation of business** or mission activities following an incident. They can include things as simple as software system backup product solutions or as extensive as hot sites and cold sites (fully redundant systems or facilities).

Residual risk: Recommendations based on cost effectiveness and the possibility of additional mitigation below a certain level were outlined for management and Board action.