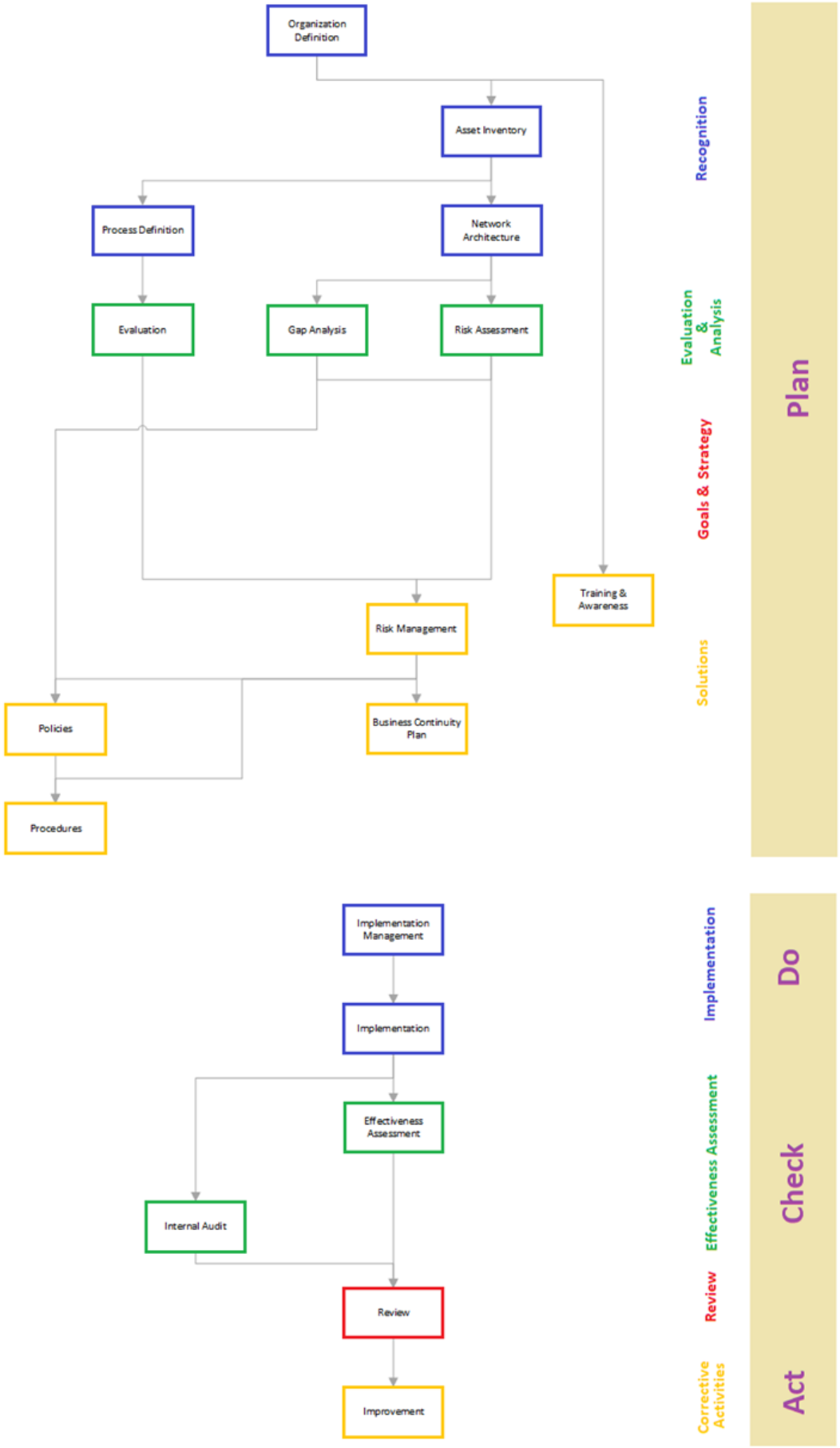
Ultimate GRC



People, Process, Technology is a holistic model for Process Improvement known and used cross industries. Introduced on a large scale about thirty years ago and by around 1999 Bruce Schneider popularized it, the model is still used as is, without major changes. Based on this model, successful implementation of framework requires more than just a technology platform. The People and the Process must also be considered in order for a holistic solution to exist.

Every organization is formed based on its vision and mission which can be translated to its goals. For achieving its goals, required to provide some products or services. To be able to provide its products or services, should define some processes and to be able to run these processes needs different type of assets. However these assets should work together as a whole system and customize according to processes.

So I believe for successful implementation of a GRC solution, the Process, People, and Technology model should be changed to Process, Asset, and Configuration model.

Ultimate GRC is developed based on this model and has the following modules:

Organization Definition: In this module basic information about interested governance including the followings is taken:

- Goals
- Objectives
- Services/Products
- Internal & External Environment
- Organization Structure and Roles
- Stakeholders
- Obligations
- Training Records

In this module some parts of Governance and Compliance is covered and belongs to Process and Asset parts of model.

Asset Inventory: This module makes a list of all assets and their specifications. Inventory of network equipment and applications and operating systems is done automatically. For Inventory of other non-digital assets such as human resource, documents if you have any inventory application or even a file, you can upload information from there. However you can enter any asset into software manually.

In this module some parts of Governance is covered and belongs to Asset part of model.

Process Definition: In this module details of all processes including the followings is documented:

- Locations
- Organization Structure
- Assets
- Technologies
- Assets involved

This module covers some parts of Process and belongs to Process part of model.

Network Architecture: This module, documents Network Infrastructure. In this module following items is documented:

- Passive Connections
- Racks Arrangement
- Protocols
- Users Information
- Infrastructure Services
- IP Addressing Scheme
- VLAN information

This module covers some parts of Governance and belongs to Configuration part of the model.

Evaluation: In this module details of all processes including the followings is documented:

- Locations
- Organization Structure
- Assets
- Technologies
- Assets involved

This module covers some parts of Process and belongs to Process part of model.

Risk Assessment: In this module vulnerabilities of all Assets is identified. For some assets such as web apps, data bases and network equipment, it will be done automatically and for other assets such as human resource and physical locations, some special forms are designed and information is entered through these forms. After vulnerability assessment Risk Assessment will be done automatically. For this purpose, all risks of all assets will be identified automatically and for each risk of each asset, likelihood and Impact and Risk Number is calculated and Risk Matrix will be generated.

Gap Analysis: In this module based on the interested governance and its related standards, the gap between current status and ideal level of standard, is calculated. This module covers some part of Compliance and belongs to Process part of the model.

Objectives Definition: There is a very famous idiom which says if you don't know where you want to go then any way you go is correct. Most organizations have no objective for the level of required security and they have no measurable index to evaluate it. In this module based on business objectives, GRC objectives is calculated. Indexes for objective definition are:
Risk Number
Level of Compliance to Standards

Risk Management: In this module, depending on the type of threat and its related vulnerabilities in various assets, appropriate solutions are proposed.
For each solution,
The implementation method which could be:

- Hardware
- Software
- Configuration
- Procedure
- Training
- Awareness

Type of solution which could be:

- Preventive
- Detective
- Reaction
- Recovery

Its impact on different security parameters of each asset which could be:

- Confidentiality
- Integrity
- Availability

is determined and for each proposed solution, following items is calculated:

- No of covered Vulnerabilities
- Risk Number Decrement

Policies: Policies are the first level of system documentation that their initial list is taken from standard and the results of the Risk Analysis. Policies are in two major types:

- Subject-based security policies
- System-based security policies

At this stage, the existing organization's policies are compared with the list of required policies and deficiencies are determined. Then, for existing policies, type, significance, template status, and structure and status of supporting documentation, including standards and procedures reviewed, and policy status. Finally, the necessary corrections are made to the existing policies in line with the policy status and the preparation of policies that are needed but not exist.

Procedures: According to the Policies and requirements in the standard and the results of the Risk Analysis, a draft of the procedures is finalized.

Training & Awareness: In this module, according to the tasks defined in the information security structure and the training background obtained in the recognition phase, the training program of each of the personnel is determined purposefully.

Business Continuity: In this module:

- Key Business Processes
- RTO and RPO for each Key Process
- Incident Management Procedure

Will be identified and developed and following documents will be generated:

- Business Continuity Plan.
- Disaster Recovery Plan.

Implementation Management: Resource Management and Implementation Operation are required before the start of the implementation phase. At this stage, the design is carried out to the stakeholders and the necessary checks are made about the remaining risks, and after the permission is issued, the implementation begins. In this module following activities will be done:

- Exchange of information with stakeholders.
- Prioritizing Risk Treatment Plan solutions.
- Acceptance of remaining risks.
- Determine the various responsibilities of implementation.
- Determine the implementation schedule.
- Estimates of implementation costs and funding.
- Obtaining an implementation license

Implementation: At this stage, implementation of the solutions presented in the design phase will be considered and includes the following:

- Implementation of configurations.
- Providing RFP for the implementation of the proposed projects.
- To justify the implementation of policies and guidelines for audiences.
- Project Management documentation for proposed projects and solutions.

Effectiveness Assessment: At this stage, by assessing the information security status of the organization based on the indicators determined before and after the implementation phase, the effectiveness of the implementation of the information security management system is measured and compared with the goals set. In module following items will be assessed:

- The degree of improvement in the Level of Risk
- The degree of improvement in the Controls Maturity
- The degree of improvement in the Process Maturity

Review: At this stage, after an internal audit and an assessment of effectiveness, if the intended security objectives are not met, the necessary corrective actions are defined to achieve these goals and are approved at the management review meeting. In accordance with the approvals of the management review and, if necessary, the technical documentation provided, in particular the revision of the risk management plan, shall be carried out.

Improvement: At this stage, while implementing corrective plans on the basis of a revision document, information on the improvement is communicated. The three main activities of this phase are the implementation of corrective plans resulting from the review phase, reassessment of the goals achieved after corrective actions, and finally information on the improvements. The output of this stage is improvement plan.