

**Brief History:**

In the last four decades, First American CREDCO has been extraordinarily successful in delivering consolidated credit information to lenders by the fastest and safest means available. First American CREDCO processes millions of credit reports annually across a broad clientele base. The company was the first to provide merged credit data to the mortgage lending industry, and is the first preferred provider to Fannie Mae and Freddie Mac. First American CREDCO provides one of every three reports used by mortgage professionals. The company is also the leading provider of specialized credit reports to the automotive industry. The success of First American CREDCO stems from the company's mission, vision, and values.

Mission Statement:

To provide specialized credit reports for consumers, such as mortgage lending industry, mortgage professionals, and the automotive industry, through the fastest and safest means available.

Vision Statement:

First American CREDCO will gain instant partner credibility and will validate and certify its security posture to conduct business online with the world's largest credit reporting organization and will keep partners.

Values Statement:**Constant Need for Improvement:**

Constantly investigating and testing new ways to streamline and automate the information delivery process.

Dedication to Securing the Information for the Customer

Always thinking about keeping the partners and the customers happy; decreasing their costs and ensuring efficient delivery of information.

Prioritizing Security

Establishing firewall software and intrusion detection systems in protect the core servers that support daily transactions via CREDCO's network.

Commitment to Excellence and Self-Improvement

Auditing existing systems to find vital components that are need in CREDCO's security defense.



SECS DLC:

Investigation:

1. Specify process, outcomes, goals of First American CREDCO
2. Define Budget and other constraints
 - a. How much do we have to spend?
 - b. What other controls/constraints are we facing?
3. Analyze problems, define their scope, and specify goals and objectives.

Analysis:

4. Study documents from implementation phase
5. Conduct preliminary analysis of existing security policies or programs
 - a. What is the current security policy?
 - b. What does the current security policy contain?
 - c. What security programs do we have right now?
6. Conduct preliminary analysis of threats and associated controls
7. Analyze relevant legal issues that affect design of the security solution.
 - a. Privacy laws
 - b. Regulations
8. Risk Management
 - a. Identify risk
 - i. Acts of Human Error or Failure
 - ii. Compromises to Intellectual Property
 - iii. Deliberate Acts of Espionage or Trespass
 - iv. Deliberate Acts of Information Extortion
 - v. Deliberate Acts of Sabotage or Vandalism
 - vi. Deliberate Acts of Theft
 - vii. Deliberate Software Attacks
 - viii. Deviation in Quality of Service by Service Providers
 - ix. Forces of Nature
 - x. Technical Hardware Failures or Errors
 - xi. Technical Software Failures or Errors
 - xii. Technological Obsolescence
 - b. Assess and evaluate the levels of risk facing the organization (specifically security threats)

Logical Design:

9. Create blueprint for security
10. Implement key policies
11. Create critical contingency plans for incident response
12. Conduct Feasibility analysis
 - a. Should we outsource or keep it in house?

Physical Design:

13. Evaluate technology needed to support the security blueprint
14. Generate alternative solutions
15. Agree on final design.



16. Develop criteria for successful solutions
17. Review the project with interested parties for their approval or disapproval.

Implementation:

18. Acquire security solutions, test them, implement and re-test.
19. Conduct specific training and education programs
20. Evaluate Personnel issues
21. Present entire package to upper management for final approval.
22. Management of the project plan
 - a. Execute the project plan
 - i. Planning the project
 - ii. Supervising the tasks and action steps within the project plan
 - iii. Wrapping up the project plan

Maintenance:

23. Monitor
 - a. Continuously keep an eye on the security program
24. Test
 - a. Continue testing to make sure everything works as it was intended to.
25. Modify
 - a. Make changes if necessary
26. Update
 - a. New threats emerge and old threats evolve.
27. Repair



Contingency Planning:

Since First American CREDCO provides confidential credit information, there is a greater need for contingency planning. Any potential threats to the security of the First American CREDCO's data may lead to catastrophic disaster. In anticipation of this, First American CREDCO should have in place an incident response plan, and disaster recovery plan, and a business continuity plan effectively prepare for, react to, and recover from events that threaten information assets and resources.

Incident Response Plan:

In the Incident Response Planning, First American CREDCO will create a detailed set of processes and procedures that anticipate, detect, and mitigate the effects of an unexpected event that might compromise information resources and tasks. There should be three categories of plans created:

1. Before an attack
2. After an attack
3. During an attack

These plans will serve as procedures and guidelines for the entire organization; to keep everyone fully aware of what needs to be done to prevent an incident, to deal with it when it occurs, and how to recover from it.

In addition, there needs to be an alert roster, a document containing contact information on the individuals to be notified in the event of an actual incident, available in every department of First American CREDCO.

All the other components of IRP, such as alert message board or documenting the incident, occur after an incident has been detected and are listed on the "After an Attack" or "During an Attack" plan mentioned earlier.

Disaster Recovery Plan:

Disaster Recovery Plan is very important because it contains the plan for reestablishing operations at the location where the organization is usually located in the event of a disaster.

For First American CREDCO, the CP team must classify disasters, so that if an unexpected event does occur, it can quickly be identified as either an incident or a disaster. Having a list-type source that classifies disasters, can help make the



reestablishment of operations at the primary site more smooth due to the fact that the CP can react faster if the type of the unexpected event is quickly identifiable; the CP team will know which plan to use, the IRP or the DRP, in a much faster time span.

In addition, the CP team at First American CREDCO should engage in scenario development and impact analysis, along the way categorizing the level of threat that each disaster poses. In scenario development, important questions, such as, “do we have appropriate resources to carry out our DRP plans?” need to be asked and analyzed.

Finally, the DRP should be tested regularly to make sure that it is feasible and does what it was intended to do.

Business Recovery Plan:

The Business recovery plan is activated at the same time the DRP is, but it is activated to reestablish the critical business functions of the business in the case of a disaster. First American CREDCO needs to choose a continuity strategy, such as hot site, warm site, or cold site. In determining the strategy, it needs to do a budget analysis to see which one of the strategies it can afford, as some are more expensive than others, i.e. hot site is the most expensive. This strategy needs to be tested as well, to make sure that it is fully attainable.