



# Benchmarking Your Business Continuity Plan

*August 2010*

# **2010 Business Continuity Report – Benchmarking Your Plan**

## Introduction

A new business continuity planning section was added to Callahan & Associates annual technology survey for the first time in 2010 to help gather information on this key area. Ongoing Operations, a national business continuity CUSO, helped develop and sponsor this portion of the survey to allow credit unions to benchmark their plans. Data has been segmented by asset size to help facilitate this type of comparative analysis.

## Methodology

Callahan's seventh annual technology survey presents an annual picture of credit union technology priorities and budgeting. The 2010 survey results are based on 95 credit union responses, representing \$62 billion in industry assets. Respondents ranged from \$7 million to \$5 billion in assets, with an average asset size of \$652M.

Respondents to the online survey were surveyed on their existing technology, future plans, technology budgeting and staffing.

Data included in this report is based on a series of questions regarding the credit union's business continuity planning.

## Key Findings

### ***Credit union technology budgets expected to rise with investment due to regulatory compliance and member service enhancements.***

- The majority of credit unions (63%) say their technology budget has increased in 2010. Overall, 22% of credit unions say that their budget will remain the same, with 15% reporting a decline. This represents a change from the 2009 survey, when more than a quarter of respondents reported a decreased technology budget (28%).
- One reason that many credit unions are increasing their technology budgets is due to regulatory compliance. New and existing federal regulations are placing a greater burden on credit union operations.
- Despite the difficult operating environment, credit unions are investing in member-facing enhancements, particularly those that help them target new segments, and streamline their ability to meet member needs. The majority of credit unions across all asset sizes have increased their spending for member-facing enhancements, although the types of projects vary.
- The majority of credit unions do not expect to add IT staff this year, while few are planning to decrease their staff. Credit unions expecting to add any staff will increase by one or two positions.

### ***Business continuity strategies vary by credit union asset size.***

- The person with responsibility for business continuity at the credit union varies, with no single functional area mentioned by a majority of respondents. About one-third of credit unions place responsibility with the IT department, including the CTO, VP IT or an IT manager. For about one-fourth of credit unions, a committee has responsibility.
- Spending on business continuity varies by asset size, but the majority of credit unions say they are spending less than \$50,000 annually. This figure may be understated because only about one-third of credit unions tie their budget to a business impact analysis, and many say that they do not budget business continuity separately from other costs.

- Smaller credit unions (less than \$250M) are typically spending less than \$25,000 annually. Larger credit unions are spending a significantly higher amount of money, with about half spending more than \$100,000.

***Restoration time is a critical issue for developing back-up systems and appropriate staffing.***

- While most of the credit unions (94%) have back-up operations for member service in place, only two-thirds have full data redundancy and real-time replication of transaction systems in place. Credit unions are often so focused on their transaction processing or core system, that they may overlook the full back-up operations required to maintain business as usual. However, the majority of credit unions plan to make further investments to these technologies during 2010 or 2011.
- The recovery time objective measures how quickly your credit union can put critical systems back online, while the recovery point objective measures how far back the credit union will have to go to restore data. Credit unions need to balance these two measures with cost and member service needs to arrive at an appropriate objective.
- Credit unions have very different objectives for these two metrics. On average, the majority of credit unions have recovery time objectives of less than five hours. No credit unions say they have an RTO of no loss.
- By asset size, credit unions with over \$1B in assets have the least tolerance, with the majority having an RTO of less than 60 minutes. But many of the smallest credit unions (39% of those under \$100M) cite an RTO of less than 60 minutes as well, perhaps because they are outsourcing these services.
- The majority of credit unions have a fairly stringent recovery point objective, with 31% tolerating no loss, and 19% requiring a loss of less than 15 minutes. However, as seen with RTOs, some credit unions tolerate a wider loss, with 27% between 10 and 28 hours.
- RPOs vary widely across asset sizes, following a similar patterns as RTOs. The largest credit unions tolerate less loss of data. Credit unions over \$1B in assets tolerate no loss (52%) or a loss of less than 15 minutes (29%). One third of the smallest credit unions (<\$100M in assets) tolerate no loss. A significant number of credit unions with assets between \$101M and \$500M report RPOs of 10 to 48 hours.

***Security and fraud protection continue to be a focus due to ongoing threats and regulatory requirements***

- The majority of credit unions are conducting penetration testing (91%) and have layered security infrastructure installations in place (81%). Three-fourths of credit unions report having outsourced firewall/IDS/IPS management or monitoring in place. Almost two-thirds of credit unions report using automated fraud/compliance monitoring tools (65%).
- Credit unions who are not currently outsourcing their firewall/IDS/IPS management and monitoring are not planning to do so in the future.
- Smaller credit unions are far less likely to have automated fraud/compliance monitoring systems in place, with less than half of them saying they already have them in place. Virtually all of the credit unions with more than \$1B in assets (95%) have these tools in place.

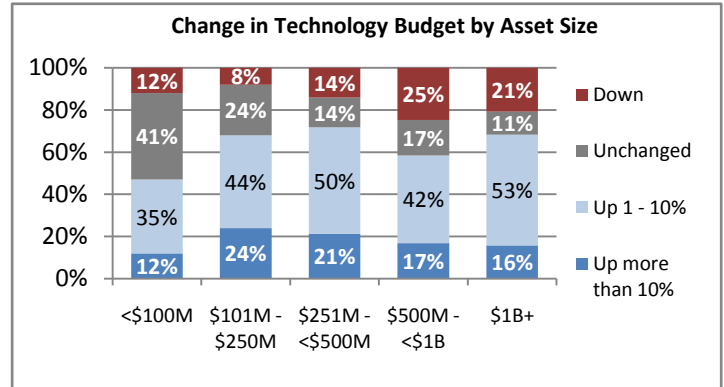
## Technology Budgeting

### 2010 Technology Budgets Are Increasing

The majority of credit unions (63%) say their technology budget has increased in 2010. Overall, 22% of credit unions say that their budget will remain the same, with 15% reporting a decline. This represents a change from the 2009 survey, when more than a quarter of respondents reported a decreased technology budget (28%).

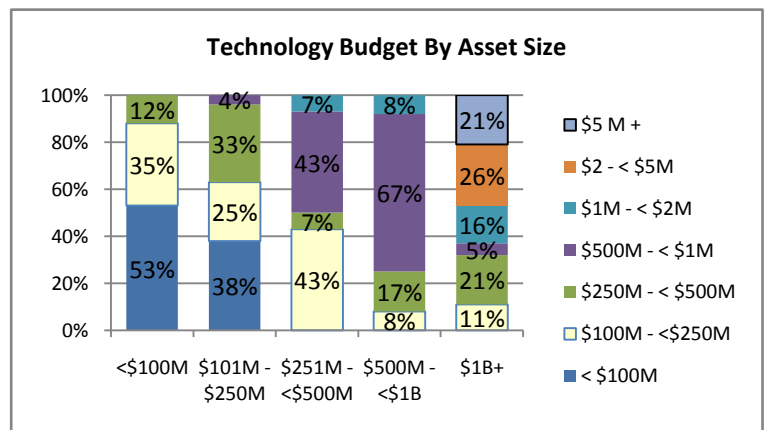
While credit unions across all asset sizes are reporting increases in their budgets, more of the smaller credit unions (<\$250M) reported that their 2010 technology budget had remained the same as 2009.

Larger credit unions overall are typically reporting an increased technology budget, but one-fourth to one-fifth are reporting decreased budgets, which is higher than other asset groups.



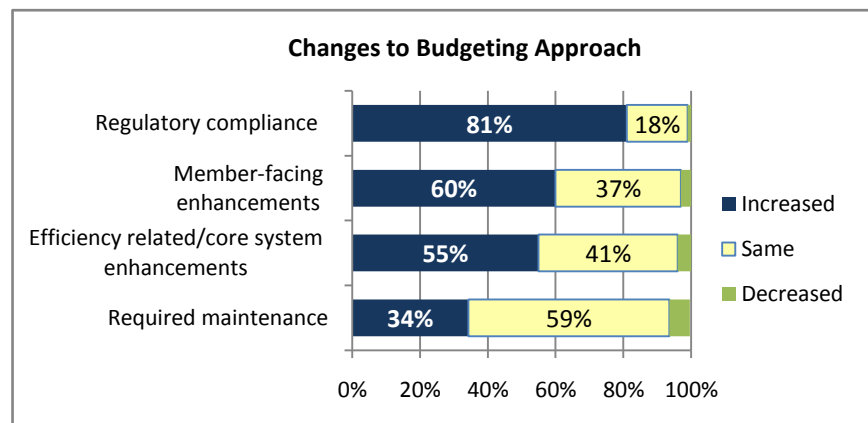
### Spending Increases for Compliance, Member Enhancements

The survey also investigated how the components of technology spending are changing, including regulatory compliance, member-facing enhancements, efficiency-related/core system enhancements, and required maintenance. One reason that many credit unions are increasing their technology budgets is due to regulatory compliance. New and existing federal regulations are placing a greater burden on credit union operations.



Despite the difficult operating environment, credit unions are investing in member-facing enhancements, particularly those that help them target new segments, and streamline their ability to meet member needs. The majority of credit unions across all asset sizes have increased their spending for member-facing enhancements, although the types of projects vary.

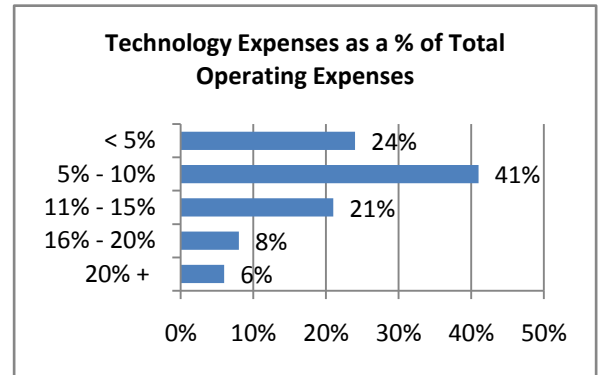
Credit unions are typically spending the same amount on required maintenance as years past.



**Technology Accounts for Small Percentage of Operating Expenses**

Technology expenses typically account for 5% to 10% of operating expenses (41%). This measure is not influenced by asset size, as credit unions of all sizes are included in each category. About one-fourth of credit unions say that their technology expenses are less than 5% of operating expenses. Few credit unions say their technology-related expenses are more than 20% of operating expenses.

Half of the credit unions have technology budgets under \$250,000. Less than one-fifth report technology budgets higher than \$1 million.

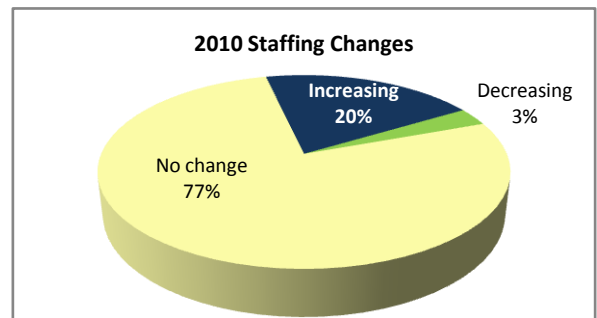


Asset size is one of many factors impacting credit union technology budgets. Credit unions in the \$1B+ asset group have the greatest variation in technology budgets, ranging from \$100M to more than \$5M.

**IT Staffing Expected to Remain Constant**

One key component in IT budgets is staffing. While the majority of credit unions do not expect to add IT staff this year, few are planning to decrease their staff. Among the credit unions planning to add any staff, they are only adding one or two. Credit unions over \$250M in assets are more likely to be adding IT staff than smaller credit unions.

In line with budgets and capabilities, the number of IT staff is correlated to size of budget and asset size. Credit unions with less than \$100M in assets typically have one or two full-time equivalent employees in their IT/e-commerce departments.

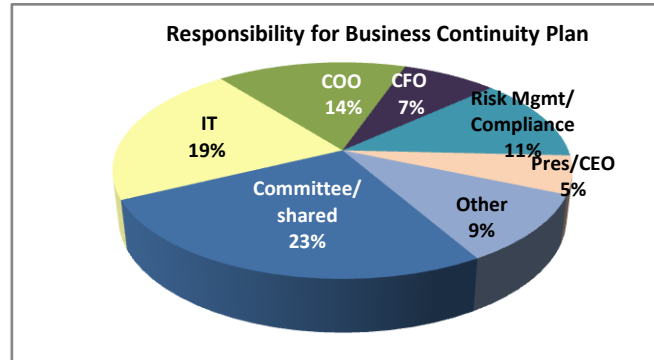


Half of the credit unions over \$1B in assets report having more than 16 FTEs.

	Number of IT FTEs by Asset Size					
	Total	<\$100M	\$101M - 250M	\$251M - \$500M	\$500M - <\$1B	\$1B+
<b>0</b>	9%	17%	20%	0%	0%	0%
<b>1</b>	13%	56%	8%	0%	0%	0%
<b>2</b>	7%	22%	12%	0%	0%	0%
<b>3 - 5</b>	24%	6%	56%	33%	13%	5%
<b>6 - 10</b>	24%	0%	4%	67%	53%	19%
<b>11 - 15</b>	5%	0%	0%	0%	13%	14%
<b>16 - 20</b>	7%	0%	0%	0%	20%	19%
<b>21 - 25</b>	2%	0%	0%	0%	0%	10%
<b>26 - 30</b>	3%	0%	0%	0%	0%	14%
<b>31-35</b>	1%	0%	0%	0%	0%	5%
<b>&gt;35</b>	3%	0%	0%	0%	0%	14%

**Business Continuity Planning Section**

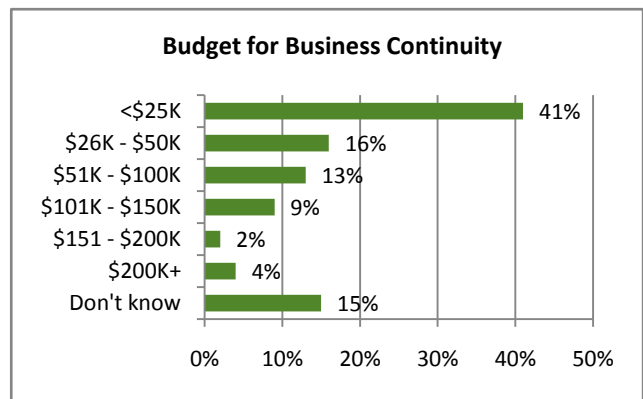
The person with responsibility for business continuity at the credit union varies, with no single functional area mentioned by a majority of respondents. About one-third of credit unions place responsibility with the IT department, including the CTO, VP IT or an IT manager. For about one-fourth of credit unions, a committee has responsibility. Other positions with responsibility include operations related staff such as a COO (11%) or Operations VP (3%). Few credit unions report having a VP or other senior level risk management personnel in charge. The CEO/President typically has responsibility only at the smallest credit unions.



***Business Continuity Spending Varies by Asset Size***

Spending on business continuity varies by asset size, but the majority of credit unions say they are spending less than \$50,000 annually. Smaller credit unions (less than \$250M) are typically spending less than \$25,000 annually. Almost one-fourth of respondents weren't sure how much they were spending on business continuity. This is because they typically are not budgeting for business continuity as a separate line item.

Larger credit unions are spending a significantly higher amount of money, with about half spending more than \$100,000. The few who report spending less than \$50,000 usually noted that they do not budget separately for business continuity, which may mean that they are underestimating their costs.



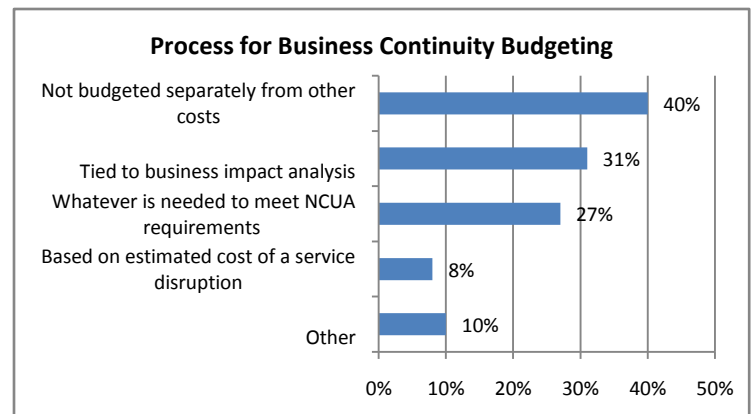
	Annual Budget for Business Continuity by Asset Size				
	<\$100M	\$101M - \$250M	\$251M - <\$500M	\$500M - <\$1B	\$1B+
<\$25K	72%	60%	47%	14%	5%
\$26K - \$50K	0%	28%	27%	0%	19%
\$51K - \$100K	0%	8%	7%	43%	14%
\$101K - \$150K	6%	0%	7%	14%	19%
\$151 - \$200K	0%	0%	0%	0%	10%
\$200K+	0%	0%	0%	0%	19%
Don't know	22%	4%	13%	29%	14%

## Most Credit Unions Are Not Doing Budgeting based on a Business Impact Analysis

About one-third of credit unions tie their business continuity budget to a business impact analysis, but many say that they do not budget business continuity separately from other costs. Few credit unions (8%) say their budget is related to the estimated cost of a service disruption. This may indicate that the credit unions are not conducting a business impact analysis or not quantifying the potential financial impact of a service disruption. Business continuity experts generally recommend analyzing both the financial impact and overall business risks as a first step in developing a complete business continuity plan.

Other ways that credit unions say they determine costs include:

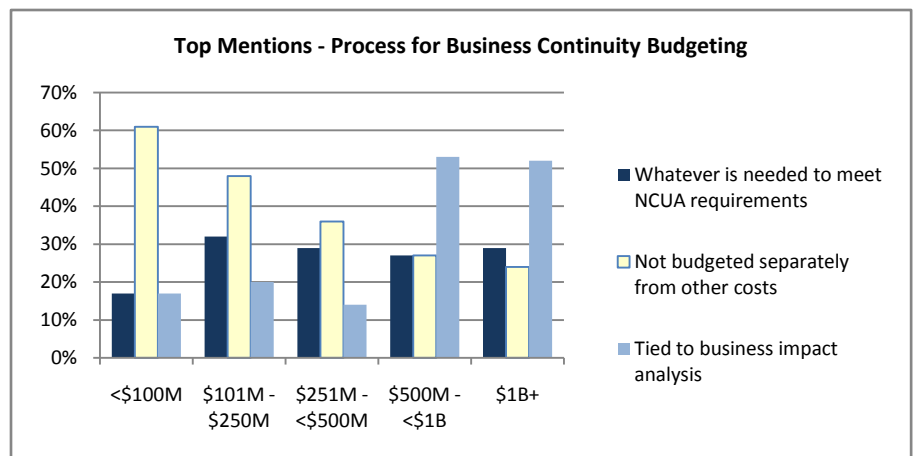
- Meet Board expectations
- Whatever is needed to provide strong security
- Some items are budgeted separately i.e. redundant site
- Separate budget based on business need and risk tolerance levels
- Failover/Redundant Systems and hot site recovery expenses
- Paying for existing backup systems, maintenance, BCP software, etc
- Based on cost of redundancy for systems required in case of DR.



Smaller credit unions are most likely to say that business continuity is not budgeted separately from other costs, with less than one-fourth tying it to business impact analysis. Credit unions with more than \$500M in assets rely on a business impact analysis, although close to a third say they budget whatever is needed to meet the NCUA requirements. A formal business impact analysis can help credit unions understand if they have considered all potential impacts should a problem occur.

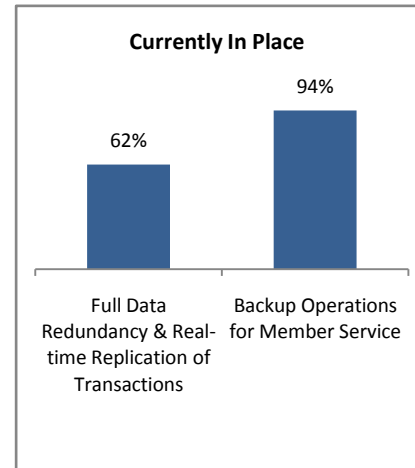
The NCUA recommends completing a business impact analysis to assess risk, including the following aspects:

- ✓ The critical system or service;
- ✓ Type of failure events;
- ✓ Minimum acceptable service levels or system output;
- ✓ The probability of occurrence;
- ✓ The probable timing of the occurrence; and
- ✓ The cost, duration, and impact of each failure.



**Business Continuity: Back-up Operations**

While most of the credit unions (94%) have back-up operations for member service in place, only two-thirds have full data redundancy and real-time replication of transaction systems in place. Credit unions are often so focused on their transaction processing or core system, that they may overlook the full back-up operations required to maintain business as usual. Phone systems, email, online banking and other key member touch points should also be addressed in any back-up or recovery planning.

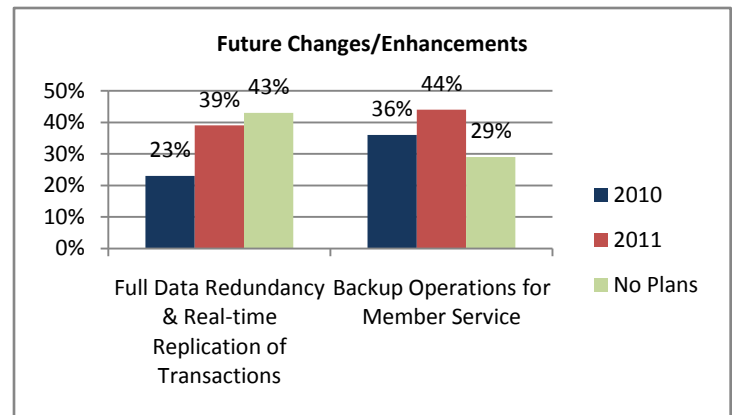


The majority of credit unions plan to make further investments to these technologies during 2010 or 2011. More credit unions are planning to make changes or enhancements to these services in 2011 rather than this year.

More credit unions with \$1B in assets have full data redundancy in place (73%) than credit unions of smaller asset sizes. Only about half to two-thirds of the smaller credit unions have this capability.

Asset size is not a factor for back-up operations for member service, as the majority of credit unions across all asset sizes have back up operations in place.

Credit unions who do not have these systems in place now are typically planning to put them in place in 2011.

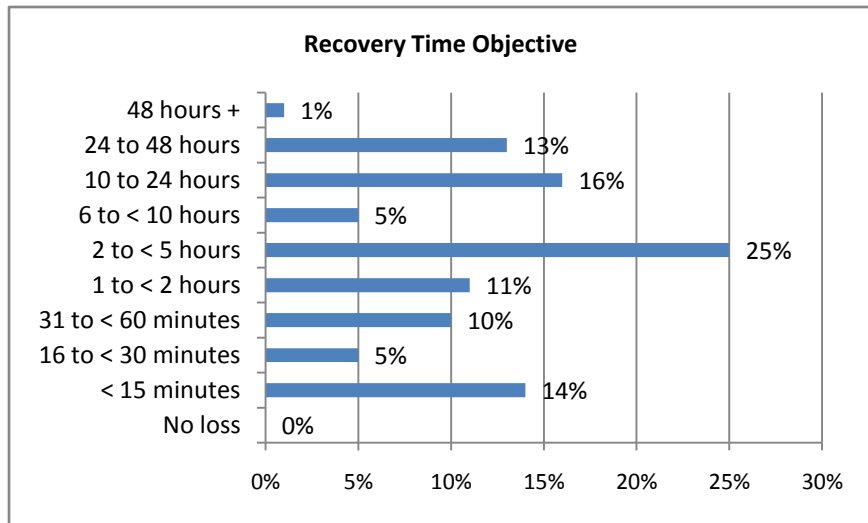


		<\$100M	\$101M - \$250M	\$251M - <\$500M	\$500M - <\$1B	\$1B+
<b>Backup Operations for Member Service</b>						
	<b>In Place</b>	89%	88%	100%	93%	100%
<b>Future Plans</b>	2010	29%	25%	43%	20%	60%
	2011	14%	50%	29%	80%	50%
	No Plans	57%	31%	29%	20%	10%
<b>Full Data Redundancy/Real-time Replication of Transactions</b>						
	<b>In Place</b>	61%	64%	57%	50%	73%
<b>Future Plans</b>	2010	17%	12%	20%	13%	50%
	2011	42%	47%	20%	38%	43%
	No Plans	42%	47%	60%	50%	21%

## Recovery Time Objectives

Restoration time is a critical issue for developing back-up systems and appropriate staffing. The recovery time objective measures how quickly your credit union can put critical systems back online, while the recovery point objective measures how far back the credit union will have to go to restore data. Credit unions need to balance these two measures with cost and member service needs to arrive at an appropriate objective.

Credit unions have very different objectives for these two metrics. On average, the majority of credit unions have recovery time objectives of less than five hours. No credit unions say they have an RTO of no loss.



By asset size, credit unions with over \$1B in assets have the least tolerance, with the majority having an RTO of less than 60 minutes. But many of the smallest credit unions (39% of those under \$100M) cite an RTO of less than 60 minutes as well, perhaps because they are outsourcing these services.

Credit unions with \$251M to \$500M in assets have the highest RTOs, with 50% citing times greater than 10 hours.

RTO By Asset Size					
	<\$100M	\$101M - \$250M	\$251M - <\$500M	\$500M - <\$1B	\$1B+
< 30 minutes	17%	8%	7%	20%	43%
31 to < 60 min	22%	0%	7%	7%	14%
1 to < 2 hours	6%	4%	7%	13%	24%
2 to < 5 hours	11%	36%	21%	40%	14%
6 to < 10 hours	6%	12%	7%	0%	0%
10 to 24 hours	28%	16%	29%	13%	0%
24 +	11%	24%	21%	7%	5%

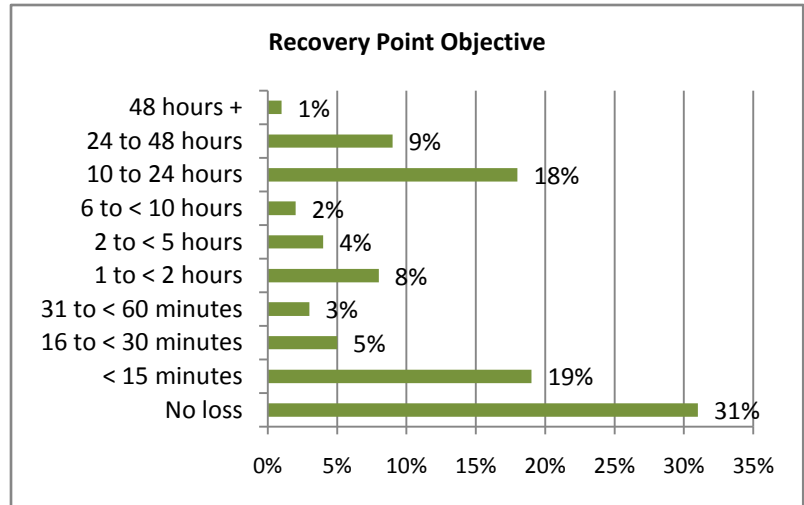
## Recovery Point Objectives

The majority of credit unions have a fairly stringent recovery point objective, with 31% tolerating no loss, and 19% requiring a loss of less than 15 minutes. However, as seen with RTOs, some credit unions tolerate a wider loss, with 27% between 10 and 28 hours.

RPOs vary widely across asset sizes, following a similar patterns as RTOs. The largest credit unions tolerate less loss of data.

Credit unions over \$1B in assets tolerate no loss (52%) or a loss of less than 15 minutes (29%).

One third of the smallest credit unions (<\$100M in assets) tolerate no loss.



A significant number of credit unions with assets between \$101M and \$500M report RPOs of 10 to 48 hours.

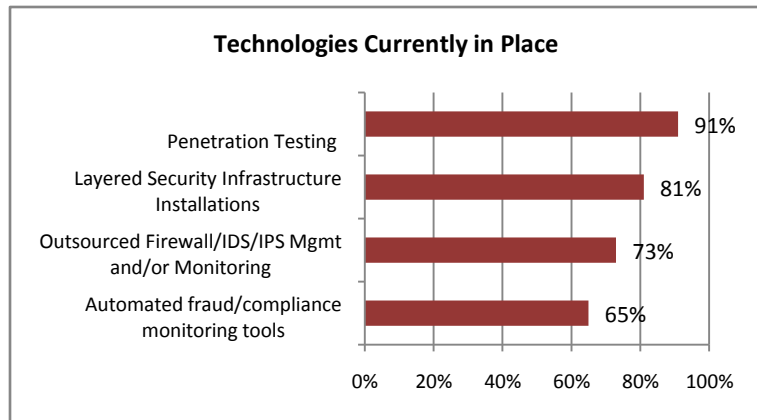
Although credit unions' technology and business continuity expenditures and planning vary by asset size, both continue to remain important areas of focus for credit unions.

RPO by Asset Size					
	<\$100M	\$101M - \$250M	\$251M - <\$500M	\$500M - <\$1B	\$1B+
No loss	35%	12%	29%	29%	52%
< 15 minutes	6%	20%	7%	29%	29%
16 to < 30 minutes	0%	8%	7%	0%	10%
31 to < 60 minutes	6%	0%	0%	14%	0%
1 to < 2 hours	18%	12%	0%	7%	0%
2 to < 5 hours	12%	4%	7%	0%	0%
6 to < 10 hours	6%	0%	7%	0%	0%
10 to 24 hours	18%	32%	21%	14%	0%
24 to 48 hours	0%	12%	21%	7%	5%
48 hours +	0%	0%	0%	0%	5%

**Continued Investments in IT Security – Related Technologies**

As security and fraud protection continue to be a focus due to ongoing threats and regulatory requirements, the majority of credit unions are conducting penetration testing and have layered security infrastructure installations in place. Three-fourths of credit unions report having outsourced firewall/IDS/IPS management or monitoring in place. Almost two-thirds of credit unions report using automated fraud/compliance monitoring tools.

- Half of the credit unions who are not currently doing penetration testing expect to do so in 2011.
- Credit unions who are not currently outsourcing their firewall/IDS/IPS management and monitoring are not planning to do so in the future.



	2010	2011	No Plans
<b>Automated fraud/compliance monitoring tools</b>	23%	28%	56%
<b>Outsourced Firewall/IDS/IPS Mgmt and/or Monitoring</b>	8%	8%	86%
<b>Layered Security Infrastructure Installations</b>	11%	32%	61%
<b>Penetration Testing</b>	27%	27%	52%

**Systems in Place Vary Greatly by Asset Size**

Smaller credit unions are far less likely to have automated fraud/compliance monitoring systems in place, with less than half of them saying they already have them in place. Virtually all of the credit unions with more than \$1B in assets (95%) have these tools in place.

<b>Systems in Place by Asset Size</b>					
	<\$100M	\$101M - \$250M	\$251M - <\$500M	\$500M - <\$1B	\$1B+
<b>Automated fraud/compliance monitoring tools</b>	44%	33%	80%	79%	95%
<b>Outsourced Firewall/IDS/IPS Mgmt and/or Monitoring</b>	78%	71%	71%	86%	62%
<b>Layered Security Infrastructure Installations</b>	67%	68%	86%	86%	100%
<b>Penetration Testing</b>	72%	92%	100%	93%	100%

***About the Business Continuity Section Sponsor: Ongoing Operations***

Ongoing Operations is the leading provider of business continuity & disaster recovery solutions to credit unions nationwide, protecting over 21.5% of industry assets. The CUSO takes a holistic approach to business continuity to ensure that all your critical systems and member touchpoints stay up and running – no matter what.

Ongoing Operations' certified business continuity planners recommend that credit unions begin their planning process by conducting a Business Impact Analysis (BIA). For more information or to download a free, customized Financial Impact Analysis (FIA) for your credit union, visit [www.ongoingoperations.com](http://www.ongoingoperations.com).