NIST Cybersecurity Framework

Complete Business Process of the Implementation Plan

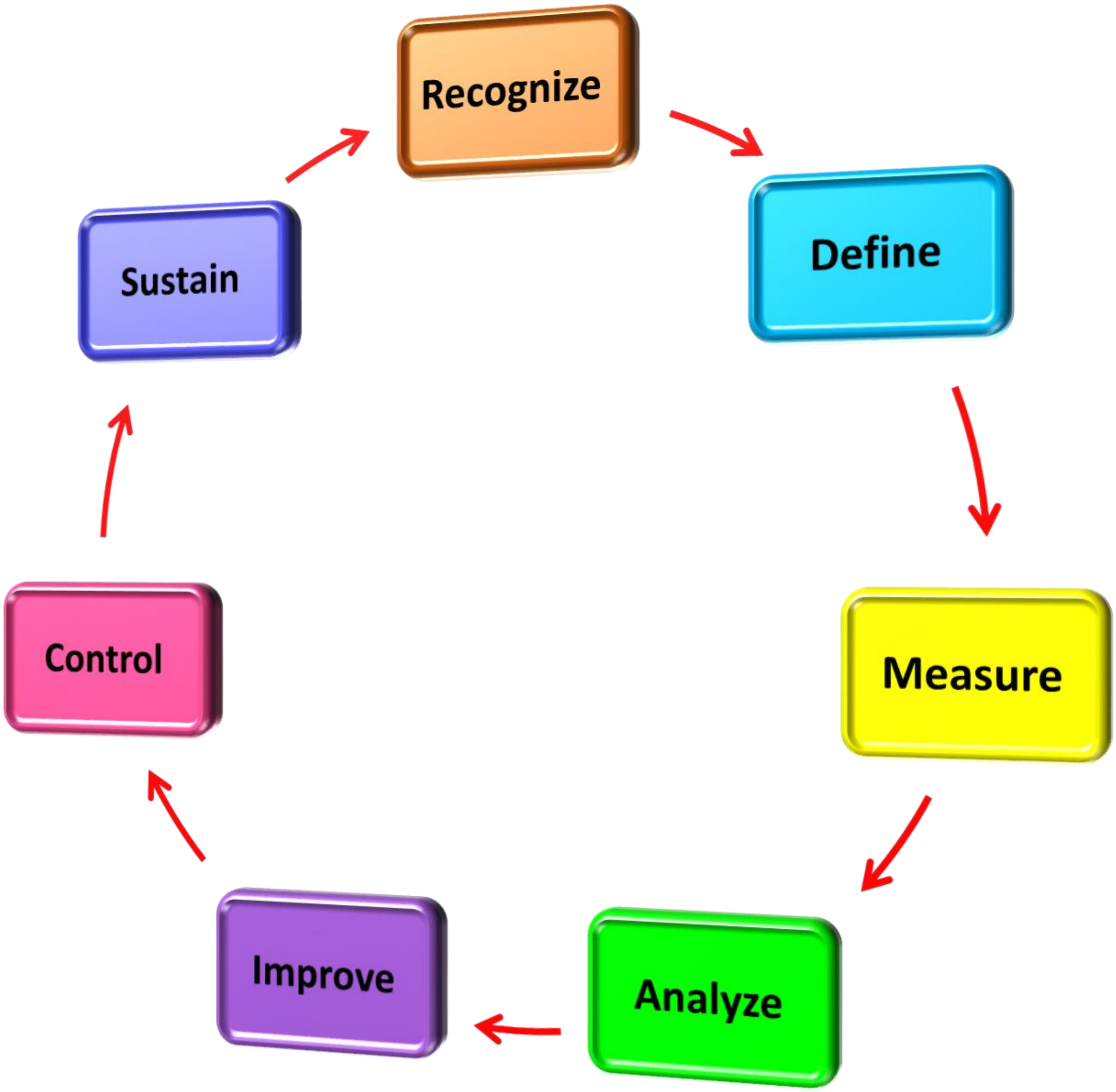
NIST ***(National Institute of Standards and Technology)*** Cybersecurity Framework self-assessment guide greatly contributes in planning & implementing the business processes accurately. This particular guideline / toolkit addresses the common security challenges towards an organization & the appropriate best practices to be followed. This is a well-documented step-by-step work plan (procedure) and a maturity diagnostic tool for any NIST Cybersecurity Framework related project.

When it comes the toolkit, mainly there are 3 main steps in implementing the NIST Cybersecurity Framework.

Step 01 :- Get your bearings

- In here, basically it gives an overview of the necessary requirements for the stakeholders. This is organized according to a data-driven improvement cycle which contains the following characteristics.

  - ➢ Recognize
  - ➢ Define
  - ➢ Measure
  - ➢ Analyze
  - ➢ Improve
  - ➢ Control
  - ➢ Sustain


Recognize
Define
Measure
Analyze
Improve
Control
Sustain

Step 02 :- Setting concrete goals, tasks, dates & numbers you can track

- In here, there are altogether 998 new and updated case-based questions that are organized into seven core areas of process designs. This particular step becomes very helpful in identifying the areas in which NIST Cybersecurity Framework can be improved furthermore.

- Following are some of the very **base level requirements** in implementing the NIST Cybersecurity Framework for an organization.

1) What threats will you protect yourselves against, what will you tolerate for the sake of efficiency, and what risk will remain exposed simply because you cannot overcome the policy problems to fix it?

2) Are alternate command/control methods identified, and are agreements in place to permit the resumption of operations within a defined time period when the primary system capabilities are unavailable?

3) Does your current insurance program, which might include Directors and Officers Liability, Errors and Omissions, Property and General Liability products, address all your corporate assets at risk?

4) Have adequate security management protocols and procedures been implemented for systems with known, identified vulnerabilities which cannot be stopped/shut down until the next maintenance cycle?

5) How do you evaluate the effectiveness of your cyber security program in protecting organization, customer and business partner data that has been stored, processed or transmitted in cyberspace?

6) How can individuals accurately assess costs, risks, and benefits, especially when risks may be determined by others choices and an individuals understanding of consequences is generally poor?

7) Have you taken measures to ensure proper coordination among safety, security (including cyber) and emergency response arrangements and have adopted an all-hazards approach to risk management?

8) What are your organizations policies and procedures governing risk generally and cyber security risk specifically? How does senior management communicate and oversee policies and procedures?

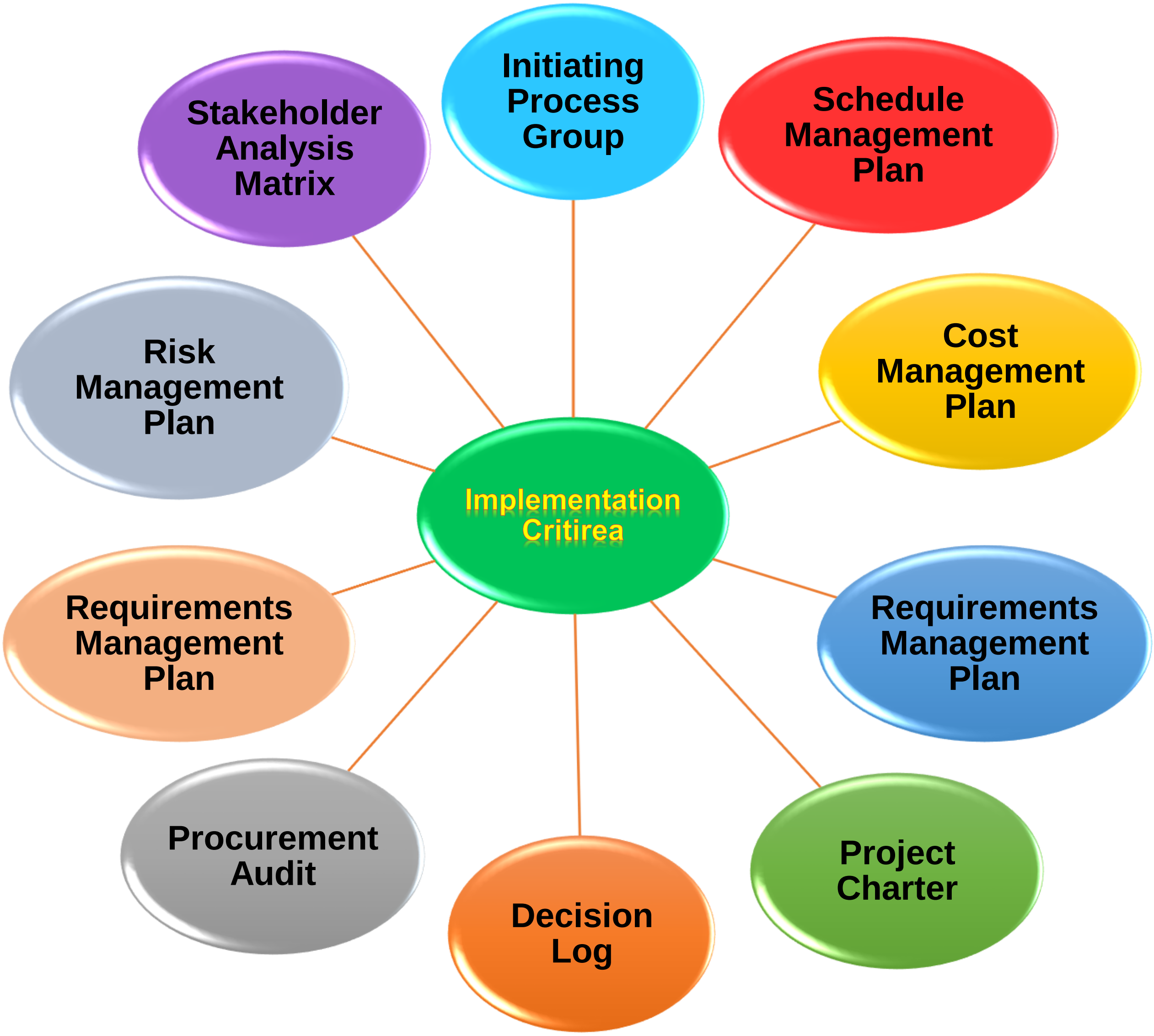
9) Is there a particular practice, framework, guidance or system that your organization has deployed on cyber-risk management that you as a board director find to be helpful or a best practice?

10) How can financial services organizations begin the journey toward establishing programs to really be more secure, vigilant, and resilient and hence transform cyber risk management programs?

- You are able to complete this self-assignment by yourself or else you can complete it by gathering a team as well. By completing the above tasks, you are able to find the appropriate solutions for those questions after prioritizing them.

Step 03 :- Implement, Track, follow up and revise strategy

- The final outcomes of the 2nd stage are required as inputs, in order to perform the 3rd step. In this particular stage, **starting & managing** of the NIST Cybersecurity Framework projects is performed using 62 different implementation resources. Following check box represents the base-level project requirements & success criteria.



1) ***Initiating Process Group*** :-

- What input will you be required to provide the NIST Cybersecurity Framework project team?

2) ***Schedule Management Plan*** :-

- Is the IMS development and management approach described?

3) ***Cost Management Plan*** :-

- Are any non-compliance issues that exist due to State practices communicated to your organization?

4) ***Requirements Management Plan*** :-

- Will the product release be stable and mature enough to be deployed in the user community?

5) ***Project Charter*** :-

- What outcome, in measurable terms, are you hoping to accomplish?

6) ***Decision Log*** :-

- What are guidelines that the team has identified that will assist them with getting the most out of team meetings?

7) ***Procurement Audit*** :-

- Are there appropriate controls in place to ensure that the procurement NIST Cybersecurity Framework project complies with relevant legislation?

8) ***Requirements Management Plan*** :-

- Who is responsible for monitoring and tracking the NIST Cybersecurity Framework project requirements?

9) ***Risk Management Plan*** :-

- People risk -are people with appropriate skills available to help complete the NIST Cybersecurity Framework project?

10)***Stakeholder Analysis Matrix*** :-

- Who shall you involve in the making of the stakeholder map?

- Each of the above-mentioned groups consist with the following components.

	Components
Initiating Process Group	1) NIST Cybersecurity Framework project Charter 2) Stakeholder Register 3) Stakeholder Analysis Matrix
Planning Process Group	1) NIST Cybersecurity Framework project Management Plan 2) Scope Management Plan 3) Requirements Documentation 4) Requirements Traceability Matrix 5) NIST Cybersecurity Framework project Scope Statement 6) Assumption and Constraint Log 7) Work Breakdown Structure 8) Schedule Management Plan 9) Activity Attributes 10)Network Diagram 11)Activity Resource Requirements 12)Resource Breakdown Structure 13)Activity Duration Estimates 14)Duration Estimating Worksheet 15)NIST Cybersecurity Framework project Schedule 16)Cost Management Plan 17)Activity Cost Estimates 18)Cost Estimating Worksheet 19)Cost Baseline 20)Quality Management Plan 21)Process Improvement Plan 22)Responsibility Assignment Matrix 23)Roles and Responsibilities

	24) Human Resource Management Plan 25) Communications Management Plan 26) Risk Management Plan 27) Risk Register 28) Probability and Impact Assessment 29) Probability and Impact Matrix 30) Risk Data Sheet 31) Procurement Management Plan 32) Source Selection Criteria 33) Stakeholder Management Plan 34) Change Management Plan
Executing Process Group	1) Team Member Status Report 2) Change Request 3) Change Log 4) Decision Log 5) Quality Audit 6) Team Directory 7) Team Operating Agreement 8) Team Performance Assessment 9) Team Member Performance Assessment 10) Issue Log
Monitoring and Controlling Process Group	1) NIST Cybersecurity Framework project Performance Report 2) Variance Analysis 3) Earned Value Status 4) Risk Audit 5) Contractor Status Report 6) Formal Acceptance
Closing Process Group	1) Procurement Audit 2) Contract Close-Out 3) NIST Cybersecurity Framework project or Phase Close-Out 4) Lessons Learned

Results :-

- By following the above-explained 3-step process, you get the opportunity to experience the following advantages.

1) You will be able to diagnose NIST Cybersecurity Framework projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices.

2) You will get the opportunity to implement evidence-based best practice strategies aligned with overall goals.

3) You can integrate the recent technological advancements with the process design strategies while adhering to best practices guidelines.