VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

SPACE EXPLORATION AGENCIES DISASTER AND THEIR RECOVERY

B.Tech in Computer Science and Engineering **(CSE)**, Fall-Semester **2021-22**

DISASTER RECOVERY AND BUSINESS CONTINUITY MANAGEMENT

J-COMPONENT REVIEW 2

TEAM MEMBERS:

ADYA SHARMA 18BCI0219

RIYAZ MOHAMMAD ARBAZ 20BDS0274

BANDI HARSHAVARDHAN REDDY 2OBCE2265

Under the Guidance of

Prof. Swarnalatha P

AIM

Over the years, a lot of projects have been implemented on space exploration. While the ones that succeed bring in a lot of valuable information, the ones that don't cause a lot of loss in terms of finance, manpower, authority etc. This project will focus on such topics. We aim to study limited to any one particular agency and will try to cover multiple major ones such as SpaceX, NASA etc. different disasters caused at space exploration agencies and how recovery can be made. To do the same we would be studying the projects launched, the success, the failures, cause of such failures, what kind of disasters they brought and how it can be overcome. We would not be

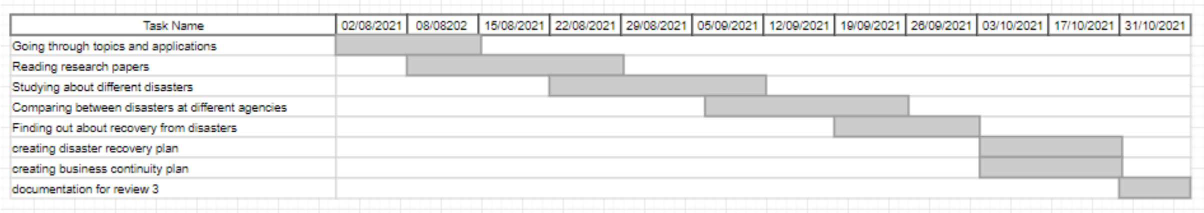
ABSTRACT

With advancement in technology, humanity has expanded its horizon in every field of research. Space research has seen a major impact of this as multiple space exploration agencies like NASA, Spacex, ISRO have discovered a lot. Every year multiple expensive space missions are launched. Anything from something as tiny as a data overflow to something as huge as hole in the rocket can cause a massive disaster. It costs Billions of dollars ,years of research and a lot of crew work to launch one mission. It often happens that these missions are unsuccessful due to some disaster. all the resources that go into these projects then become a waste as the desired output is not obtained. In this project we aim to study the different kinds of disasters that take place during the execution of above mentioned missions and how recovery from these disasters are followed. We can also come up with a disaster recovery plan which can help avoid future disasters.

OBJECTIVE

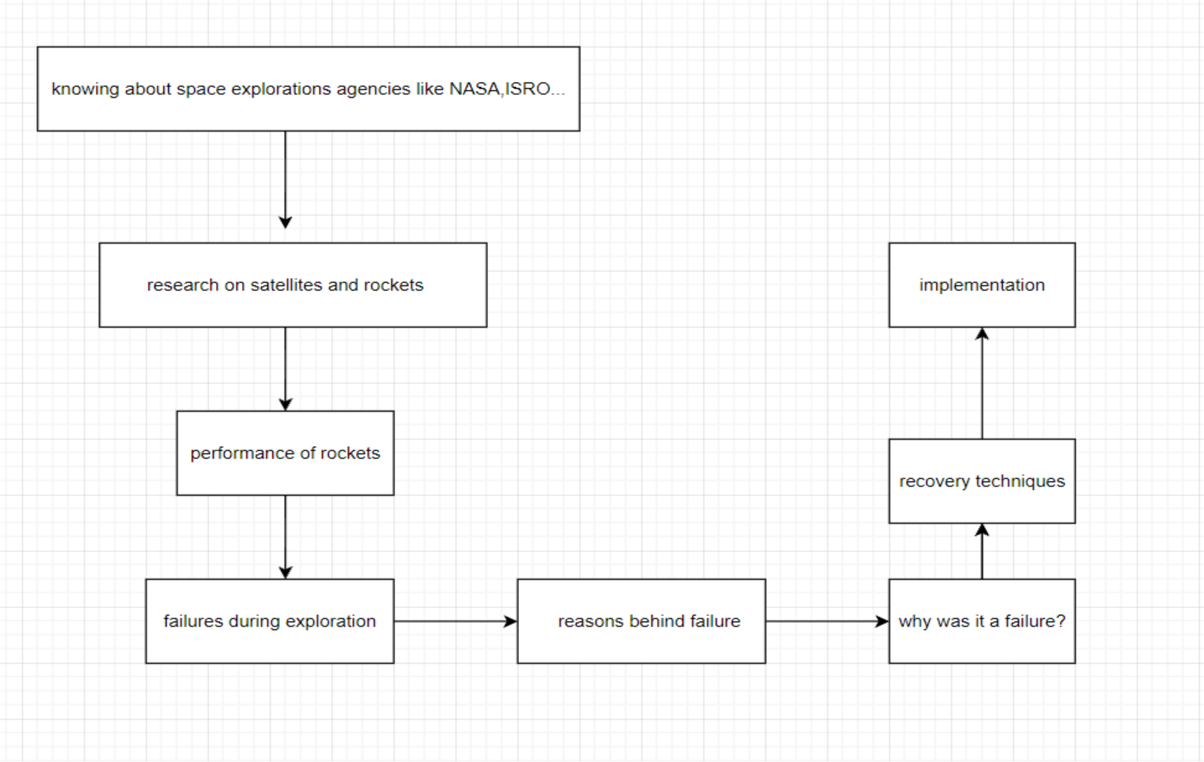
There are many space exploration agencies which have been competing with each other and elaborating their explorations. There may be many people working in each agency and many efforts but still there will be failures meanwhile they will work on the failures to come up with better solutions with enhancing technologies. So here, in this project we are going to work on the failures and know where the problem occurs so that we can overcome those failures and implement it in a better way. Keeping in mind the disaster recovery plans and business continuity plans, the objective of the project would be to find out about different types of disasters happening at space exploration agencies and how to recover from these disasters. Right from protection of the crew to the protection of resources and environment would be kept in mind. Comparison between space stations, Major and minor mistakes done by the space station which caused mass disasters, Recovery points which can fix the destruction caused by those space stations would be the main point of focus. In the end we could come with disaster recovery and business continuity plans and would focus on things that are not already included.

SCHEDULE DIAGRAM



Task Name	02/08/2021	08/08202	15/08/2021	22/08/2021	29/08/2021	05/09/2021	12/09/2021	19/09/2021	26/09/2021	03/10/2021	17/10/2021	31/10/2021
Going through topics and applications	▨	▨										
Reading research papers		▨	▨	▨								
Studying about different disasters				▨	▨	▨						
Comparing between disasters at different agencies						▨	▨	▨				
Finding out about recovery from disasters								▨	▨			
creating disaster recovery plan										▨	▨	
creating business continuity plan										▨	▨	
documentation for review 3												▨

BLOCK DIAGRAM


knowing about space explorations agencies like NASA,ISRO...
research on satellites and rockets
performance of rockets
failures during exploration
reasons behind failure
why was it a failure?
recovery techniques
implementation

1. DRBCP

1.1 Phases of DRP and BCP:

Phases of DRP:

To facilitate any project there are five phases to disaster recovery planning

Phase 1: Disaster assessment and risk analysis

In this phase the main focus is assessing the extent of damage done and further the amount of damage that could be caused if a disaster recovery plan is not followed immediately. The disaster recovery plan must mention the team members who will be responsible for identifying, notifying and accounting the damage. This usually includes finding out the origin of the problem, likelihood and extent of further damage and chief areas that could have been affected. Apart from this if any damage has been done to any equipment, resources, inventory or finished products also has to be identified. This also includes checking things that need to be replaced. We also need to gather other critical information and check the estimated time available for dealing with the disaster without hampering the progress of the project if possible. Carrying out a detailed risk analysis is also important in the first phase. For example in case of a rocket explosion at the time of launch the officials would have to check what all equipment they should salvage, if anything else is damaged or not etc.

Phase 2: Activation and Planning

In this phase a team is brought forward who will actively participate in planning and executing the disaster recovery solution. The role of each and every member has to be clearly defined. Some of the important aspects of planning are listing the items that are to be restored and also assigning priority to these items. All the procedures are to be detailed and assigned to team members. A communication, review and report system is to be set up as well as time lines and schedules for activities to be performed. All the resources and equipment are to be allocated. Quality and operating standards are to be set up. All the data sources are identified and imported. Then the recovery plan is documented.

Phase 3:Execution of the disaster recovery Plan

In the execution phase, the recovery team finally gets into action and begins executing the recovery activities as per the procedures specified in the plan. At the end of each phase of the recovery, or after execution of the important recovery activities, a review or appraisal must follow to monitor the progress and ensure compliance with the established quality standards.

Phase 4: Integrating the Disaster Recovery Plan with the Project Plan

Disaster recovery is not something that is carried out completely in isolation. Thus, in this phase, efforts are made to integrate the disaster plan with the overall project plan. This phase also involves testing and verifying the disaster recovery plan for its feasibility. This integration will ensure optimum usage of resources and concentrated efforts toward the overall objective of the project.

Phase 5: Reconstitution and Restoration

This final phase of the five phases in a disaster recovery plan follows after the disaster has been completely managed and it is time to get back to restoring normalcy. Once the execution and testing of the recovery plan is over, this reconstitution phase begins and may last even for a few weeks. The resources and team members that were diverted toward the disaster recovery must be moved back to their original places. In this we would need to ensure that there are no remaining aftereffects of the disaster and that no threats have remained unaddressed. Also need to see that all team members have returned to their original roles and all resources deployed for the recovery have been secured and relocated to where they are needed.

Phases of BCP:

Phase 1: Initiation

Pull together a team of people who are aware of the different operational aspects of your business to evaluate what potential events create the greatest threats to your organization. Here in Florida, it is easy to fall into thinking of disasters as natural events like a hurricane or flood; But hazards also include technological events such as cyber-attack, utility outage, or a fire.

Phase 2: Business Impact Analysis (BIA)

BIA is a systematic process of gathering and analyzing information about critical business functions to determine the most important elements of your business with the greatest risk potential. Don't waste time or resources if there is little or no impact on business operations. Remember that key employees and management succession are important subjects of a BCP (Does your business have a policy that prevents key employees from traveling together? What happens if a key leader is incapacitated and not able to respond in the event of a disaster?).

The essential part of the BIA phase is that you ask the right questions. Creating a BCP may seem overwhelming, but there are a number of tools available to assist in the process. Find a good checklist and use it. BKS-Partners has created a comprehensive hurricane preparedness website where you can find resources and other tools to help you with this process.

Phase 3: Develop Recovery Strategies

Communication is key during and after a disaster. In an effective BCP, people come first. It is essential to have a functional means of communication with employees, vendors, and customers.

Determine the business impact of a function or process first, and then develop recovery capability for it. Your objective in this phase is to identify the people, facilities, and assets that are required to achieve the four "R's" which are: Response, Resumption, Recovery, and Restoration.

Phase 4: Implementation

An effective BCP must be written and communicated to all employees on an ongoing basis.

Phase 5: Test and Monitor

Risk is not static. Personnel changes, potential threats, and critical business functions will change over time. A BCP must be validated through testing or practical application and must be kept up-to-date.

1.2 Functional Area

The three phases of the disaster recovery functional area include recovery, restoration, and transferring data back to the production machines. Exactly when catastrophe strikes, you really expected to absolutely recuperate as quickly as could be anticipated. Go through these on various occasions of catastrophe recovery.

In our Business Continuity and Disaster Recovery sorting out, we contribute a great deal of our energy researching, revealing and making frameworks for when an event may occur. This is all to get ready for or prevent a power outage. Then, at that point, we'll design each stage, and how to work inside them with the objective that your business can forge ahead from an event

Recovery:

Once the infrastructure is in place, it will be necessary to recover production data.

Since recovery may not be up to the point of failure, it is important to identify any processing that needs to be redone. We need to know if all the data fed to the system can be identified and how many of them can be redone with 100% certainty of success. It is important to identify holes in data and then to identify the action to be taken when data inconsistencies are detected. An audit trail should be conducted for all work performed during this phase.

For example, if the ISO determines that the system must be recovered within 24 hours, measures to meet the requirement and obtain the necessary resources to accomplish the recovery goals must be determined. By prioritizing these recovery strategies, the ISO may make more informed, tailored recommendations regarding contingency resource allocations and expenditures, as well as save time, effort, and cost. Implementing recovery strategies usually requires coordinating with other Agency organizations.

Restoration:

Before beginning the restoration task we need to consider a few things. After review the restoration team is to be provided with orientation on logistics and expectations on following the plan and reporting issues. Our goal would be to ensure organized and disciplined implementation of tasks. Otherwise it may lead to chaos. The team should follow everything from plan and not from memory.

In order to support events requiring the recovery of information systems, the information system backups to recover the system must be stored at an alternate site. Backup frequency should be based on Agency policy, data criticality, and the frequency that new information is introduced. The location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite should be documented in the contingency plan. The specific method selected for conducting backups should be based on system and data availability and integrity requirements. When the data is required for recovery or testing purposes, the organization contacts the storage facility requesting that the specific data be transported to the organization or to an alternate facility.

Transferring data back to production machines:

Eventually production will need to shift from a “hot site” back to a permanent location. A process needs to be defined to manage this migration. Often the client will elect to execute the DRP on the production machines in order to synchronize the machines to a specific point in time.

1.3 Technical Area

A DRBCP should address these main technical area

Hardware issues:

This includes machine type, configuration and operating system version and patch level. Another issue is deciding whether to use an existing pre-configured machine or to completely configure a machine. There are pros and cons to each scenario. Our motive is to plan for the worst case. It may not be possible to reconstruct the production machine on a new machine using a tape backup. This method does not leave very much room for flexibility relative to hardware configuration, but is very fast when compared to a manual system reconstruction.

Networking issues:
It deals with some of the following questions: What part of the Production system must be replicated for the drp? This environment most likely consists of several machines, and there is a good chance that the environment is not homogenous. Is there any special type of LAN or VPN software required? How do the Machines communicate with one another? Do applications connect to machines using hostname for hard coded IP addresses? What other configuration information is required? Are there requirements for connections to an external network? Are there requirements for dial in access? Is there any other type of client/ server or n-tier activity that will need to be supported? All networking requirements are issues that need to be identified, documented, and then addressed in the TRP. What about bandwidth?

If the information system is damaged or destroyed or the primary site is unavailable, necessary hardware and software must be activated or procured quickly and delivered to the alternate location. Three basic strategies exist to prepare for equipment replacement. When selecting the most appropriate strategy, note that the availability of transportation may be limited or temporarily halted in the event of a catastrophic disaster. The three basic strategies are described as follows:

• Vendor Agreements—as the DRP plan is being developed, SLAs for hardware, software, and support vendors may be made for emergency maintenance service. The SLA should specify how quickly the vendor must respond after being notified. The agreement should also give the organization's priority status for the shipment of replacement equipment over equipment being purchased for normal operations. SLAs should further discuss what priority status the organization will receive in the event of a catastrophic disaster involving multiple vendor clients. In such cases, organizations with health- and safety-dependent processes will often receive the highest priority for shipment. The details of these negotiations should be documented in the SLA, which should be maintained with the contingency plan.

- Equipment Inventory—required equipment may be purchased in advance and stored at a secure offsite location, such as an alternate site where recovery operations will take place (i.e., warm or mobile site) or at another location where it will be stored and then shipped to the alternate site. This solution has certain drawbacks since the organization must commit financial resources to purchase this equipment in advance and the equipment could become obsolete or unsuitable for use over time because system technologies and requirements change.
- Existing Compatible Equipment—equipment currently housed and used by the contracted hot site or by another organization within the agency may be used by the organization. Agreements made with hot sites and reciprocal internal sites stipulate that similar and compatible equipment will be available for contingency use by the organization.

2. Disaster Recovery Plan

2.1.Security

Cyber security and era of space activity

Introduction

The Internet is proportional to the space enabled communication and its informative services. Since the 1950s outer space has been a major national security for spacefaring nations. Government established many space programs which lead for intelligence, military, political, and scientific purposes and developed countermeasures estimating space-based threats from rivals, such as anti-satellite capabilities. Many countries were responsible for banning weapons of destruction in space And initiated on peaceful uses of space in 2002 the U.S. general accounting office concluded effort on critical infrastructure protection didn't include satellite industry but that should have been included in the same way cybersecurity was not prioritized by government and private sector space endeavours Analysis noted that cybersecurity discussion is frequently pointing space activities vulnerability to cyberattack. Neither the UN governmental group of experts (GGE) on outer space nor the UN GGE on cyberspace addressed the convergence of their respective agendas.

The United States pointed out that China has been engaged in cyber operations against U.S. satellites. Chinese military writings emphasize the need to target satellites to "blind and deafen the enemy." Space agencies, satellite industries, intergovernmental satellite organizations are collaborating to show increasing awareness of the space cybersecurity challenge.NASA's then chief information security officer, Jeanette Hanna-Ruiz, said "it's a matter of time before someone hacks into something in space."

The attack surface of space activity is going on expanded but government and higher authorities are not taking any adequate actions on the attacks First before protecting space activities, we must have an understanding and overview on particular cyber vulnerabilities that can arise in space stations and in their operations The United States has declared that space is now a warfighting domain States continue to conduct cyber operations that violate international law Taking an example the UN International Telecommunication Union prohibits interference with satellite transmissions, yet such interference frequently occurs.

Putting "space" before "cybersecurity" does not alleviate the geopolitical tensions that already limit cooperation on cyberspace and space. Example The mechanical failure of panamsat galaxy IV satellite 1998 disabled around 90% of the paging network in the united for two to four days. In orbit satellite face major threat from space junk floating on orbit and from bad weather on earth

A list of natural threats to commercial satellite system is noted in table 1

Type of threat	Vulnerable satellite system component
Land based threats Natural diaster Power outage	Ground stations control centers and data links

Space based threat Space environment Space objects (debris)	Satellites control centers and data links
Interference based threats Solar activities such as atmosphere and solar disturbances Unintentional human interference	-

The next following table shows some possible intentional threats that have to be considered

Types of threats	Vulnerable satellite system component
Land based Physical or man made destructions Such as natural disasters and wars	Land stations communications networks and linking errors
Space based Distractions such as space mines and space wars Directed energy weapons	Satellites and control center links
Interference and content oriented Cyber attacks Jamming	Systema and communication networks

Solutions and recommendations for all the threats

Governments all across the world must take the responsibility for the exploration of various security techniques to protect satellite systems from unauthorized use disruption and damages. Example the president of India made a call for an international space force to protect satellites from any war that may take place into space. Satellites system engineers will need to prepare new protective materials that can shield satellites' from atmospheric and other attacks. The space arena needs to establish a proper organization to assure safety, enforce laws, protect the environment and conduct security operations. The organization must have the means to operate as a global space police force to ensure space security.

Commercial satellite companies must also take in considerations of the location and design their satellite earth stations in order to avoid possible damages to natural disasters such as earthquakes, storms and floods. Physical protection is also needed to protect from terrorist attacks. Nations are only looking to dominate space in order to serve their national interest and political gain. It is the responsibility of every citizen to get together for a peaceful effort and seek space as our future arena for scientific and technological exploration to benefit all living beings. Outer space might not be a final frontier for cybersecurity but achieving cyber security beyond earth is one the main responsibility of the new era of space activity of government and society.

2.2. Applications Of Space Technology

Agriculture

Forestry

Energy Sector

Mining Environment

Climatology

Oceanography

Glaciology

Business Sector

Hydro Exploration

2.3.DISASTER RECOVERY PLAN

An unexpected moment and disaster recovery occurred in 1988 when a fire destroyed a central office operated by Illinois Bell in the suburbs of Chicago. The Hinsdale central office handled 40,000 local phone lines, which supported the O'Hare international airport and numerous businesses.

Fuchs(a multinational manufacturer of lubricants) says there are two driving factors when it comes to disaster recovery: interoperability and deploy ability "initially responders need to establish radio networks and then extend their coverage region-wide. VSATs are often used as the backhaul solution for these radio networks," trustComm's Satellite Emergency Operations Network (SEON) solution has been successfully deployed by Harris County, Texas, and other government agencies. They must address questions such as planning for a partial failure or for a catastrophic failure, as well as addressing the need of whether to turn up capacity very quickly without much planning.

Japan was hit by the most powerful earthquake ever recorded in the country. At the moment SKY perfect JSAT's satellite services were used as the country dealt with the aftermath. Flyaway were in action to help coordinate emergency equipment supply and deployed satellite connections to help wireless carrier to restore their data

During ground level threat satellites play a major role by saving the data and transferring the information to people. Large data from far location are sent to people by transfer from person to satellite and satellite to people

2.4.BIA(Business impact analysis)

Space activities, embedded in the larger aerospace domain, can be a noteworthy contributor to an economy. The current supply of space-related statistics contains many gaps. Most of the available input metrics are of low comparability over countries. Most widely available indicators of space activities are the least useful for tracking the development of space economy while most valuable indicators are largely missing except few apps. There is lack of official space related data which need to be calculated for true productivity based on value added per employee from sales of space goods and services

Considering an example, the effect of space on competitiveness is also hard to determine since we would require data on the cost of using a specific space production process or the productivity of specific space products.

The main use of this BIA is to co-relate specific system components with critical conditions and services provided and on the basis of those info we can characterize the consequence of disruption to system components.

2.5 Steps:

To recover from a disaster first we need to establish a program by which all the material and sites damaged by the disasters come to stable and usable states.

Determine the priority for restoration works and get advice and steps from conservators for best methods and options to obtain the best cost of recovery.

Removing and discarding all the items which are not worthy any more and replacing and rebinding the item which lead to a positive conservation treatment.

Cleaning and rehabilitating the damaged site by disaster and contact insurance.

Replacing the treated or recovered materials in rigged out sites.

Analysing the disasters and implementing the plan and improving it in experience.

2.6. Notification And Activation Procedures:

In an immediate emergency or disaster, the main objective of space stations is to preserve the health and safety of their staff before proceeding for notification s and activation procedure

The space station contingency plan coordinator must be the responsibility to initiate notifications using the emergency team. While making notifications we must begin at the beginning of the contact list and continue till the positive contact is made. Space stations contingency plan coordinator takes the responsibility to update the emergency notifications contact

The contingency plan coordinator follows an emergency plan based on the damage occurring and will implement the plan if it is too necessary. It is imperative to the nature of disaster and the implementation will be assessed as quickly as conditions allow.

Activation criteria is unique for each and every organization and it will stated in contingency planning policy statement

- safety of staff and extent of damage to the facility.
- extent of damage in system it can be physical or operational or costed
- criticality of the system to organizations goals

Roles and responsibilities

By activating the plan all the team leaders must be informed with the details of the event and if relocation is necessary.

When the notification is passed from contingency plan activation criteria, the team leader must take the responsibility to inform and lead the whole team and be prepared to respond and face and to relocate if needed.

The CPC is to notify the safe site for storage facility which contingency event has been declared and pointed and shp all the necessary materials to the alternate site.

In that site declared by contingency event all must be prepared to facilitate the organization's arrival.

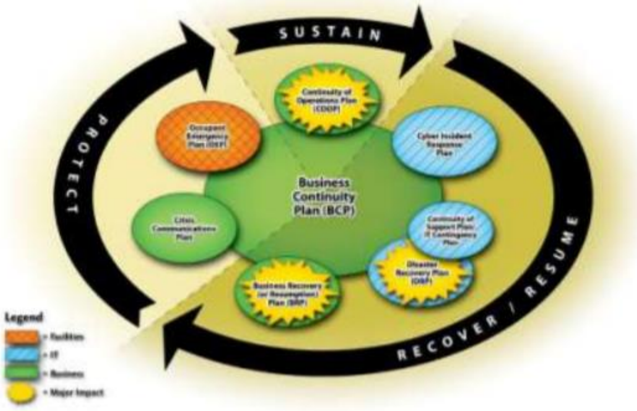
Then finally to notify remaining personnel on the general status of the disaster.

3. Business Continuity Management

3.1 Business Continuity Plan And Strategies

strategies of nasa:

- Expand human knowledge through new scientific discoveries
- Extend human presence deeper into space and to the moon for sustainable long-term exploration and utilization.
- Address national challenges and catalyze economic growth.
- Optimize capabilities and operations.


SUSTAIN
PROTECT
RECOVER / RESUME
Business Continuity Plan (BCP)
Continuity of Operations Plan (COOP)
Occupant Emergency Plan (OEP)
Cyber Incident Response Plan
Crisis Communications Plan
Continuity of Support Plan/ IT Contingency Plan
Disaster Recovery Plan (DRP)
Business Recovery (or Resumption) Plan (BRP)
Legend
= Facilities
= IT
= Business
= Major Impact

Purpose: The main purpose of this plan is that we shouldn't discontinue the plan when some obstacles occur instead we must be ready to face the difficulties.

Overview:

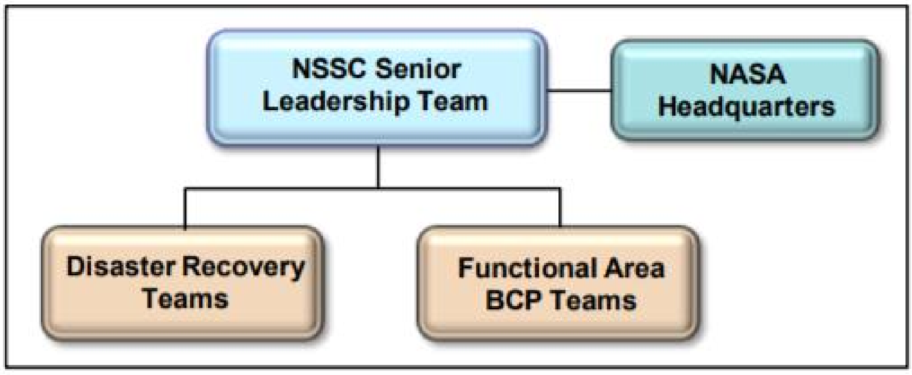
-protection

-Sustainability

-Recovery/resumption of operations

Further, the steps regarding the rescue and other telecommunications contact would be set up by a team and the head of the authority will take care of all the jobs which were distributed such that they are done on time.

- BCP focuses on sustaining an organization's business functions while there is a disaster and even after the disaster during the recovery process.
- The plan that is designed maybe for a particular company or it might address all the companies and help them in making a plan so that it doesn't come to an end after a disaster occurs.
- Sometimes BCP may not address long term recoveries but it will help the company to come out of that intermediate business conflicts.
- In the process of elimination of these conflicts, Continuity Of Operations(COOP) helps in restoring an organization's essential functions at an alternate site such that functions return to normal operations.



3.2 Project Organisation-Implementation

1.DRBCP-Adya Sharma(18BCI0219)
(1.1,1.2,1.3)
2.Disaster Recovery Plan- Riyaz Mohammad Arbaz(20BDS0274)
(2.1,2.2,2.3,2.4,2.5,2.6)
3.Business Continuity Management- Bandi Harshavardhan Reddy(20BCE2265)
(3.1,3.2,3.3,3.4,3.5)
4.Drp Implementation- Adya Sharma(18BCI0219)
(4.1,4.1.1)

3.3 Crisis Communication Plan

- Assemble the team: by giving them roles and responsibilities such that they have to be attentive and complete their assigned tasks without fail. There must be a crisis response coordinator and one must take the leadership. There must also be media relations and internal communication between employees.
- Gather information
- Assess and decide
- Prepare to communicate
- Communicate: there must be a response from time to time in a crisis situation. There must be correct decisions taken during these times so that no one gets affected and even though they get affected there must be recovery backup plans to get out of the crisis situation.

Immediate steps within one hour:

- Assembling the whole team and discuss the strategies that are needed to be followed
- Communicating with customers and contacting media relations
- Monitoring the place and giving the updates on time and preparing a checklist based on the plan.
- The way the organizations handle the crisis is important. Without a communication plan the organizations have to scramble their work and it becomes difficult to communicate with each other.
- During Apollo 1, NASA failed to execute the plans and respond quickly.

3.4 Emergency Response Plan

- During an emergency NASA coordinates a team of experts from all over the world and gathers all the data and analysis of the disaster and comes to a conclusion about the plan they are pondering to execute.
- NASA combines with various datasets and discusses various upcoming questionnaires from customers and answers them effectively meanwhile manages to rescue the people who got affected and plan accordingly. These things would be allotted to individuals in the form of their duties so that working speed would be much higher than expected.

3.5 Contingency Plan

- Contingency plans must be made such that there would be quick and clear information about the plan to everyone.
- Plans must be concise and easy to implement during the process of recovery.
- This kind of concise and well formatted plan reduces an unnecessary complexity during a disaster and reduces confusion at the time of implementation.
- There must be a preplanned idea before every step so that that would be executed when needed without delay.
- Although NASA had contingency plans for space but it had none for emergencies on the ground. As said before, NASA didn’t have a crisis

communication plan when Apollo 1 broke out so it was not prepared to execute even the further plans. Apollo 1 taught them a big lesson which they sorted out for the next missions.

4. DRP Implementation

4.1 Implementation

In the study that we performed we came up with a few things that the new space technology should keep in check to cover the area they are lacking in.

Propulsion systems:

Over the decades only relatively minor changes have been made in launch vehicles. Nothing substantial has changed with solid or liquid propellants performance and related technologies which are key to overall launcher capability. On a longer timescale, the challenge is to develop and implement technologies, such as hypersonic air breathing rocket engines, to be used in hybrid launchers to cut the need for large amounts of oxygen that have to be carried by current vehicles. Launch vehicles that could take off and land as aircraft, without the need for extensive and expensive service between missions, should also be developed.

New space: the space sector should consider exploiting new opportunities in front of them. These could include new services, offered through applications of space data (from precision navigation/agriculture, surveillance, to Earth environment monitoring, etc.), to more futuristic opportunities, such as space tourism or asteroid mining. Here is where we can identify a first challenge and learn a lesson from history, preventing space from becoming a lawless “wild west” where the strongest can take an unfair advantage. This should apply to Low Earth Orbit (LEO), where the current regulatory framework should be further developed and enforced to manage the increasing “space traffic” as well as to Medium (MEO) or Geosynchronous Earth Orbit (GEO) and interplanetary exploration and exploitation. Indeed, new regulations should be implemented respecting established treaties and principles (e.g., “Outer Space Treaty” or the “Convention on International Liability for Damage Caused by Space Objects”).

Large Space Structures(LSS): The capability to deploy LSS is another factor that, similarly to advances in propulsion, would enable a range of applications, but they present a series of significant challenges which depend on the specific areas.On the one hand there are instruments like telescopes, cameras, and antennas that require large (>10 m and possibly an order of magnitude larger) high-precision reflective surfaces. Here the current methodologies are limited by the size and number of segments that can be deployed, and the overall staggering cost. Concerning the antennas, a variety of deployable solutions have been proposed, from inflatables to tensegrity structures, but some countries still need to develop an appropriate commercial solution for current and future applications. Overall, new lighter-weight technologies have to be deployed, to increase packaging efficiency without compromising the quality of the final reflector.

In-Orbit Servicing and Active Debris Removal: there are a lot of opportunities offered by robotic in-orbit servicing and the development of flexible technologies that can support multipurpose missions. These opportunities include the servicing and potential repairing of current satellites, to active debris removal. in 1984 the Space Shuttle Discovery mission STS-51-A, brought back to Earth two old satellites no longer functioning (probably the first example of Active Debris Removal), and similarly the mission of the shuttle Endeavor in 1993 (and other following missions) provided essential fixes and services to the Hubble Space Telescope. the opportunity here is to develop robotic technologies able to perform these type of missions at a fraction of the cost

5. TESTING:

5.1 RISK MANAGEMENT

5.1.1 RISK MANAGEMENT LIFE CYCLE POLICIES AND PROCEDURES

The risk management method is a framework for the moves that need to be taken. There are 5 primary steps which may be taken to govern hazard; those steps are referred to as the risk manipulate technique. It starts off evolved with identifying risks, is going on to analyze dangers, then the danger is prioritized, a solution is completed, and in the end, the threat is monitored. In guide structures, each step involves masses of documentation and control.

Step 1: Identify the Risk

The first step is to become aware of the risks that the agency is uncovered to in its working environment. There are many awesome kinds of dangers – prison risks, environmental risks, market dangers, regulatory risks, and masses more. It is vital to pick out as loads of those threat factors as viable. In a manual environment, the ones dangers are stated down manually. If the commercial company commercial employer corporation has a chance control answer hired all these records is inserted immediately into the tool. The benefit of this approach is that those risks are simply seen to each stakeholder inside the commercial corporation company with get right of entry to the device. Instead of this essential data being locked away in a document which ought to be asked via e-mail, definitely everybody who desires to see which risks were identified can get entry to the records within the hazard manage device.

Step 2: Analyze the Risk

Once a risk has been diagnosed it desires to be analyzed. The scope of the risk must be determined. It is also important to apprehend the link most of the danger and different factors inside the corporation. To determine the severity and seriousness of the risk it's miles vital to appearance what number of enterprise talents the hazard influences. There are risks which could supply the whole organization to a standstill if actualized, whilst there are dangers for you to awesome be minor inconveniences in the assessment. In a manual risk management surroundings, this evaluation must be finished manually. When a threat manipulate solution is done one of the most important easy steps is to map dangers to big files, regulations, techniques, and business organization techniques. This way that the tool will have already got a mapped risk framework with a view to evaluate dangers and will permit you to understand the ways-engaging in outcomes of every threat.

Step 3: Evaluate or Rank the Risk

Risks want to be ranked and prioritized. Most hazard manage answers have one in each of a type training of dangers, counting on the severity of the threat. A risk that may motive a few inconveniences is rated lowly; dangers that can result in catastrophic loss are rated the high-quality. It is important to rank dangers because it allows the enterprise organisation to benefit a holistic view of the risk exposure of the complete agency. The business enterprise organisation can be liable to several low-degree risks, however it cannot require pinnacle control intervention. On the possibility hand, surely one of the most-rated dangers is sufficient to require right now intervention.

Step 4: Treat the Risk

Every risk wishes to be eliminated or contained as a good deal as feasible. This is completed with the useful resource of connecting with the specialists of the sphere to which the hazard belongs. In a guide surroundings, this includes contacting every and each stakeholder and then installing vicinity meetings so anyone can communicate and speak the problems. The trouble is that the speak is damaged into many one-of-a-kind email threads, across tremendous documents and spreadsheets, and masses of taken into consideration one in every of a type mobile phone call. In a danger control solution, all the applicable stakeholders may be sent notifications from within the device. The discussion regarding the chance and its viable answer can take vicinity from inside the tool. Upper control also can hold a close to eye at the solutions being endorsed and the development being made inside the tool. Instead of all and sundry contacting every different to get updates, actually all people can get updates without delay from within the chance manipulate answer.

Step 5: Monitor and Review the Risk

Not all dangers can be eliminated – a few dangers are typically present. Market dangers and environmental risks are simply examples of dangers that continuously need to be monitored. Under manual structures monitoring occurs via diligent personnel. These experts want to ensure that they hold a close to watch on all hazard elements. Under a digital environment, the threat manages device video show units the entire threat framework of the organization business enterprise. If any trouble or risk adjustments, it's far without delay seen to clearly every person. Computers also are tons better at constantly tracking risks than human beings. Monitoring dangers moreover allows your industrial organization commercial enterprise organisation to make sure continuity.

5.2 ASSESSMENT AND EVALUATION

5.2.1 DEVELOPMENT OF RISK ASSESSMENT METHODOLOGY

5.2.1.1 CBA

A cost-benefit analysis is the method of evaluating the projected or predicted costs and blessings (or opportunities) associated with a task selection to determine whether or not or no longer it makes feel from a company attitude.

Generally speaking, rate-advantage assessment includes tallying up all prices of a challenge or choice and subtracting that quantity from the entire projected benefits of the undertaking or preference. (Sometimes, this price is represented as a ratio.)

If the projected advantages outweigh the prices, you may argue that the choice is a terrific one to make. If, instead, the charges outweigh the advantages, then a corporation also can want to reconsider the choice or assignment.

Cost-gain evaluation is a shape of facts-pushed preference-making most often implemented in commercial enterprise employer, both at set up corporations and start-ups. The simple necessities and framework may be implemented to sincerely any desire-making way, whether or not or not business enterprise-related or in any other case.

How To Conduct A Cost-Benefit Analysis

1. Establish a Framework for Your Analysis

For the assessment to be as correct as feasible, you need to first set up the framework interior that you're carrying out it. What, precisely, this framework looks like will depend on the specifics of your business enterprise.

Identify the goals and goals you're seeking out to address with the idea. What do you want to carry out to remember the company a fulfilment? This permit you to emerge as aware of and recognize your fees and blessings, and can be crucial in interpreting the consequences of your assessment.

Similarly, determine what metric you'll be the use of two diploma and examine the benefits and fees. To effectively take a look at the 2, the charges and benefits want to be measured within the same "not unusual foreign exchange." This doesn't need to be an actual foreign places coins, but it does frequently include assigning a dollar quantity to each functionality charge and gain.

2. Identify the Costs and Benefits

The next step is to sit down and acquire separate lists: One of all the projected expenses, and the possibility of the anticipated blessings of the proposed assignment or motion.

When tallying expenses, we'll likely start with direct charges, which embody prices right away associated with the producing or improvement of a services or products (or the implementation of an assignment or business organisation business enterprise preference). Labour costs, manufacturing prices, materials prices, and stock costs are all examples of direct fees.

But it's moreover important to transport past the obvious.

Other cost categories that must be accounted for include:

- Indirect Costs: These are typically fixed expenses, such as utilities and rent, that contribute to the overhead of conducting business.
- Intangible Costs: These are any costs that are difficult to measure and quantify. Examples may include decreases in productivity levels while a new business process is rolled out, or reduced customer satisfaction after a change in customer service processes that leads to fewer repeat buys.

- Opportunity Costs: This refers to lost benefits, or opportunities, that arise when a business pursues one product or strategy over another.

Similarly, benefits can be:

- Direct: For example, increased revenue and sales generated from a new product
- Indirect: Such as increased customer interest in your business or brand
- Intangible: For example, improved employee morale
- Competitive: For example, being a first-mover within an industry or vertical

3. Assign a Dollar Amount or Value to Each Cost and Benefit

Once the exhaustive lists of all charges and advantages have been compiled, a fixed amount is to be assigned to each. If we can't deliver all of the fees and blessings a cost, then it's far going to be tough to assess them as it need to be.

Direct prices and blessings may be an appropriate to assign a dollar amount to. Indirect and intangible expenses and blessings, as an alternative, can be tough to quantify. That does now not imply you shouldn't strive, despite the fact that; there are numerous software program options and methodologies to be had for assigning those a lot less-than-obvious value.

4. Tally the Total Value of Benefits and Costs and Compare

Once every price and advantage have a dollar quantity next to it, you could tally up every list and feature a look at the two.

If basic benefits outnumber common prices, then there can be a enterprise case if you need to keep with the task or selection. If large fees outnumber well known blessings, then you could want to rethink the belief.

Beyond in reality looking at how the entire charges and benefits evaluate; you need to moreover bypass once more to the framework set up in step one. Does the evaluation show you accomplishing the dreams you've diagnosed as markers for success, or does it show you falling short?

If the charges outweigh the benefits, ask yourself if there are alternatives to the idea you haven't taken into consideration. Additionally, you'll be able to recognize fee reductions at the way to will can help you attain your goals greater cheaply on the same time as though being powerful.

5.4 RISK CONTROL POLICIES AND COUNTERMEASURES

Generically, risk management is a set of activities aimed at understanding, communicating, and managing risk to the achievement of objectives. Risk management operates continuously in an activity, proactively risk-informing the selection of decision alternatives and then managing the risks associated with implementation of the selected alternative. In this NPR, risk management is defined in terms of RIDM and CRM. This NPR addresses the application of these processes to all Agency activities directed toward the accomplishment of Agency strategic goals, including: strategic planning and assessment; program and project concept development, formulation, and implementation; institutional management of infrastructure, including physical, human, and information technology resources; and acquisition. This NPR also adds requirements for a formal process of risk acceptance that assigns accountability for each risk acceptance decision to a single responsible, authoritative individual (e.g., organizational unit manager), rather than to a committee or group of individuals. In addition, institutional risks and the coordination of risk management activities across organizational units are addressed.

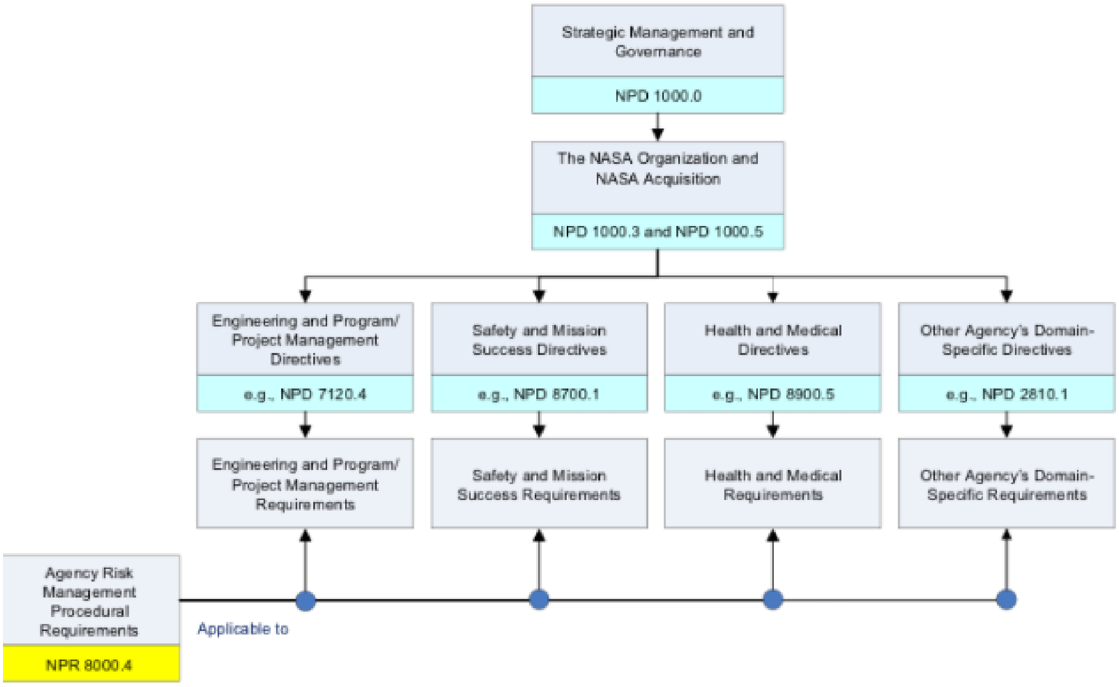

Strategic Management and Governance
NPD 1000.0
The NASA Organization and NASA Acquisition
NPD 1000.3 and NPD 1000.5
Engineering and Program/ Project Management Directives
e.g., NPD 7120.4
Safety and Mission Success Directives
e.g., NPD 8700.1
Health and Medical Directives
e.g., NPD 8900.5
Other Agency's Domain-Specific Directives
e.g., NPD 2810.1
Engineering and Program/ Project Management Requirements
Safety and Mission Success Requirements
Health and Medical Requirements
Other Agency's Domain-Specific Requirements
Agency Risk Management Procedural Requirements
NPR 8000.4
Applicable to

Fig. Intersection of NPR 8000.4 with Program/Project and Domain-Specific Directives and Requirements

In general, risk is concerned with uncertainty about future outcomes. For the purposes of this NPR, risk is the potential for shortfalls with respect to achieving explicitly established and stated objectives. As applied to programs and projects, these objectives are translated into performance requirements, which may be related to institutional support for mission execution or related to any one or more of the following domains:

a. Safety

b. Mission Success (Technical)

c. Cost

d. Schedule

Conceptually, the risk to an objective consists of the following set of triplets:

a. The scenario(s) leading to degraded performance with respect to one or more performance measures (e.g., scenarios leading to injury, fatality, destruction of key assets; scenarios leading to exceedance of mass limits; scenarios leading to cost overruns; scenarios leading to schedule slippage);

b. The likelihood(s) (qualitative or quantitative) of those scenario(s); and

c. The consequence(s) (qualitative or quantitative severity of the performance degradation) that would result if the scenario(s) was (were) to occur.

6. BACKUP and disaster recovery:

Backup means making a duplicate copy of the original file/data.

This comes in use when someone clashes with an unexpected data deletion, database has been corrupted, virus attacked, hacked, or technical issue in software update

Disaster recovery refers to quick reestablishment access for data, apps, or any resource after a outbreak.

Keeping a copy of data is no use. To make sure for business continuity, it’s important to robust and have a tested, verified and successful DRP (disaster recovery plan).

Let’s first come to know the key terms:

--Recovery time objective (RTO):

Time taken to recover a business operation after an outbreak. Recovering a data means lose of time, so while making a RTO you need to consider what amount of time you’re willing to lose.

Example:

If NASA lost its data like while launching a rocket if it loses its fuel calculating data then, it may take much time to physically check the fuel tanks and to recover the data it may take 30min (consider for example) then rocket launching delay may occur and may lead to major problems (the travel distance may be increased).

--Recovery point objective:

This means theamount of data that is expected to be lost in a disaster. So, we need to copy the data frequently soo that the recent updated data may be recovered after the disaster. if this is neglected then its his individual responsibility for losing the data which took year to be build.

--Failover:

It is offloading tasks to backup data in such a way that its is perfect to user. One may fail over to primary data center to secondary site, with a reductant system that are good to take over the data immediately.

--Failback:

Its disaster recovery process to switch back to the original data. When the disaster has passed and the primary center is backed up and running successfully the we must be able to failback perfectly as well.

--Restore:

It is the process of transferring he backed up data to the main system or data center. This process is majorly considered as part of backup more than disaster recovery.

One last main term:
Disaster Recovery as a Service (DRaaS):

Let's consider this as a managed proper approach for disaster recovery. A third-party host or management is responsible to manage the infrastructure used for disaster recovery. Counted DRaaS provide tools for the management of disaster process or establish an organization to have the processes managed by them.

NASA Technical Reports Server (NTRS) is the nasa's database – https://ntrs.nasa.gov/

As per the record in march 2019, in NAS archival strogae system approx. 110 petabytes of unique data is being stored.

Nasa has adopted a diverse system, with an established commercial platform i.e. cloud platform and its own data centres.

Here AI play a major role. It helps the human scientists find correct data source and point them to joint up the dots with previous research.

Nasa has divided the data into various component

Earth science data: Nasa's Earth Observing System Data and Information System is build as a distributed system holding major facilities of Nasa's Distributed Active Archive Centers.

Space science Data, which holds atmospheric nodes, geoscience nodes, cartography and imaging science nodes, planetary plasma interactions, ring-moon system, small bodies, navigations and ancillary informations., Astro material data system , exoplanet archive, the Astro-biology habitable environment database

Life science data: this focuses on the life sciences as behavior and performance data and so on.

NASA people data: this holds the data of who works where, on what, and changes happened.

NASA data information & Tools:

These are few variety of sites that offer data tools;

Landsat Satellite Data Explorer (USGS & NASA): , Global Imagery Browse Services (GIBS): , NASA Earth Observations: , Earth Observatory: , Earth Plus:

Astrophysics: , Heliophysics: , Solar System Exploration: , Helioviewer: , Find Visible Near Earth Small Bodies (Asteroids & Comets): , Physical Data & Dynamical Constraints:

Human Research Program:

Space Weather Action Center: , NASA STEM: , My NASA Data: , MultiSpec: , WorldWind:

Nasa backup

If we lost someone's log the it will be safe in a library and can be recovered. But what about Nasa and other international space stations. Every end of the day NASA's robots back up miles of tapes which contain the latest data from satellites and space stations. And additionally ongoing missions produce still more data which is stored in additional tapes. Soo the media holds so much of data. Its not possible to copy the large tapes before they are deteriorated. According to rough calculation it may take 20years to read the whole data but the tapes life span is less than 20 years. With accordance with Moore's law the data-storage capacity has been increased. We can read 40 Gb tapes at a max of 12mbps(according to 2000 records). Soo the time taken to copy increases. Even if third-party agencies implement new tapes, it will be impossible to completely transfer the whole data before a nonrecoverable data loss occurs. This can be fixed by encouraging the new generation for mass-storage technologies, partnering public agencies with industries to handle and maintain research programs.

SpaceX backup

But now cloud is playing a major role in everyone's life, in same way google cloud gets into orbit by connecting with SpaceX for data and cloud services. They have forged a new fresh partnership using the google cloud and ability of space technology firm's starlink low earth orbit satellite constellation to use high speed internet broadband all across the world. This was done because cloud's private network closes the loop, supports the delivery of satellite internet service, brings business and consumers in connection to cloud and internet. Cloud provides perfect, secure, and fast access to critical applications and services organization need to implement in their team and run.

7. BUSINESS RECOVERY

7.1 BUSINESS RECOVERY TEAM:

In business recovery team, we include prevention, monitoring and correction departments and allot their specific works to them

PREVENTION:

This team will take care of the project and ensure that there is no failure that is going to happen and recheck all the functionalities.

MONITORING:

This team will take care of the overall path of the rocket or any other project handled. They would be dealing the time to time works done by that particular rocket and make sure that no deployment is going to happen.

CORRECTION:

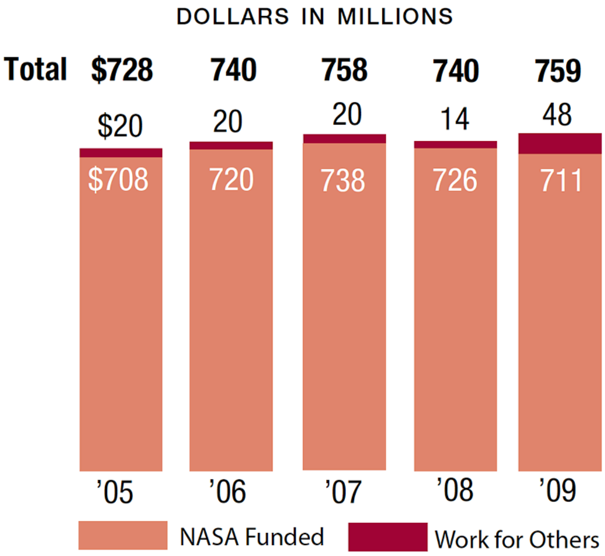
This team would be doing the correction part and rectify the mistakes which lead to the failure and make sure that they don't repeat in their further projects.

7.2 ASSESSMENT OF DAMAGE AND BUSINESS IMPACT:

There would be definitely an impact on business and the staff working in that particular organization also get affected. As seen in contingency plans and recovery plans there would be teams assigned to each and every work such that fast initiatives would be taken and the damage would be overcome in a shorter span of time.

There also would be damage occurred and time would be taken for the recovery. The companies associated with the organization would also be affected and there are graphs available according to the loss faced by that companies.

The drawbacks which caused the impact must be recovered and new alternatives and forward steps must be taken so that the faults don't repeat and they lead in successful completion of mission.



7.3 PLANNING RECOVERY ACTIVITIES:

Develop recovery strategies:

A recovery strategy is used to restore information system operations quickly and effectively after a disruption. This plan should consider the disruption impacts and allowable outage times identified in the business impact analysis. The recovery strategy should consider several factors, including cost, outage time, security, and integration with larger recovery plans at the organization level.

A recovery strategy should address potential impacts identified in the BIA during the design and implementation phases of the information system life cycle.

Recovery strategies should combine multiple methods that complement each other to provide recovery capabilities across a wide range of incidents

A wide range of recovery methods may be employed, with the appropriate choice depending on the incident, type of system, and operational requirements.

Several types of recovery methods can be used when developing a system recovery strategy, including cold, warm, hot, mobile, mirrored, and reciprocal agreements with internal and external technologies.

Backup methods:

A backup of an information system must be stored at an alternate site to support recovery in the event of an information system failure. Data backup frequency should be determined by Agency policy, data sensitivity, and new information introduced frequently.

The contingency plan should state where stored data is located, naming conventions for files, rotation frequency of media, and a method to transport data offsite

The method selected to perform backups should take into account the availability and integrity requirements for the system and data.

Whenever data needs to be retrieved or tested, the organization contacts the storage facility and requests that the data be transported to the organization or to another facility.

7.4 COMMUNICATION SYSTEMS:

Primary recovery ship: During Apollo 8 mission, it affected two significant changes of primary recovery ship, one is the use of high frequency communication and the other is use of ship board communications.

But the communications were going good in atlantic ocean, coming to pacific ocean it was difficult to communicate because of the increase in distance so the signals were not reachable enough to communicate between people. In the Apollo 9 mission the operations were successful and tests also indicated that ATS(application technology satellite) and LES-6 terminals could provide excellent ship or shore recovery communications.

Secondary recovery ship: A secondary recovery ship (SRS) was less likely to be called upon to support a recovery effort than a PRS, but reliable communications were still needed. Fewer circuits were however required. In general, destroyers were designated as SRSs, although in some cases, oilers had also been used. Rather than be needed for their regular missions, destroyers and oilers did not have the communications capacity, either in circuits or in radiated power output, that aircraft carriers and helicopter carriers did.

The nasa worldwide communication network interface:

Before each mission alternative communications channels were identified and checked so that if necessary, they could be used. The primary link between the CTF 130 RCC in Hawaii and the SAR aircraft staging base in Australia was a high-frequency circuit. As a backup, Hawaii and Australia circuits of the NASA Worldwide Communications Network (NASCOM) were set up to be available to recovery forces

In this arrangement, recovery personnel at the staging base were provided with means to monitor the CM air-to-ground communications via ground operational support systems (GOSS).

Circuits were installed near other tracking stations or NASCOM switching centers so that each RCC could monitor the GOSS circuit. These circuits were installed in Bermuda, Moron/Ramstein, Australia, Norfolk, and Hawaii.

7.5 HUMAN RESOURCES:

The NSSC provides many human resources. Let's see some of them here,

Benefits:

As part of NASA's benefits package, you can choose from health, dental, vision, and life insurance plans as well as flexible spending accounts and long-term care insurance.

Classification services:

It is the process of determining the title, occupational series, and grade of a position based on its duties and responsibilities.

NASA's Classification Team ensures that the agency's classification program follows OPM and agency policy guidelines.

In processing:

NASA's In-Processing Team provides assistance to new civil servants, transferees, retirees, reinstated, converted, and reassigned employees.

Employee notices:

NASA civil service employees receive notices on topics including annual notifications required by law and regulation, employee rights and duties, as well as various benefits and entitlements.

Staffing:

To hire the right talent for the Agency, Staffing Services works directly with hiring managers. They are provided by the OCHCO Executive Services Division and the OCHCO Office of Inspector General

When there is an emergency situation during exploration, then they use the food which would be stored in beforehand. The recovery team rescues the people and supply the food packets and other required resources so that they donot suffer with hunger.

7.6 IT systems software architecture recovery:

Fault detection, isolation and recovery:
FDIR approaches tend to focus on single subsystems and rely on a homogeneous platform and software architecture, often sharing data through shared memory or a blackboard component. It is necessary to perform FDIR across various heterogeneous networks. Ideally, FDIR should help optimize cooperation between planetary systems and group operations.

Control system failure tolerance:
Various approaches are needed to provide failure tolerance for both hardware and software components of control systems in case of failure or performance degradation. In particular, reducing crew maintenance time and reducing hardware re-supply costs are important, as these are the most expensive operations for these systems.

Planning and scheduling:
The process includes responding to system failures, supporting adjustments to operations, inventory, and logistics due to planned and unplanned maintenance, and developing applications that support planning and scheduling. It is imperative that developed applications support the integration of both planet-side and Earth-side activities.

Approaches for integration of new controls technology with existing legacy systems:
The technology behind some space technologies is relatively mature. New control technologies must be compatible with legacy fieldbuses and operations concepts as well as provide new functionality. In order to keep pace with the growth of system functionality, tools and development methodologies are needed.