BITS Pilani

Pilani|Dubai|Goa|Hyderabad

Process Frameworks for IT Organizations

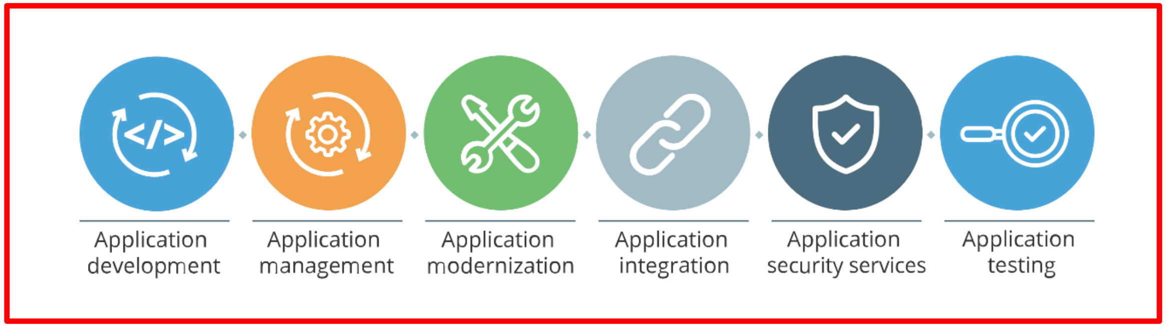
16-Oct-2022

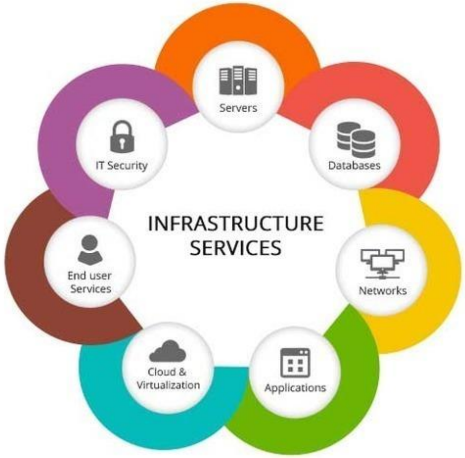
Agenda

1. Process Frameworks Landscape
2. Basic Process Framework: ISO 9001
3. Process Framework for Development: CMMI DEV
4. Process Frameworks for Services: ISO 20000, CMMI SVC
5. Process Frameworks for Information Security & Business Continuity: ISO 27001 & ISO 22301
6. Other Frameworks: ISAE 3402 & SSAE 18, HIPAA
7. Improvement Methodologies: Lean, Six Sigma
8. Business Excellence Frameworks: MBNQA, RBNQA
9. Benefits of Process Frameworks
10. Top 10 Best Practices

PROCESS FRAMEWORKS LANDSCAPE

IT Services Landscape

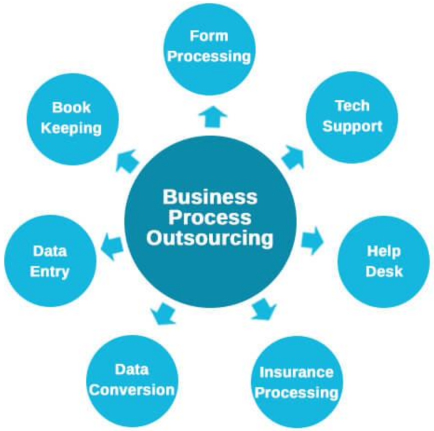




IT services refers to the application of business and technical expertise to enable organizations in the creation, management and optimization of or access to information and business processes.

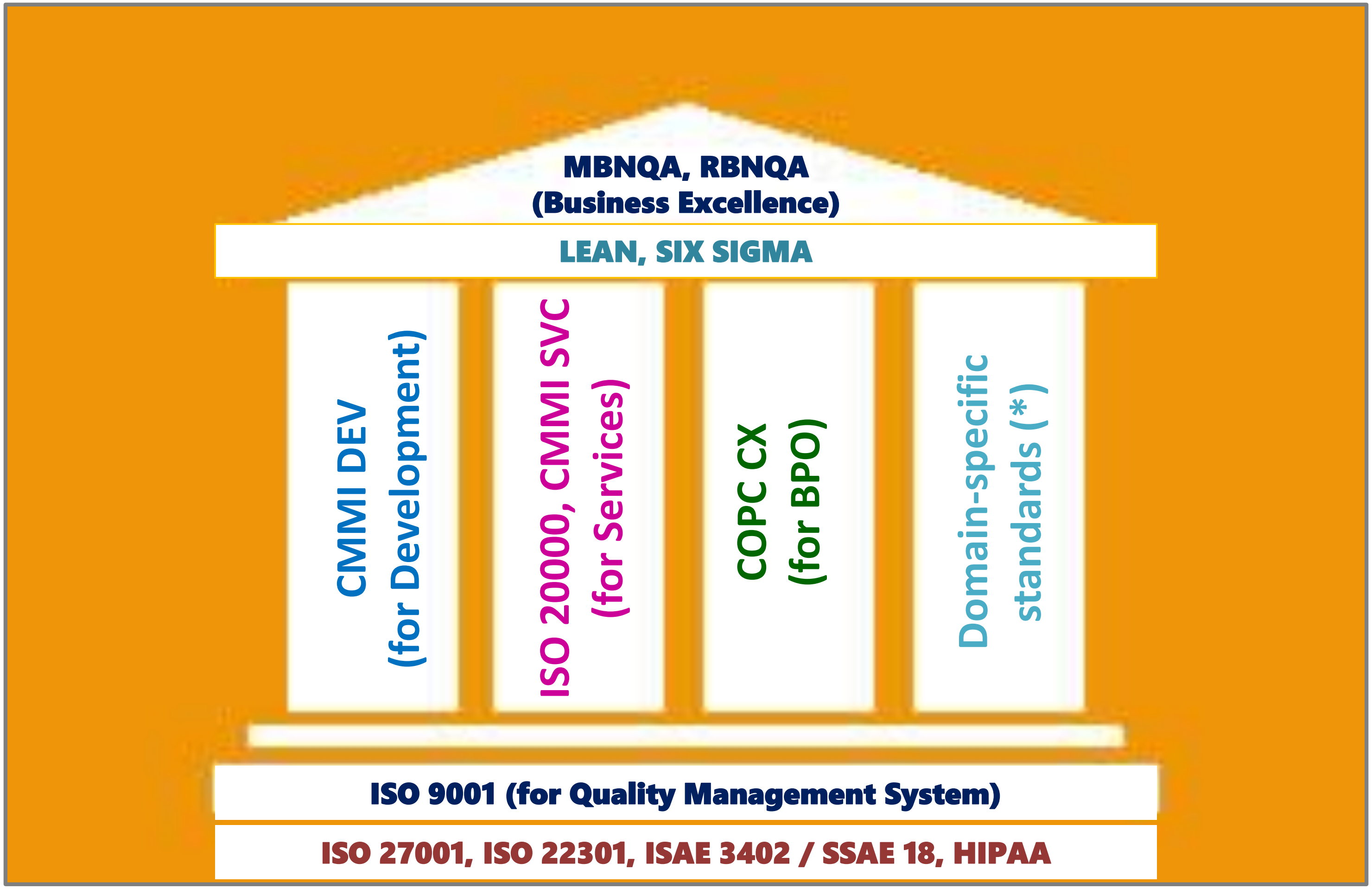
The IT services market can be segmented by the type of skills that are employed to deliver the service (design, build, run). There are also different categories of service: business process services, application services and infrastructure services.

If these services are outsourced, they are referred to as business process outsourcing (BPO), applications outsourcing (AO) and infrastructure outsourcing.



Source: https://www.gartner.com/en/information-technology/glossary/it-services

Process Frameworks Landscape

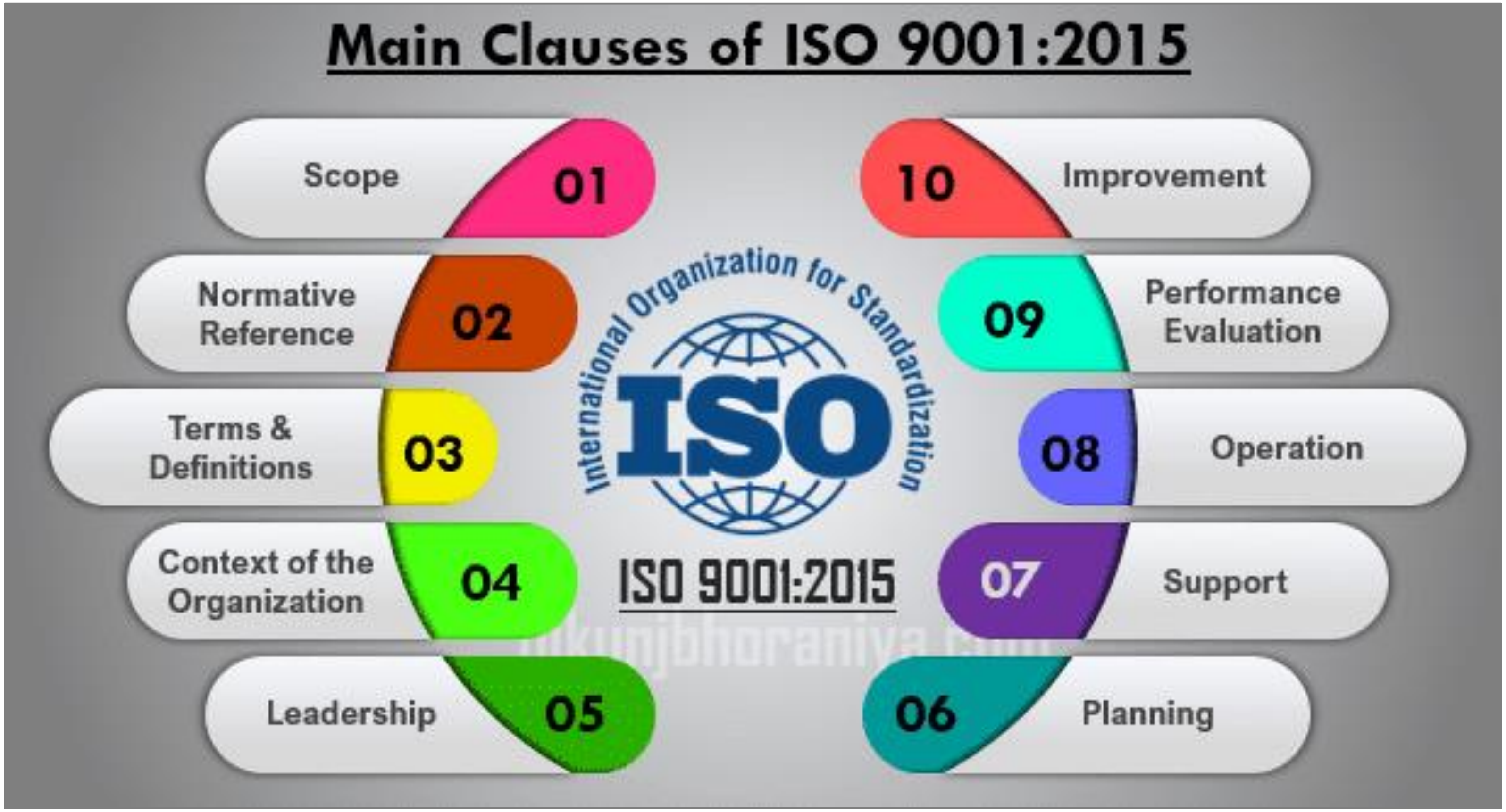


(*) Domain specific standards – Examples:

- TL 9000 - for Telecommunications industry
- AS 9100 - for Aerospace industry
- ISO 13485 - for Medical Devices industry

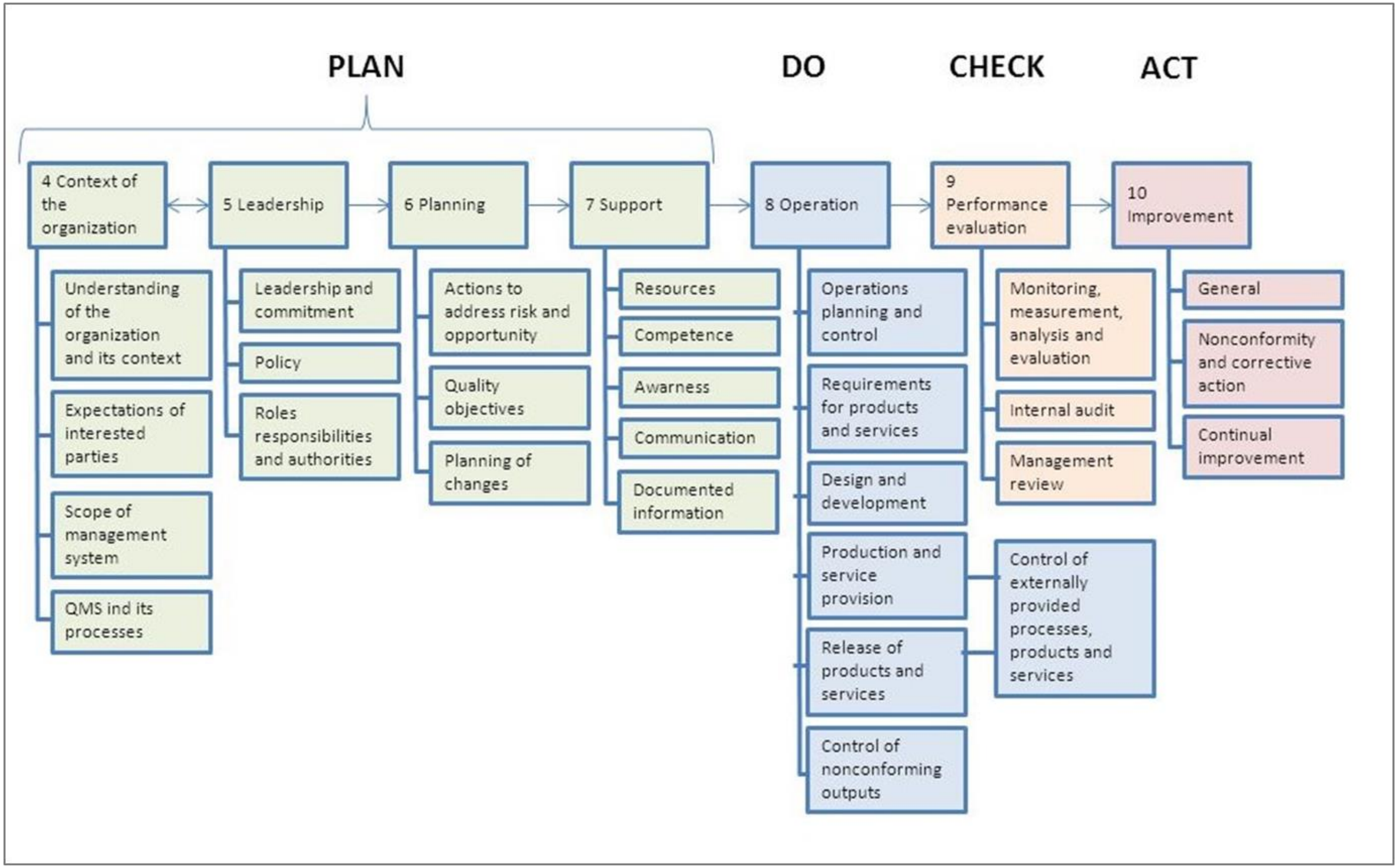
BASIC PROCESS FRAMEWORK

ISO 9001:2015



ISO 9001:2015 QMS

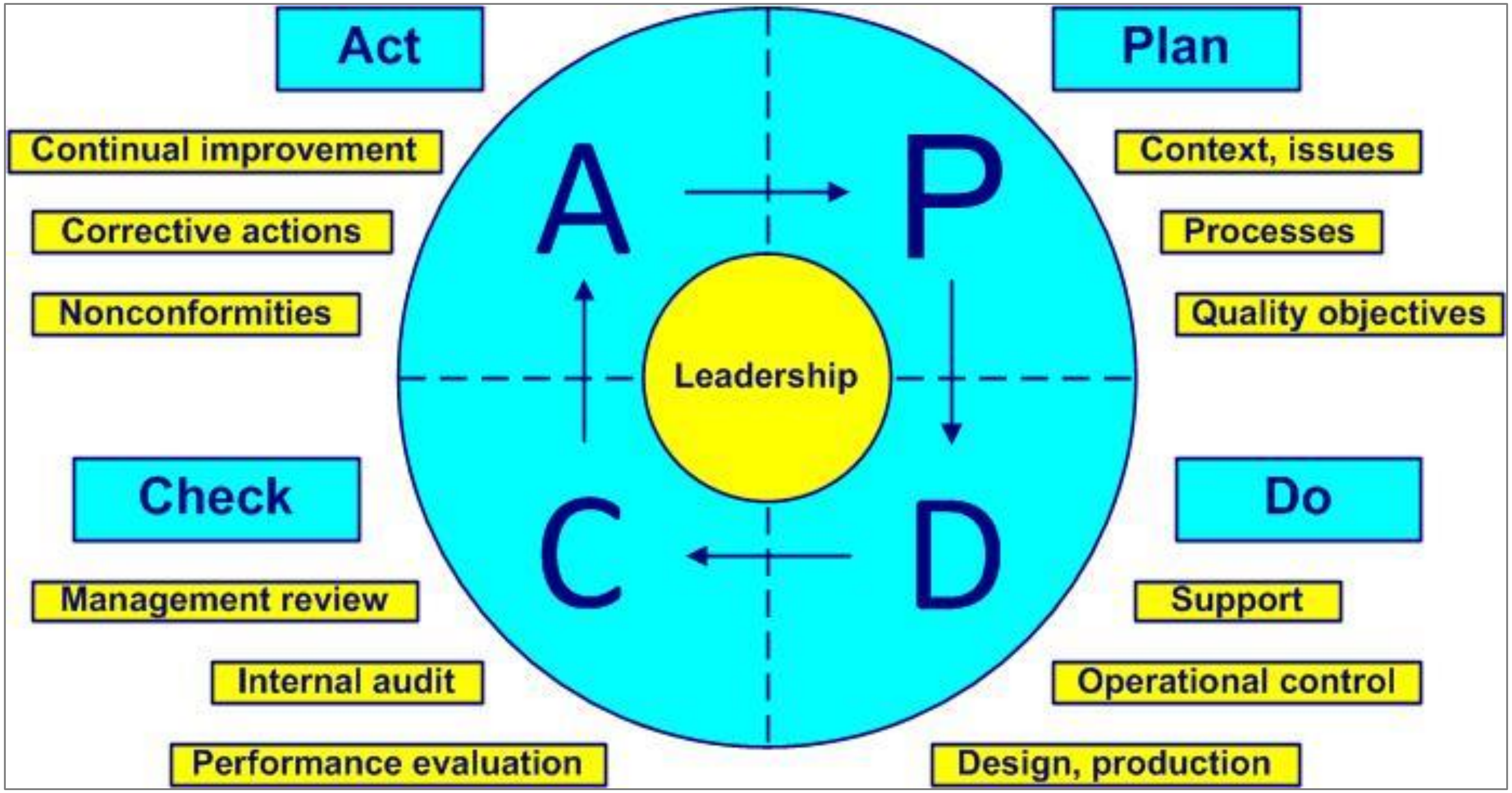
- **ISO 9001:2015 - Quality Management System**



PLAN
DO
CHECK
ACT
4 Context of the organization
5 Leadership
6 Planning
7 Support
8 Operation
9 Performance evaluation
10 Improvement
Understanding of the organization and its context
Expectations of interested parties
Scope of management system
QMS ind its processes
Leadership and commitment
Policy
Roles responsibilities and authorities
Actions to address risk and opportunity
Quality objectives
Planning of changes
Resources
Competence
Awarness
Communication
Documented information
Operations planning and control
Requirements for products and services
Design and development
Production and service provision
Release of products and services
Control of nonconforming outputs
Control of externally provided processes, products and services
Monitoring, measurement, analysis and evaluation
Internal audit
Management review
General
Nonconformity and corrective action
Continual improvement

Reference: https://www.praxiom.com/iso-9001-outline.htm

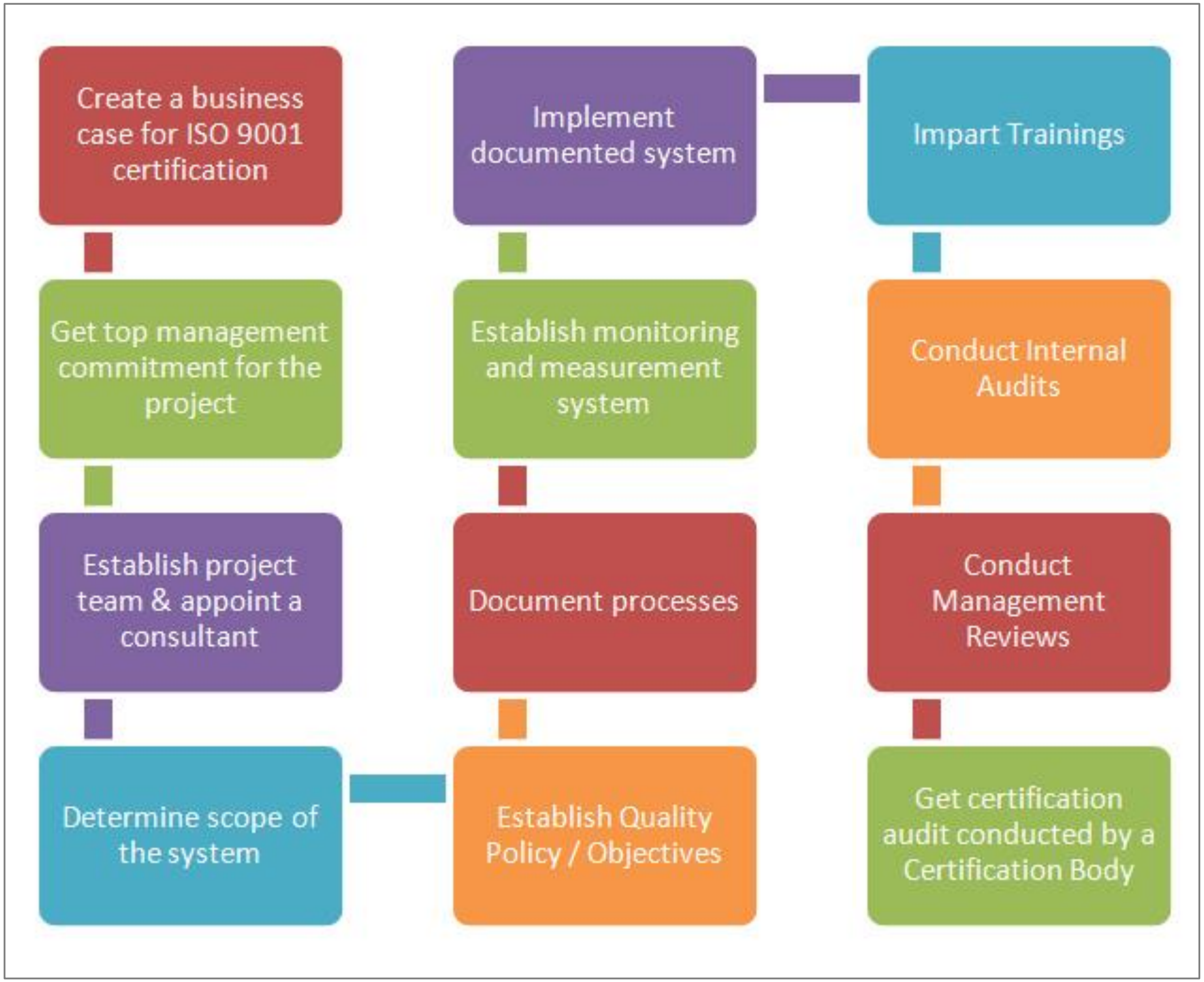
PDCA in ISO 9001:2015 structure



Key features of ISO 9001:2015 standard

- Each clause represents a group of processes.
  - The groups interact with each other.
  - The processes within the group interact with each other.
  - There are intra group interactions as well.
- All interactions are to be planned as per the requirements of this standard and/or the organization’s specific requirements.
- The requirements of the standard are generic and have to be applied to the specific situation/requirements of the organization by suitable and adequate interpretations.
- ISO 9001:2015 gives importance to risk based thinking or risk management.
- There is a provision of “non-applicability” or exclusion of certain requirements of the standard in accordance with the activities of the organization.
- There are permitted flexibilities in the standard:
  - Design of the organization’s OWN structure of QMS.
  - Prepare your OWN documentation apart from some mandated requirements.
  - Adopt and follow your OWN terminology and define the same.

ISO 9001:2015 Implementation Roadmap

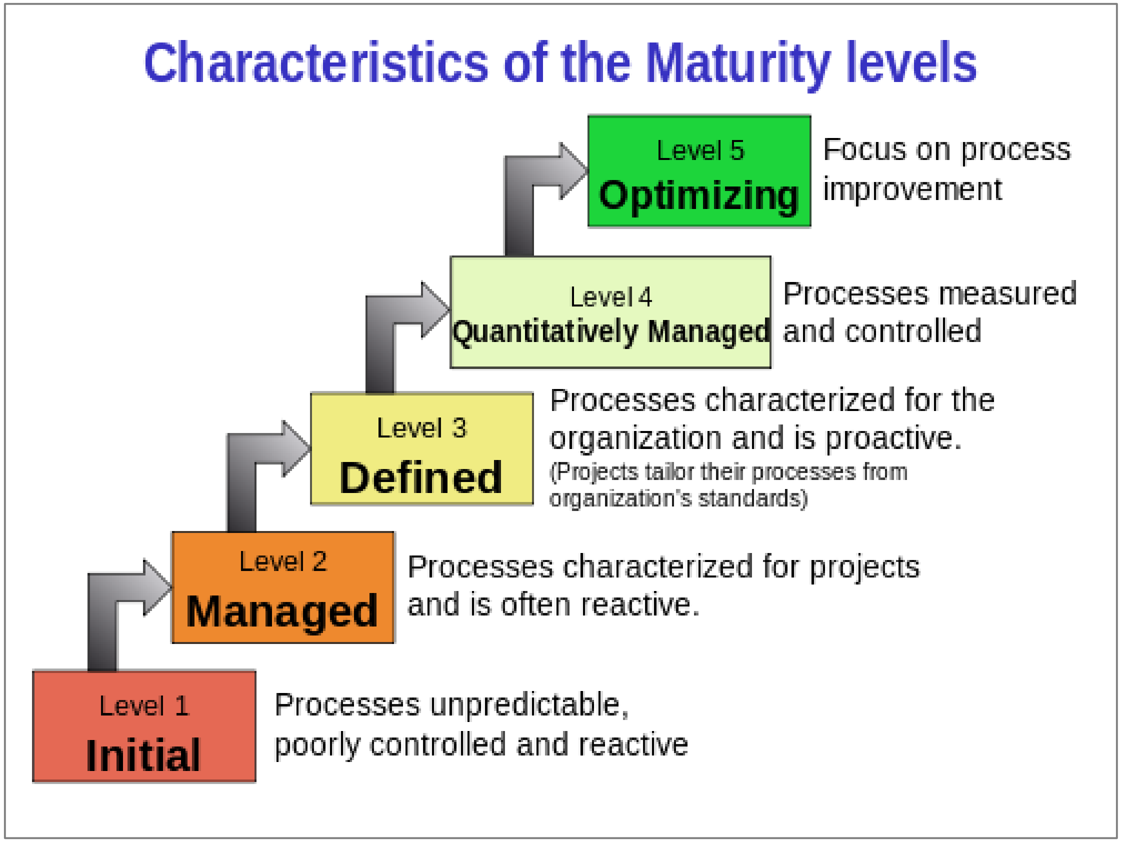


Create a business case for ISO 9001 certification
Get top management commitment for the project
Establish project team & appoint a consultant
Determine scope of the system
Establish Quality Policy / Objectives
Document processes
Establish monitoring and measurement system
Implement documented system
Impart Trainings
Conduct Internal Audits
Conduct Management Reviews
Get certification audit conducted by a Certification Body

PROCESS FRAMEWORK FOR DEVELOPMENT

CMMI for Development [1/2]

- **Characteristics of CMMI Maturity Levels**



Characteristics of the Maturity levels

Level 5 **Optimizing** — Focus on process improvement

Level 4 **Quantitatively Managed** — Processes measured and controlled

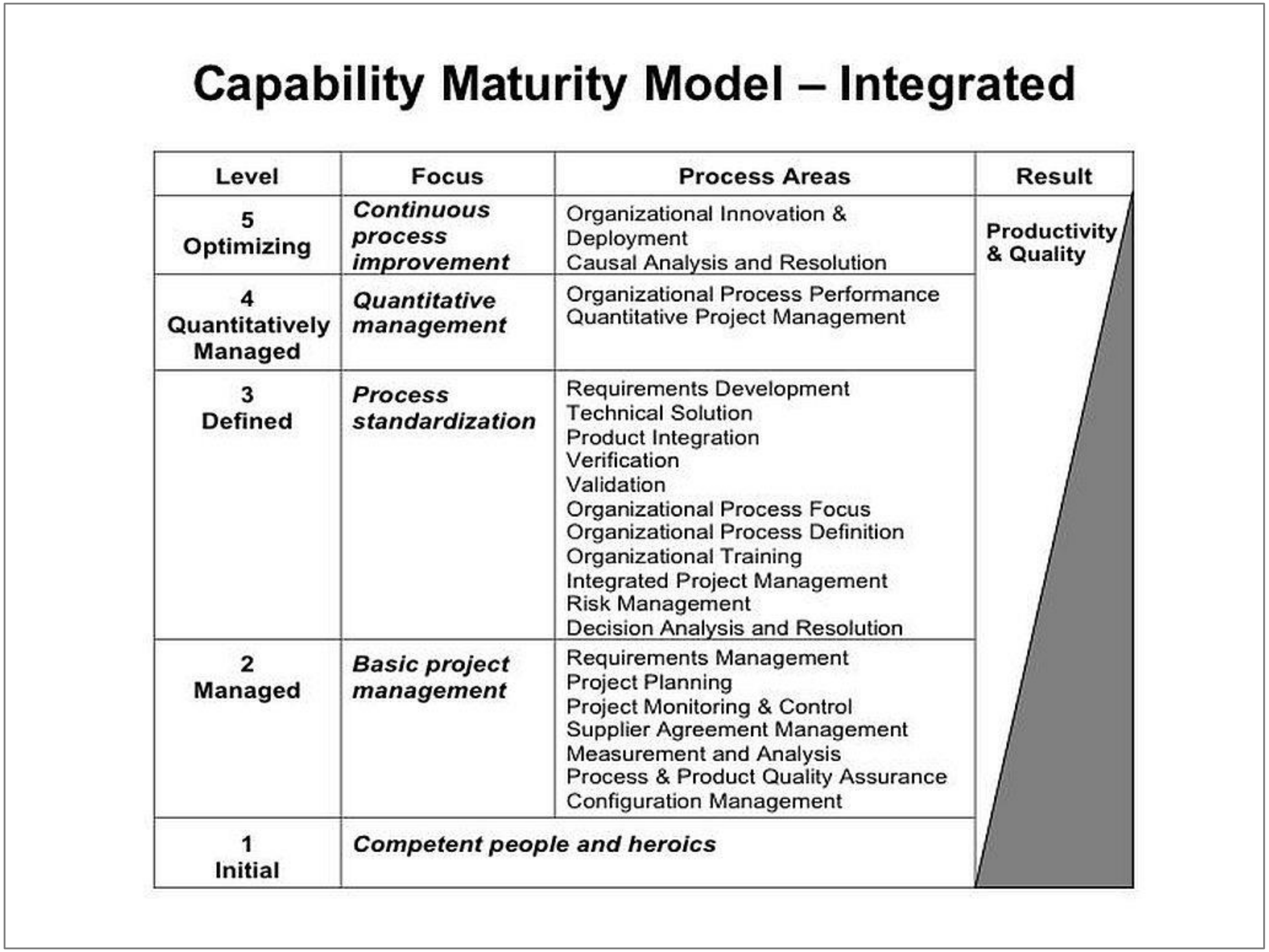
Level 3 **Defined** — Processes characterized for the organization and is proactive. (Projects tailor their processes from organization's standards)

Level 2 **Managed** — Processes characterized for projects and is often reactive.

Level 1 **Initial** — Processes unpredictable, poorly controlled and reactive

CMMI for Development [2/2]

- **Maturity Levels and Process Areas in CMMI for Development**

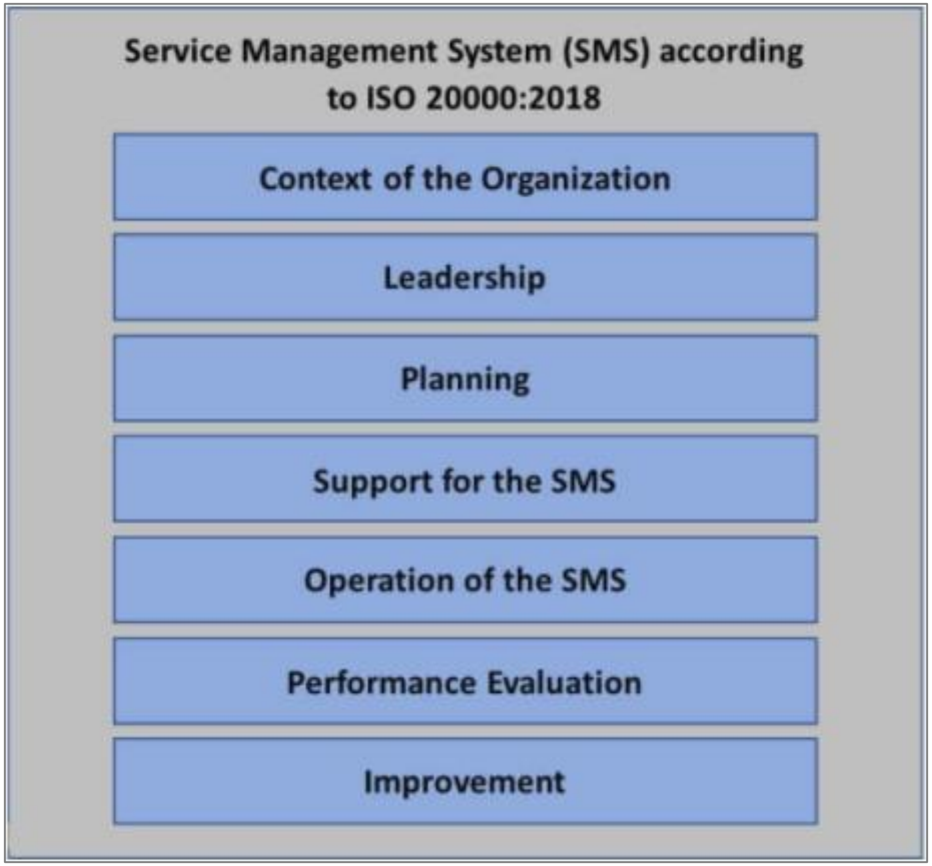


Capability Maturity Model – Integrated

Level	Focus	Process Areas	Result
5 Optimizing	***Continuous process improvement***	Organizational Innovation & Deployment Causal Analysis and Resolution	**Productivity & Quality**
4 Quantitatively Managed	***Quantitative management***	Organizational Process Performance Quantitative Project Management	
3 Defined	***Process standardization***	Requirements Development Technical Solution Product Integration Verification Validation Organizational Process Focus Organizational Process Definition Organizational Training Integrated Project Management Risk Management Decision Analysis and Resolution	
2 Managed	***Basic project management***	Requirements Management Project Planning Project Monitoring & Control Supplier Agreement Management Measurement and Analysis Process & Product Quality Assurance Configuration Management	
1 Initial	***Competent people and heroics***		

PROCESS FRAMEWORKS FOR SERVICES

Major Clauses of ISO 20000:2018

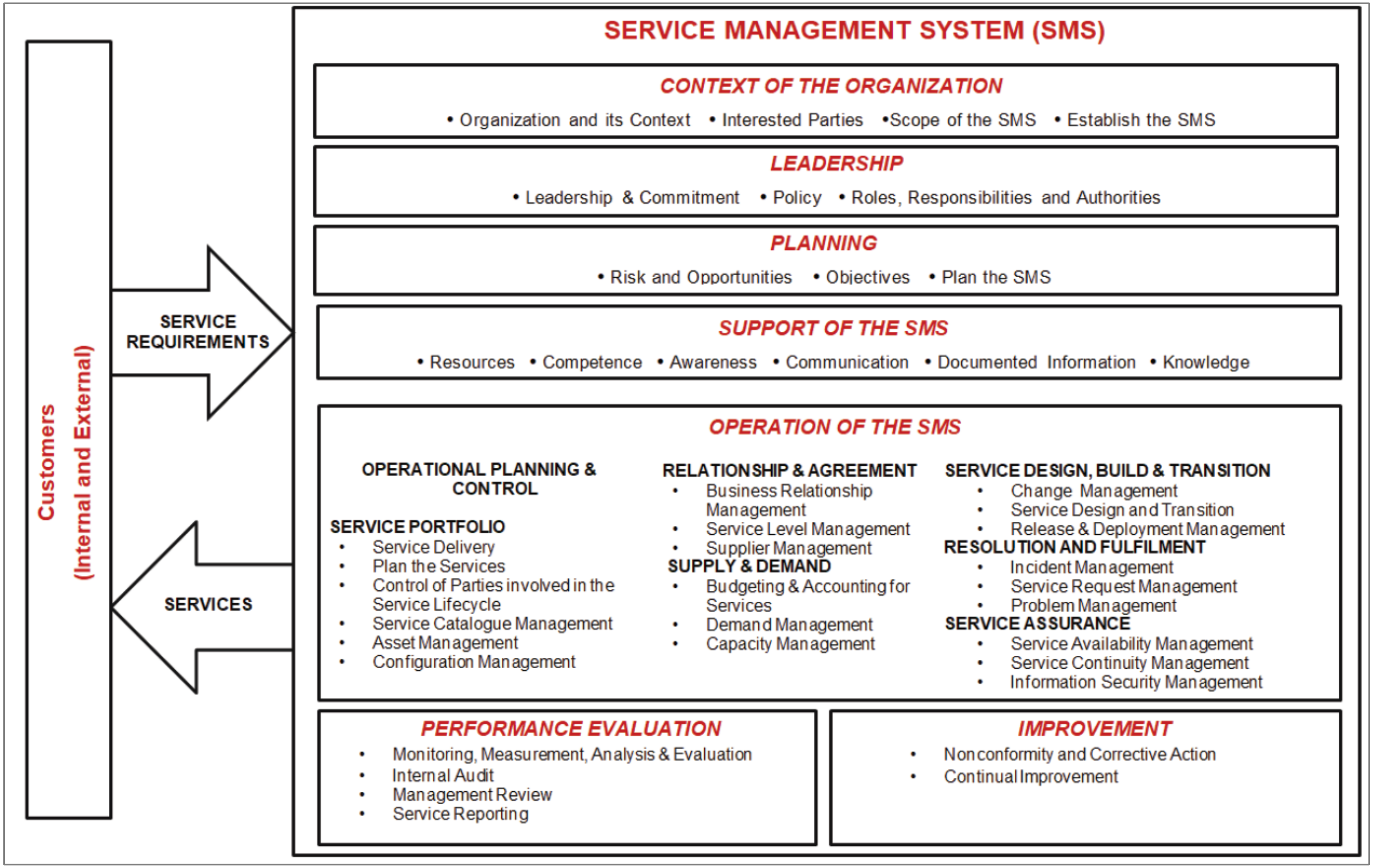


Service Management System (SMS) according to ISO 20000:2018

- Context of the Organization
- Leadership
- Planning
- Support for the SMS
- Operation of the SMS
- Performance Evaluation
- Improvement

Reference:
https://advisera.com/20000academy/blog/2019/09/05/iso-20000-requirements-and-structure/

The SMS as per ISO 20000:2018



Customers (Internal and External)

SERVICE REQUIREMENTS

SERVICES

SERVICE MANAGEMENT SYSTEM (SMS)

CONTEXT OF THE ORGANIZATION

- Organization and its Context
- Interested Parties
- Scope of the SMS
- Establish the SMS

LEADERSHIP

- Leadership & Commitment
- Policy
- Roles, Responsibilities and Authorities

PLANNING

- Risk and Opportunities
- Objectives
- Plan the SMS

SUPPORT OF THE SMS

- Resources
- Competence
- Awareness
- Communication
- Documented Information
- Knowledge

OPERATION OF THE SMS

OPERATIONAL PLANNING & CONTROL

SERVICE PORTFOLIO

- Service Delivery
- Plan the Services
- Control of Parties involved in the Service Lifecycle
- Service Catalogue Management
- Asset Management
- Configuration Management

RELATIONSHIP & AGREEMENT

- Business Relationship Management
- Service Level Management
- Supplier Management

SUPPLY & DEMAND

- Budgeting & Accounting for Services
- Demand Management
- Capacity Management

SERVICE DESIGN, BUILD & TRANSITION

- Change Management
- Service Design and Transition
- Release & Deployment Management

RESOLUTION AND FULFILMENT

- Incident Management
- Service Request Management
- Problem Management

SERVICE ASSURANCE

- Service Availability Management
- Service Continuity Management
- Information Security Management

PERFORMANCE EVALUATION

- Monitoring, Measurement, Analysis & Evaluation
- Internal Audit
- Management Review
- Service Reporting

IMPROVEMENT

- Nonconformity and Corrective Action
- Continual Improvement

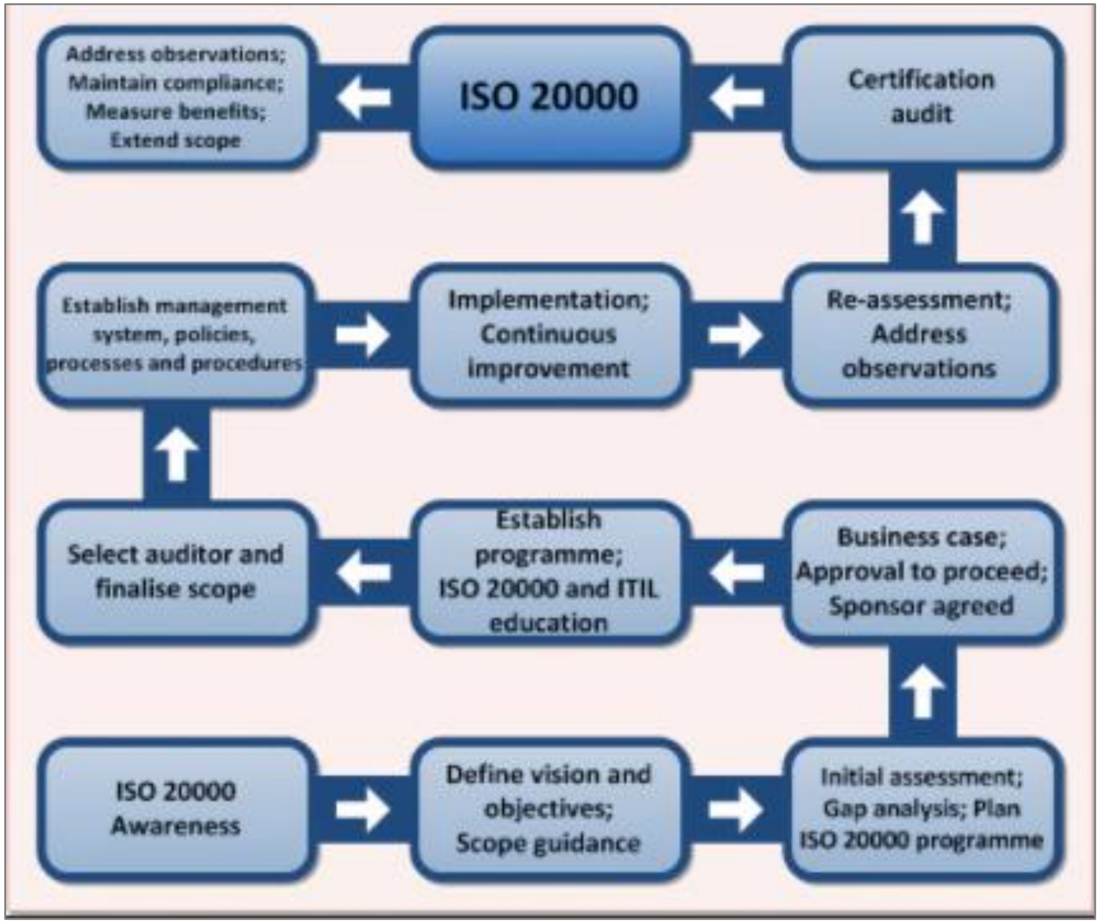
Reference:
https://pecb.com/whitepaper/isoiec-20000-1-transition

Operation of the SMS

Operation of the SMS

Reference:
https://foxitsm.com/wp-content/uploads/iso20000_wallchart_2018.gif

Roadmap for Certification

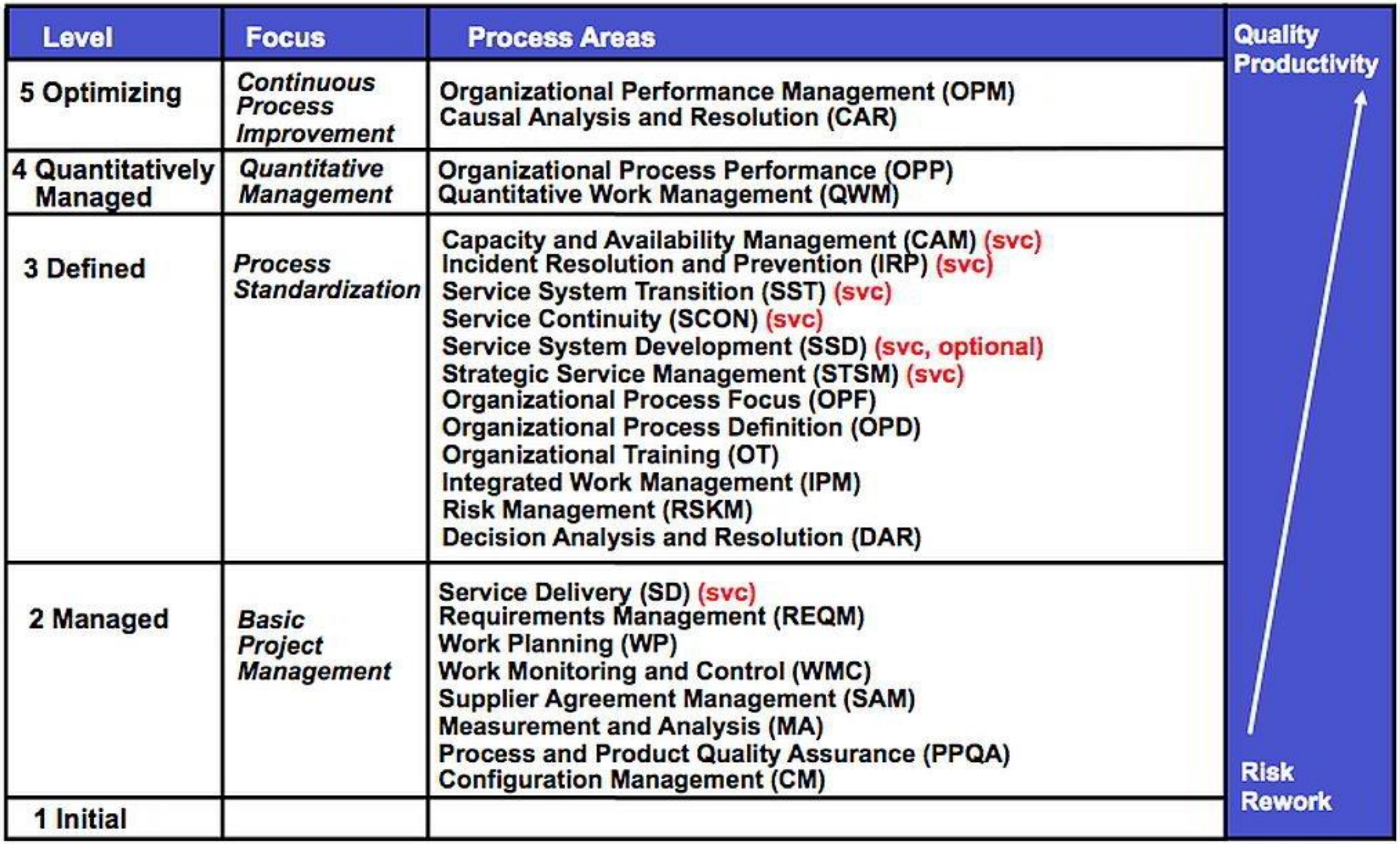

ISO 20000 Awareness
Define vision and objectives; Scope guidance
Initial assessment; Gap analysis; Plan ISO 20000 programme
Business case; Approval to proceed; Sponsor agreed
Establish programme; ISO 20000 and ITIL education
Select auditor and finalise scope
Establish management system, policies, processes and procedures
Implementation; Continuous improvement
Re-assessment; Address observations
Certification audit
ISO 20000
Address observations; Maintain compliance; Measure benefits; Extend scope

Note:

Reference to ITIL (Information Technology Infrastructure Library) in the above roadmap is applicable only in case of IT Services.

CMMI for Services

- **Maturity Levels and Process Areas in CMMI for Services**

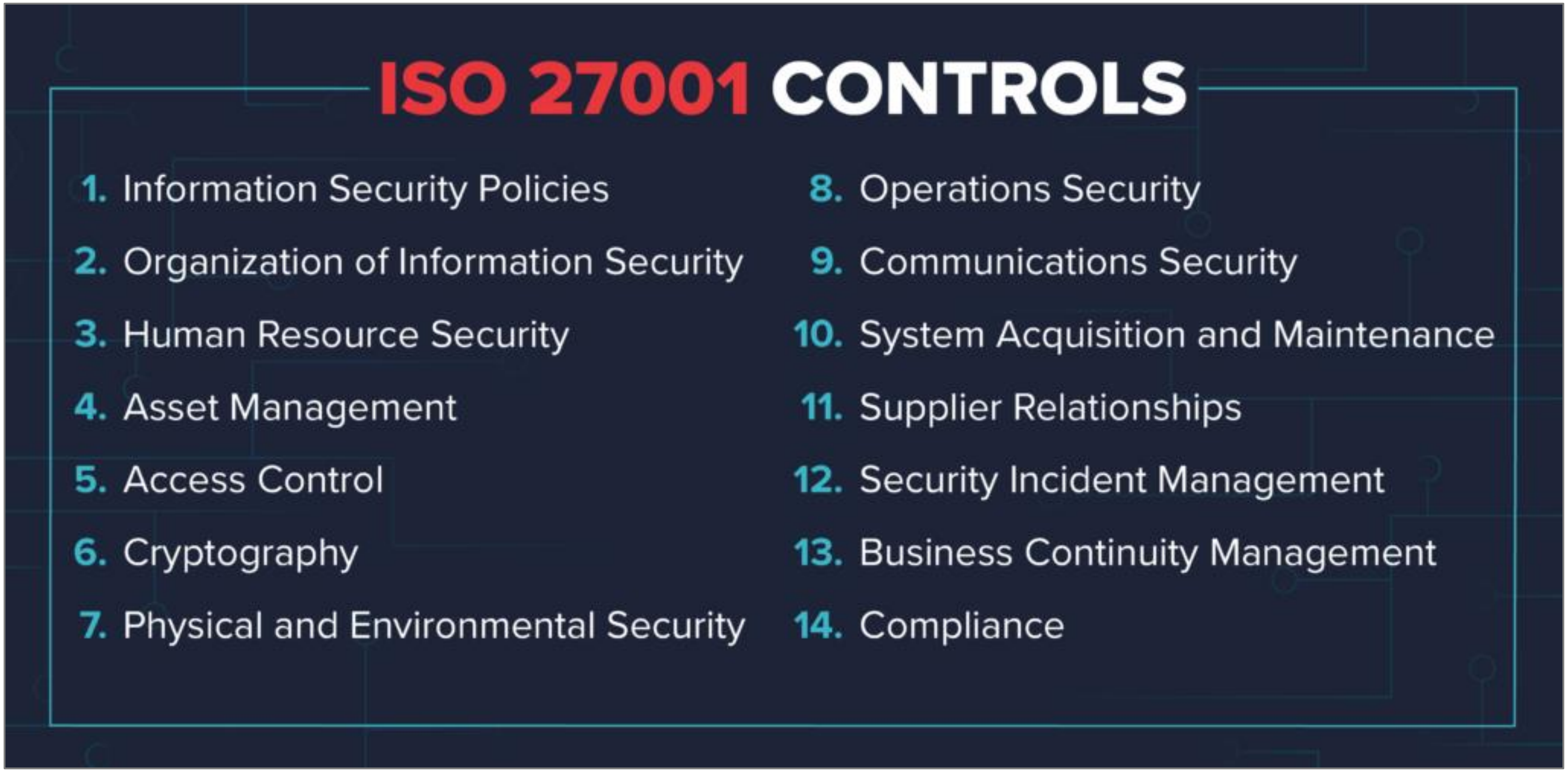


Level	Focus	Process Areas	Quality Productivity
5 Optimizing	*Continuous Process Improvement*	Organizational Performance Management (OPM) Causal Analysis and Resolution (CAR)	
4 Quantitatively Managed	*Quantitative Management*	Organizational Process Performance (OPP) Quantitative Work Management (QWM)	
3 Defined	*Process Standardization*	Capacity and Availability Management (CAM) (svc) Incident Resolution and Prevention (IRP) (svc) Service System Transition (SST) (svc) Service Continuity (SCON) (svc) Service System Development (SSD) (svc, optional) Strategic Service Management (STSM) (svc) Organizational Process Focus (OPF) Organizational Process Definition (OPD) Organizational Training (OT) Integrated Work Management (IPM) Risk Management (RSKM) Decision Analysis and Resolution (DAR)	
2 Managed	*Basic Project Management*	Service Delivery (SD) (svc) Requirements Management (REQM) Work Planning (WP) Work Monitoring and Control (WMC) Supplier Agreement Management (SAM) Measurement and Analysis (MA) Process and Product Quality Assurance (PPQA) Configuration Management (CM)	Risk Rework
1 Initial			

PROCESS FRAMEWORKS FOR INFORMATION SECUTIRY AND BUSINESS CONTINUITY

ISO 27001 - ISMS

- **ISO 27001 - Information Security Management System**

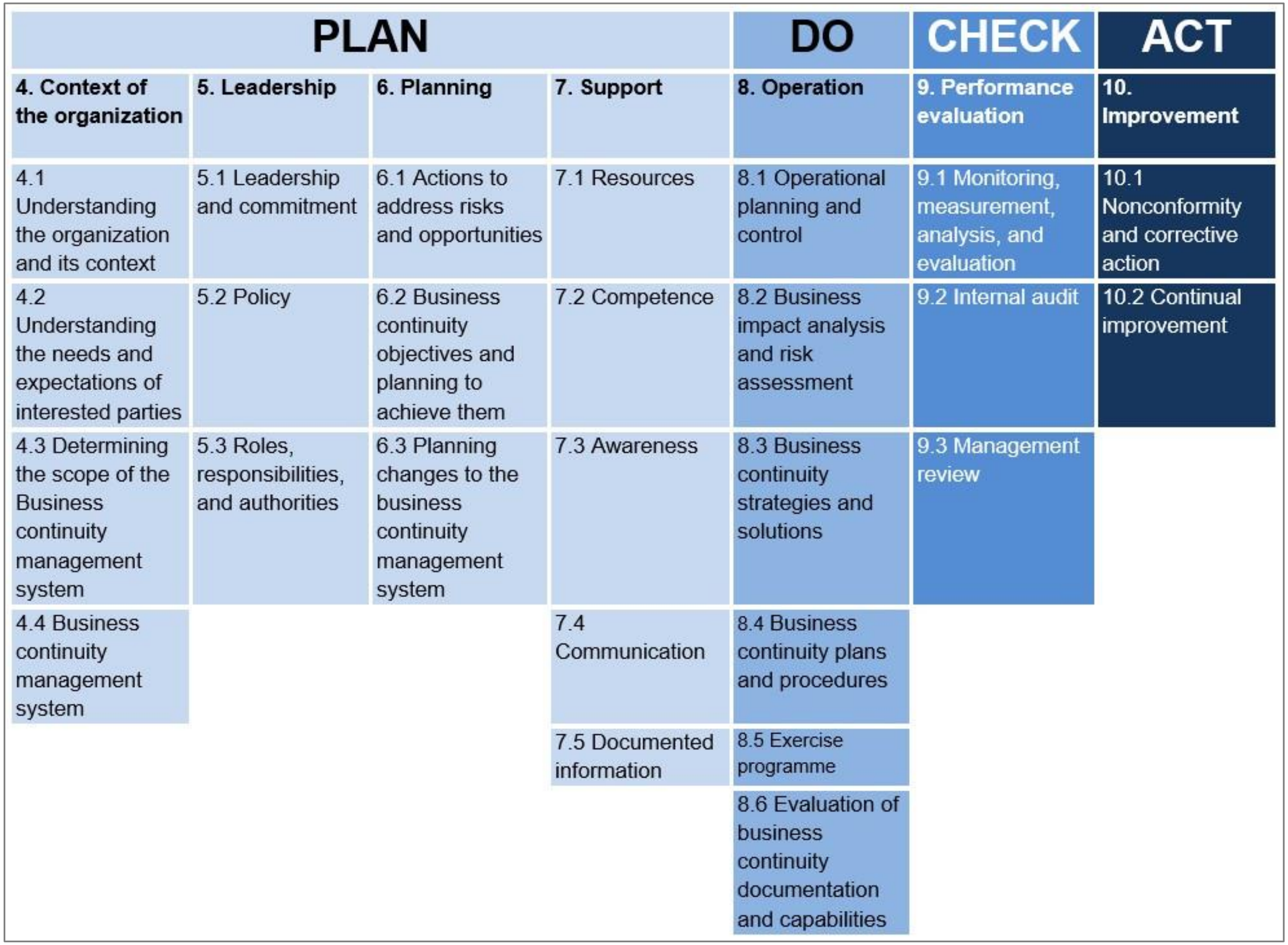


ISO 27001 CONTROLS

1. Information Security Policies
2. Organization of Information Security
3. Human Resource Security
4. Asset Management
5. Access Control
6. Cryptography
7. Physical and Environmental Security
8. Operations Security
9. Communications Security
10. System Acquisition and Maintenance
11. Supplier Relationships
12. Security Incident Management
13. Business Continuity Management
14. Compliance

ISO 22301 - BCMS

- **ISO 22301 - Business Continuity Management System**

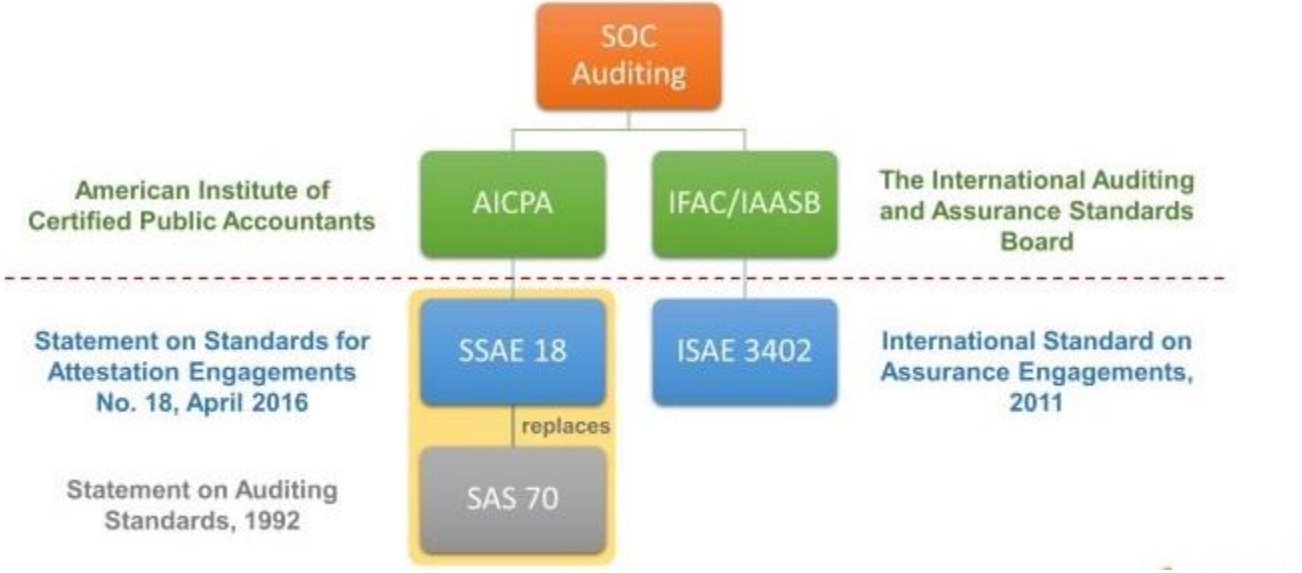


PLAN				DO	CHECK	ACT
4. Context of the organization	**5. Leadership**	**6. Planning**	**7. Support**	**8. Operation**	**9. Performance evaluation**	**10. Improvement**
4.1 Understanding the organization and its context	5.1 Leadership and commitment	6.1 Actions to address risks and opportunities	7.1 Resources	8.1 Operational planning and control	9.1 Monitoring, measurement, analysis, and evaluation	10.1 Nonconformity and corrective action
4.2 Understanding the needs and expectations of interested parties	5.2 Policy	6.2 Business continuity objectives and planning to achieve them	7.2 Competence	8.2 Business impact analysis and risk assessment	9.2 Internal audit	10.2 Continual improvement
4.3 Determining the scope of the Business continuity management system	5.3 Roles, responsibilities, and authorities	6.3 Planning changes to the business continuity management system	7.3 Awareness	8.3 Business continuity strategies and solutions	9.3 Management review	
4.4 Business continuity management system			7.4 Communication	8.4 Business continuity plans and procedures		
			7.5 Documented information	8.5 Exercise programme		
				8.6 Evaluation of business continuity documentation and capabilities		

OTHER FRAMEWORKS

ISAE 3402 & SSAE 18 [1/3]

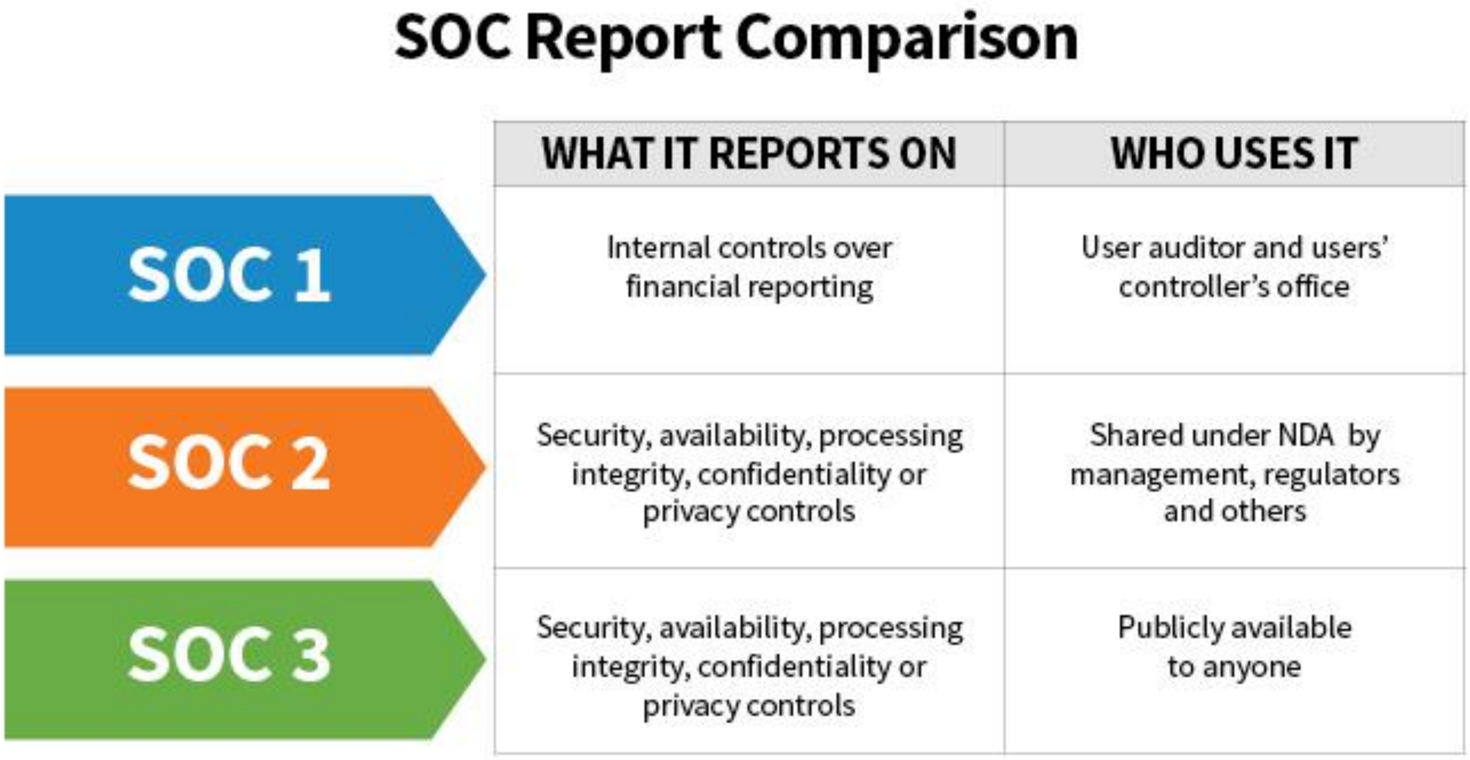
- **From SAS 70 to SSAE 18, ISAE 3402**


SOC Auditing
American Institute of Certified Public Accountants
AICPA
IFAC/IAASB
The International Auditing and Assurance Standards Board
Statement on Standards for Attestation Engagements No. 18, April 2016
SSAE 18
ISAE 3402
International Standard on Assurance Engagements, 2011
replaces
Statement on Auditing Standards, 1992
SAS 70

For more information, refer:
https://www.riskpro.in/content/soc-1-soc-2-ssae-18-audit-and-reporting-services

ISAE 3402 & SSAE 18 [2/3]

- **SOC Reports - Categories**



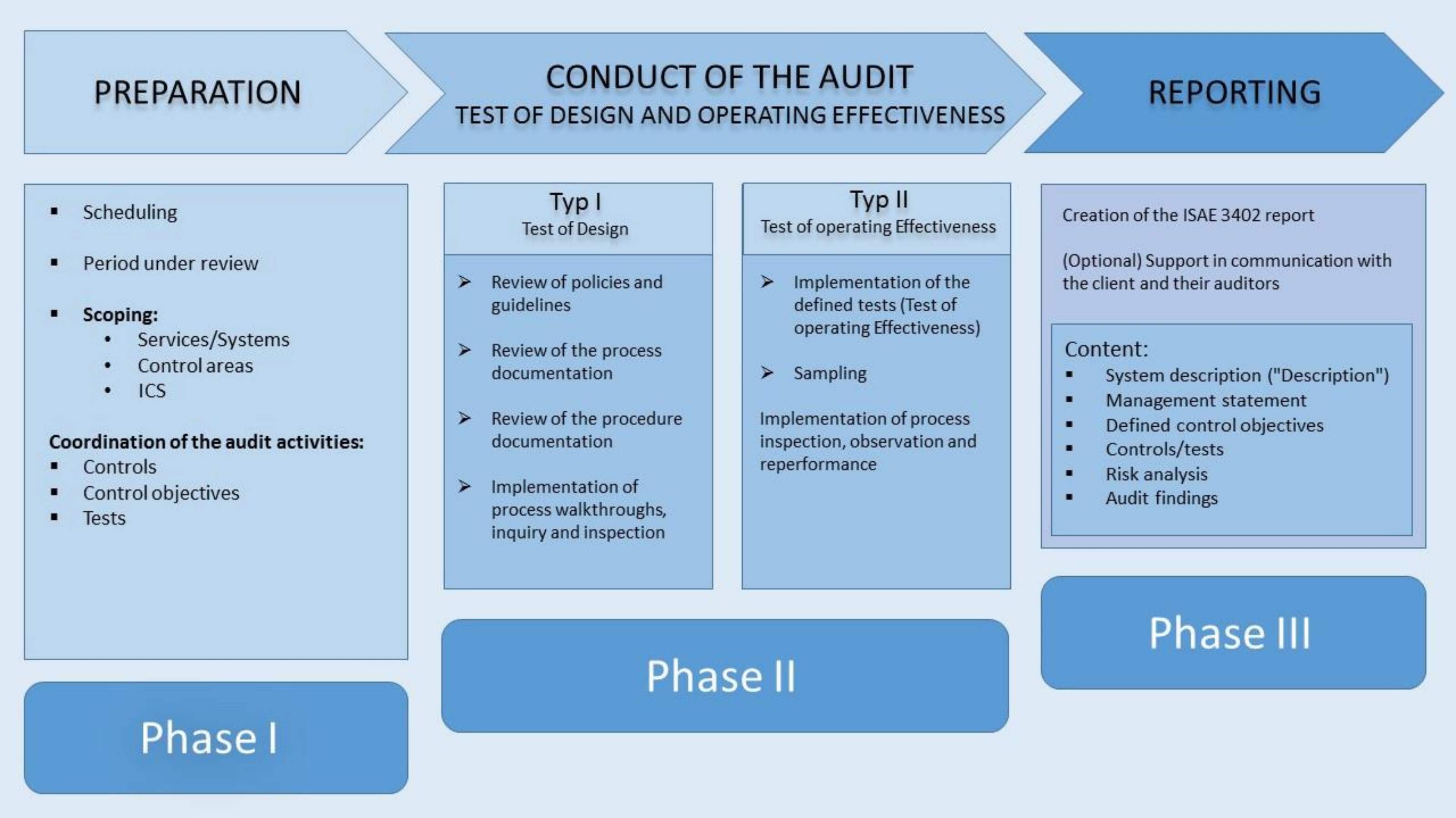
SOC Report Comparison

	WHAT IT REPORTS ON	WHO USES IT
SOC 1	Internal controls over financial reporting	User auditor and users' controller's office
SOC 2	Security, availability, processing integrity, confidentiality or privacy controls	Shared under NDA by management, regulators and others
SOC 3	Security, availability, processing integrity, confidentiality or privacy controls	Publicly available to anyone

For more information, refer:
https://www.riskpro.in/content/soc-1-soc-2-ssae-18-audit-and-reporting-services

ISAE 3402 & SSAE 18 [3/3]

- **Auditing and Reporting process, Type I & Type II Reports**



PREPARATION

CONDUCT OF THE AUDIT
TEST OF DESIGN AND OPERATING EFFECTIVENESS

REPORTING

- Scheduling
- Period under review
- **Scoping:**
  - Services/Systems
  - Control areas
  - ICS

Coordination of the audit activities:

- Controls
- Control objectives
- Tests

Phase I

Typ I
Test of Design

- Review of policies and guidelines
- Review of the process documentation
- Review of the procedure documentation
- Implementation of process walkthroughs, inquiry and inspection

Typ II
Test of operating Effectiveness

- Implementation of the defined tests (Test of operating Effectiveness)
- Sampling

Implementation of process inspection, observation and reperformance

Phase II

Creation of the ISAE 3402 report

(Optional) Support in communication with the client and their auditors

Content:

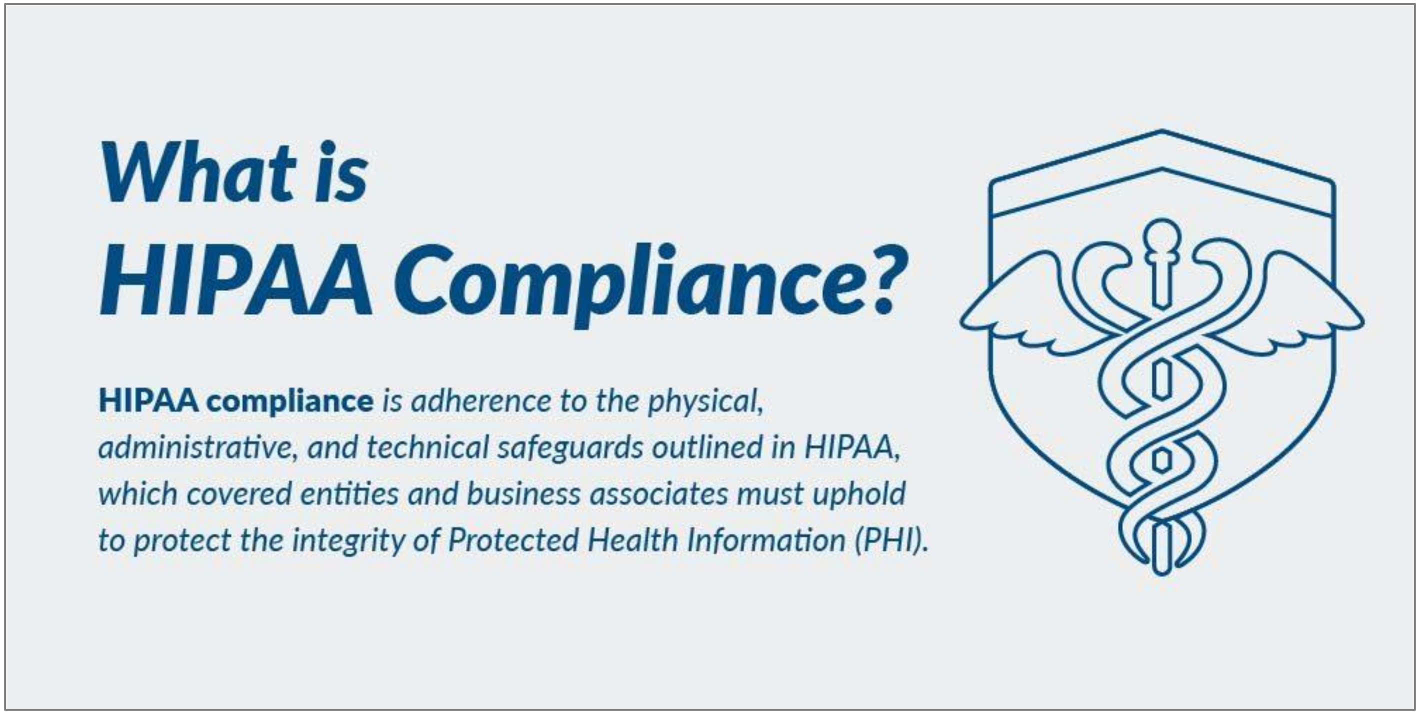
- System description ("Description")
- Management statement
- Defined control objectives
- Controls/tests
- Risk analysis
- Audit findings

Phase III

For more information, refer:
https://www.riskpro.in/content/soc-1-soc-2-ssae-18-audit-and-reporting-services

HIPAA [1/3]

- **HIPAA - Health Insurance Portability and Accountability Act, USA**



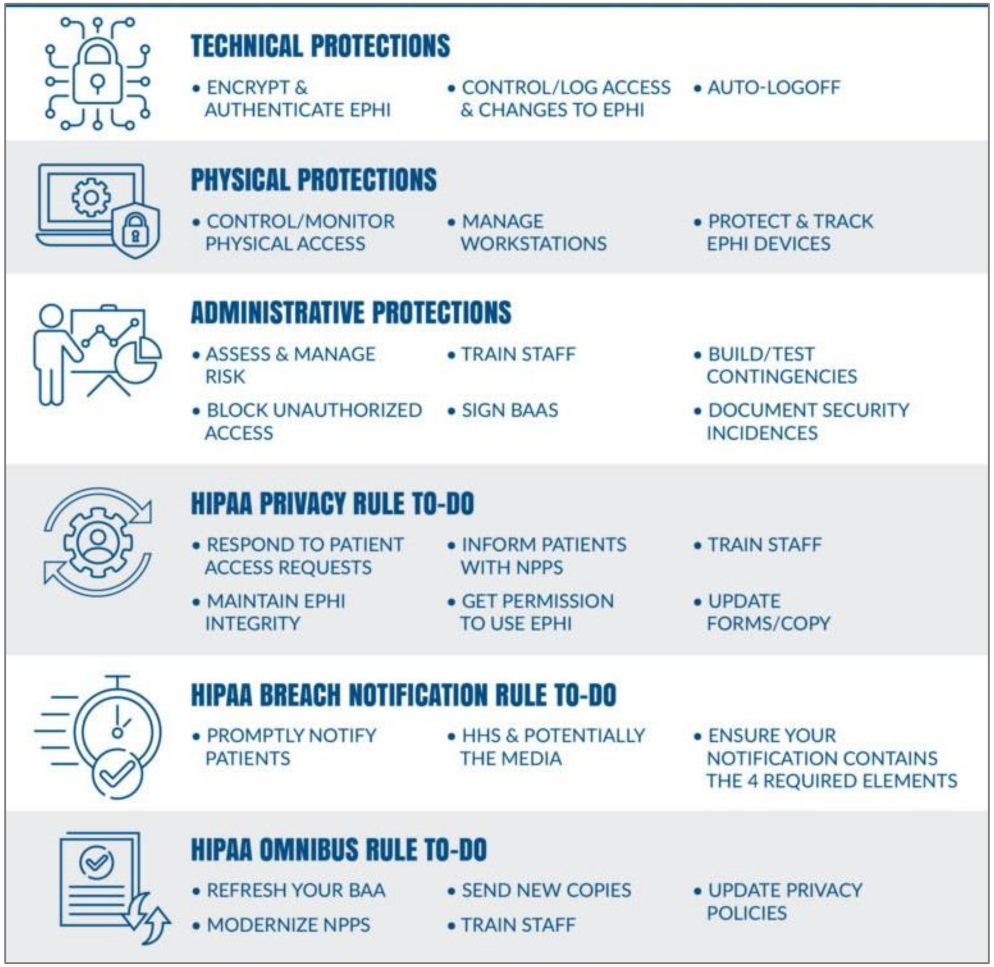
What is HIPAA Compliance?

HIPAA compliance *is adherence to the physical, administrative, and technical safeguards outlined in HIPAA, which covered entities and business associates must uphold to protect the integrity of Protected Health Information (PHI).*

For more information, refer:
https://www.riskpro.in/services/hipaa-compliance

HIPAA [2/3]

- **HIPAA - Physical, Administrative, and Technical safeguards**



TECHNICAL PROTECTIONS

- ENCRYPT & AUTHENTICATE EPHI
- CONTROL/LOG ACCESS & CHANGES TO EPHI
- AUTO-LOGOFF

PHYSICAL PROTECTIONS

- CONTROL/MONITOR PHYSICAL ACCESS
- MANAGE WORKSTATIONS
- PROTECT & TRACK EPHI DEVICES

ADMINISTRATIVE PROTECTIONS

- ASSESS & MANAGE RISK
- TRAIN STAFF
- BUILD/TEST CONTINGENCIES
- BLOCK UNAUTHORIZED ACCESS
- SIGN BAAS
- DOCUMENT SECURITY INCIDENCES

HIPAA PRIVACY RULE TO-DO

- RESPOND TO PATIENT ACCESS REQUESTS
- INFORM PATIENTS WITH NPPS
- TRAIN STAFF
- MAINTAIN EPHI INTEGRITY
- GET PERMISSION TO USE EPHI
- UPDATE FORMS/COPY

HIPAA BREACH NOTIFICATION RULE TO-DO

- PROMPTLY NOTIFY PATIENTS
- HHS & POTENTIALLY THE MEDIA
- ENSURE YOUR NOTIFICATION CONTAINS THE 4 REQUIRED ELEMENTS

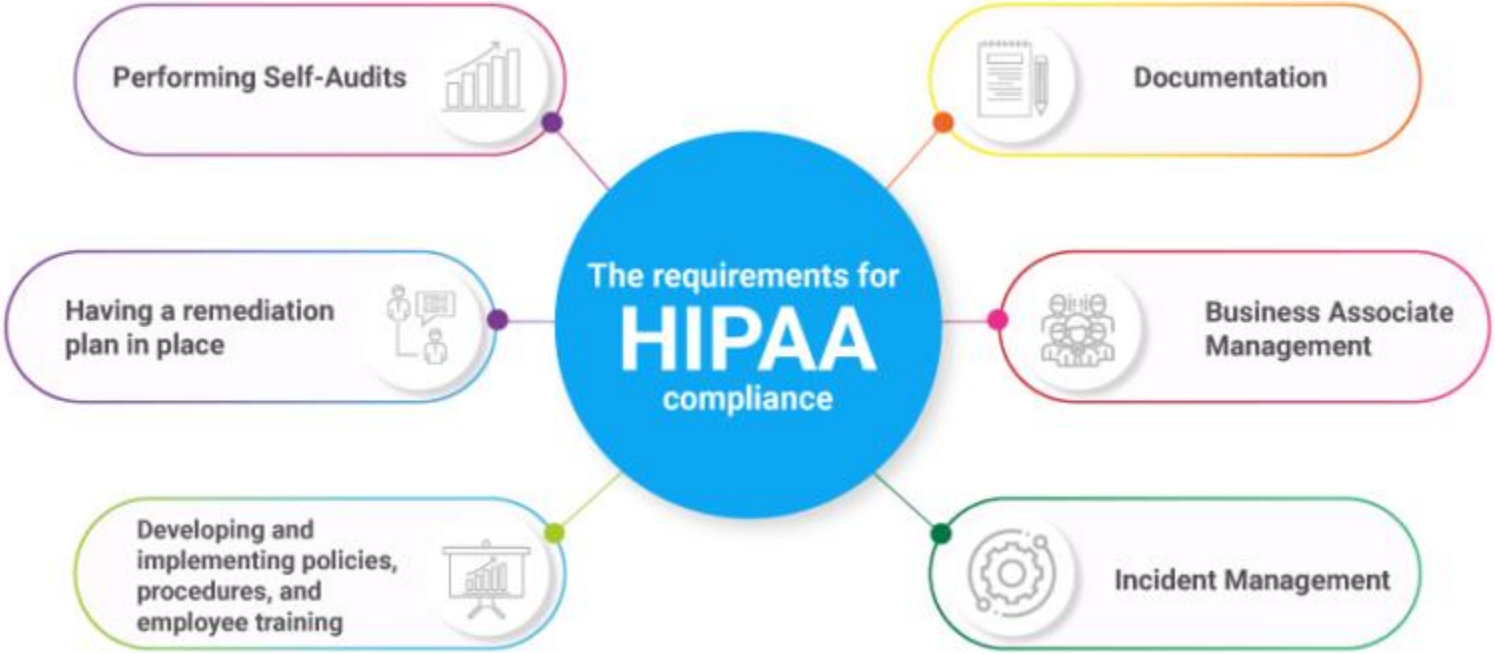
HIPAA OMNIBUS RULE TO-DO

- REFRESH YOUR BAA
- SEND NEW COPIES
- UPDATE PRIVACY POLICIES
- MODERNIZE NPPS
- TRAIN STAFF

For more information, refer:
https://www.riskpro.in/services/hipaa-compliance

HIPAA [3/3]

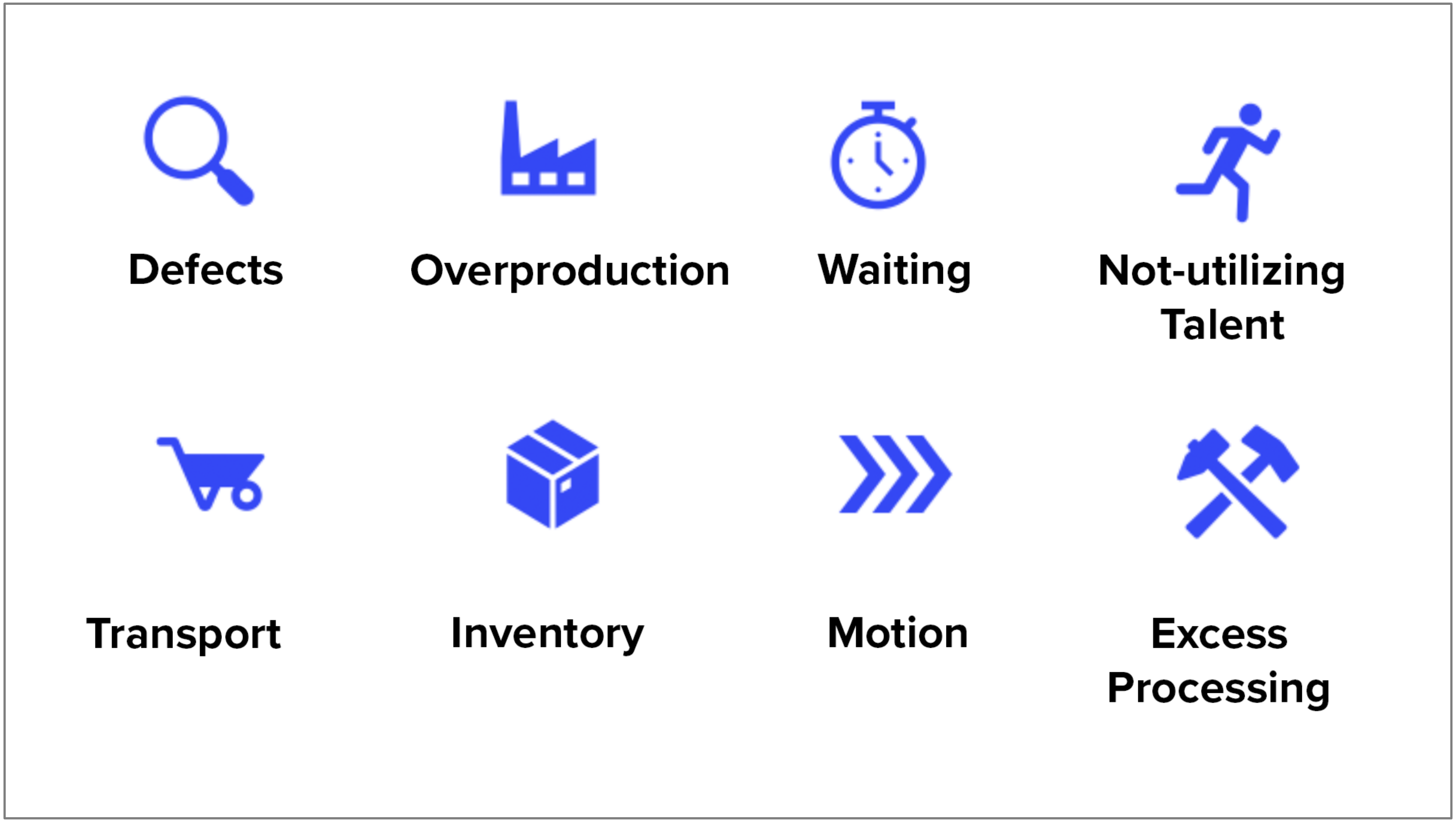
- **HIPAA - Compliance approach**


Performing Self-Audits
Documentation
Having a remediation plan in place
The requirements for HIPAA compliance
Business Associate Management
Developing and implementing policies, procedures, and employee training
Incident Management

For more information, refer:
https://www.riskpro.in/services/hipaa-compliance

IMPROVEMENT METHODOLOGIES

Lean Principles [1/2]



Defects

Overproduction

Waiting

Not-utilizing Talent

Transport

Inventory

Motion

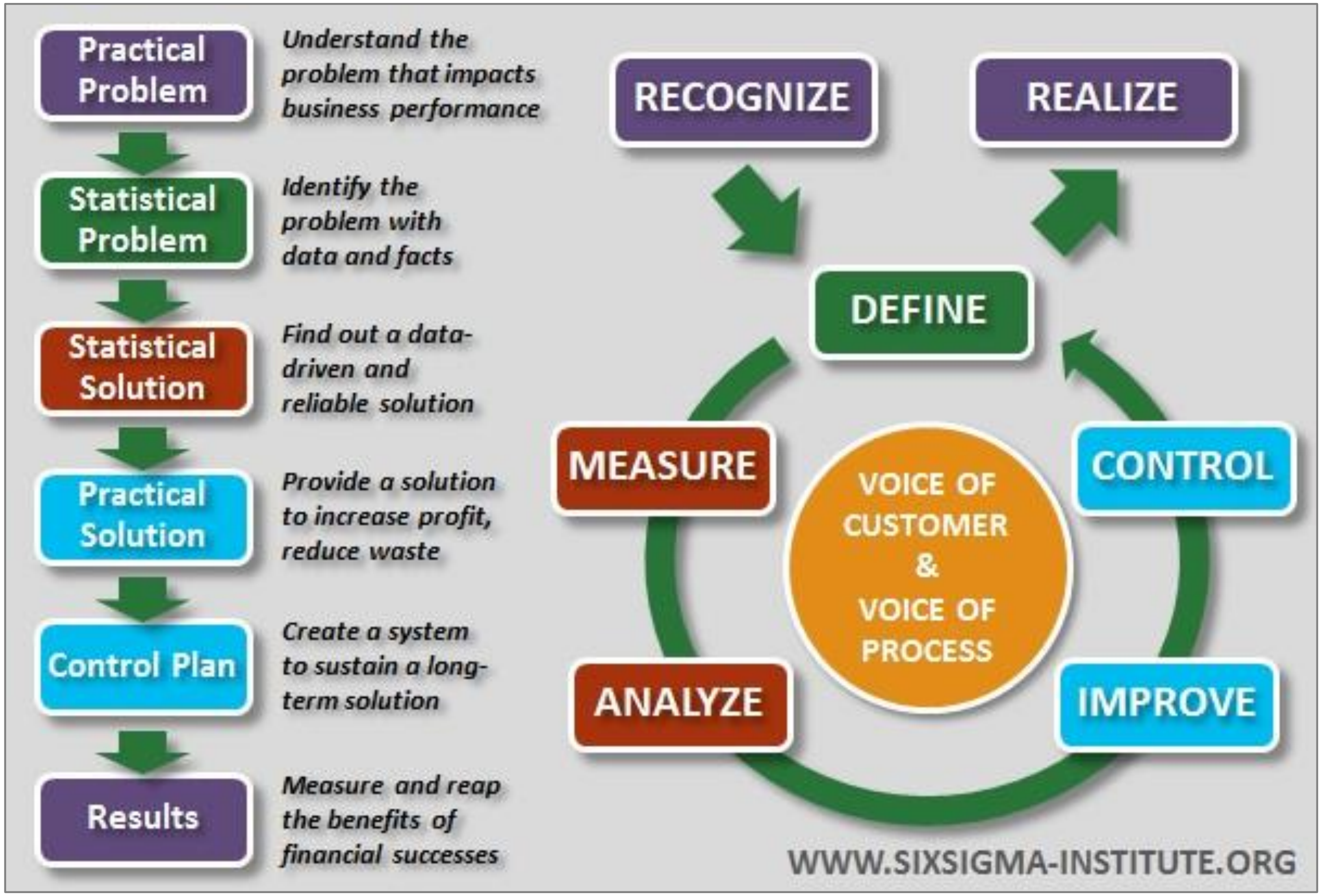
Excess Processing

Lean Principles [2/2]

Lean Waste Type	Scrum Waste	How to avoid this waste?
Defects	Defects not caught in reviews/testing, Rework	Target for defect detection, Preventing defect injection
Overproduction	Extra features, Features that no one uses, Over engineered solution	MMF, Test First Coding, Time Boxing
Waiting	Tools/resources not working, Waiting for information/work completion/decisions	Waiting is minimized in distributed agile/agile factory model
Not-utilizing Talent	Idle time of developers and testers, Under-utilization of available skills	Proactive capacity planning, Skill based allocation of developers and testers
Transport	Unnecessary discussion, clarifications, stakeholder management, too many mails	Daily standup meeting, Communication tools, Planned meetings
Inventory	Partially done, Not released for further activity	Mostly pushed to subsequent sprints when required
Motion	Handover, Searching for information manually when it can be automated	Daily build, continuous integration, automated testing, Use of tools
Excess-processing	Documentation/unused artifacts, Code that is not part of the final product, Unnecessary reviews	Minimal documentation, Refactoring of code, Reusability of the components, Test driven development

Six Sigma - DMAIC Methodology [1/2]

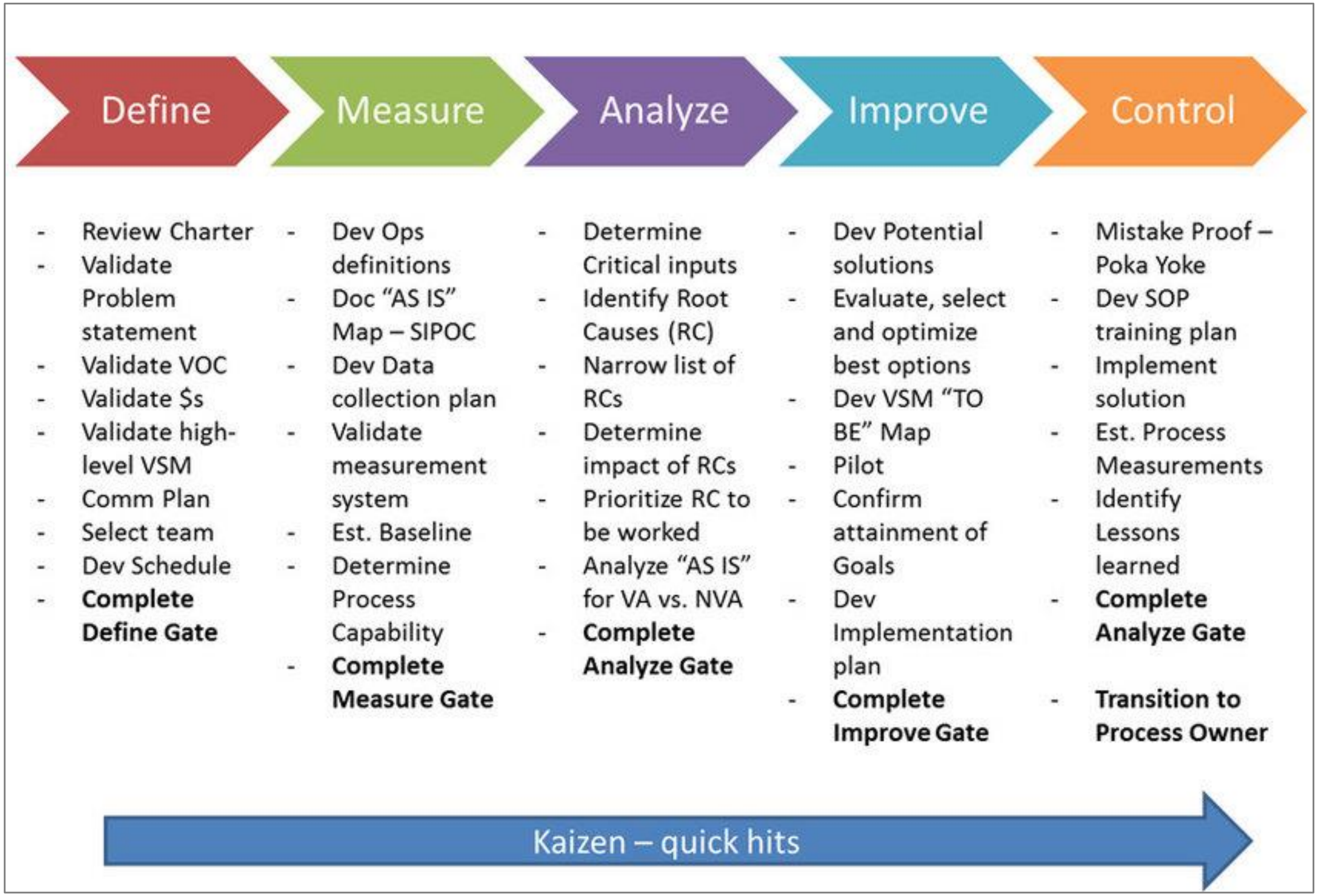
- **Define-Measure-Analyze-Improve-Control Methodology**



Practical Problem
Understand the problem that impacts business performance
Statistical Problem
Identify the problem with data and facts
Statistical Solution
Find out a data-driven and reliable solution
Practical Solution
Provide a solution to increase profit, reduce waste
Control Plan
Create a system to sustain a long-term solution
Results
Measure and reap the benefits of financial successes
RECOGNIZE
REALIZE
DEFINE
MEASURE
CONTROL
ANALYZE
IMPROVE
VOICE OF CUSTOMER & VOICE OF PROCESS
WWW.SIXSIGMA-INSTITUTE.ORG

Six Sigma - DMAIC Methodology [2/2]

- **Define-Measure-Analyze-Improve-Control Methodology (contd)**



Define

- Review Charter
- Validate Problem statement
- Validate VOC
- Validate $s
- Validate high-level VSM
- Comm Plan
- Select team
- Dev Schedule
- **Complete Define Gate**

Measure

- Dev Ops definitions
- Doc “AS IS” Map – SIPOC
- Dev Data collection plan
- Validate measurement system
- Est. Baseline
- Determine Process Capability
- **Complete Measure Gate**

Analyze

- Determine Critical inputs
- Identify Root Causes (RC)
- Narrow list of RCs
- Determine impact of RCs
- Prioritize RC to be worked
- Analyze “AS IS” for VA vs. NVA
- **Complete Analyze Gate**

Improve

- Dev Potential solutions
- Evaluate, select and optimize best options
- Dev VSM “TO BE” Map
- Pilot
- Confirm attainment of Goals
- Dev Implementation plan
- **Complete Improve Gate**

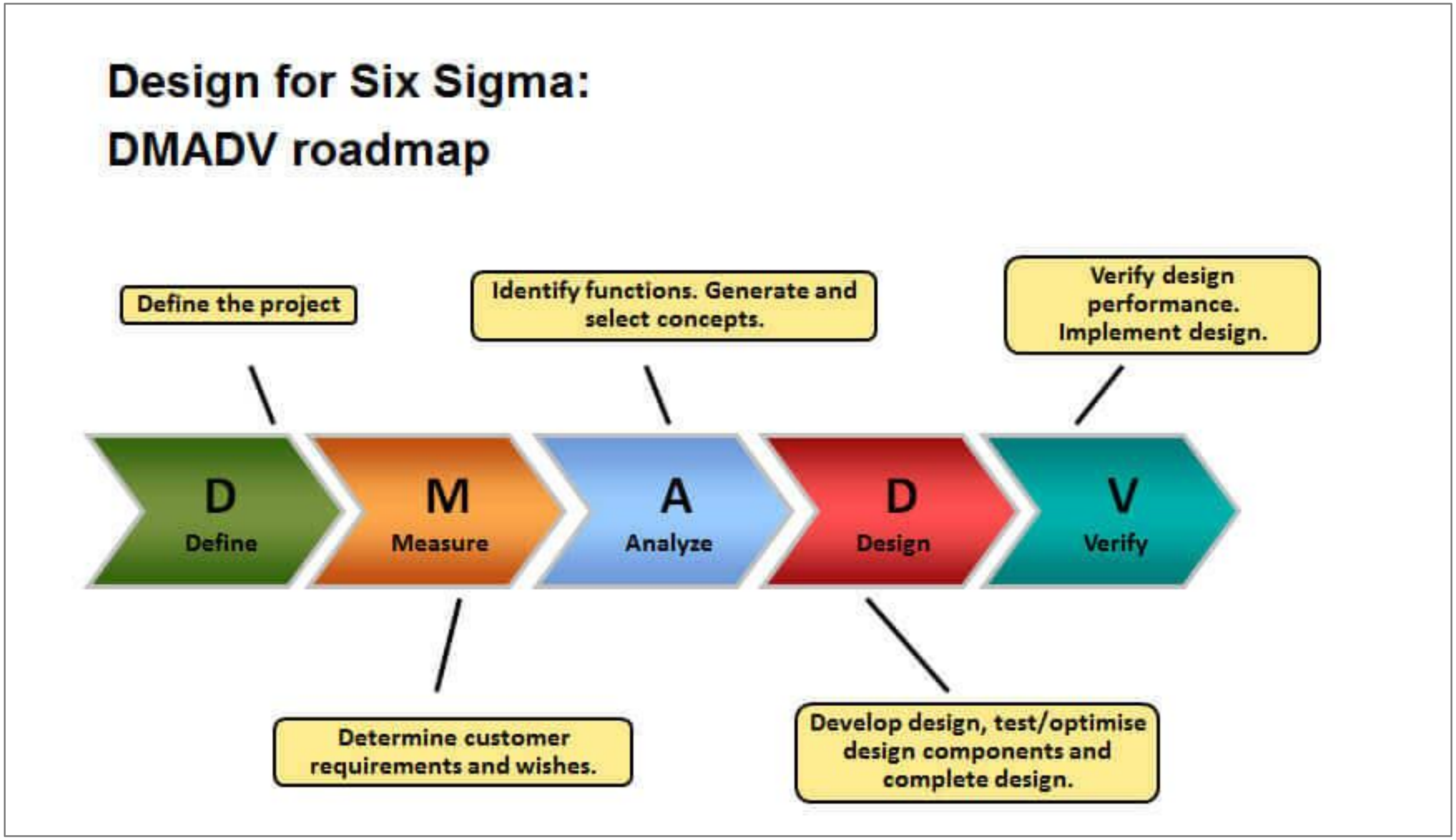
Control

- Mistake Proof – Poka Yoke
- Dev SOP training plan
- Implement solution
- Est. Process Measurements
- Identify Lessons learned
- **Complete Analyze Gate**
- **Transition to Process Owner**

Kaizen – quick hits

Six Sigma - DMADV Methodology

- **Define-Measure-Analyze-Design-Verify Methodology**



Design for Six Sigma:

DMADV roadmap

Define the project

Identify functions. Generate and select concepts.

Verify design performance. Implement design.

D Define

M Measure

A Analyze

D Design

V Verify

Determine customer requirements and wishes.

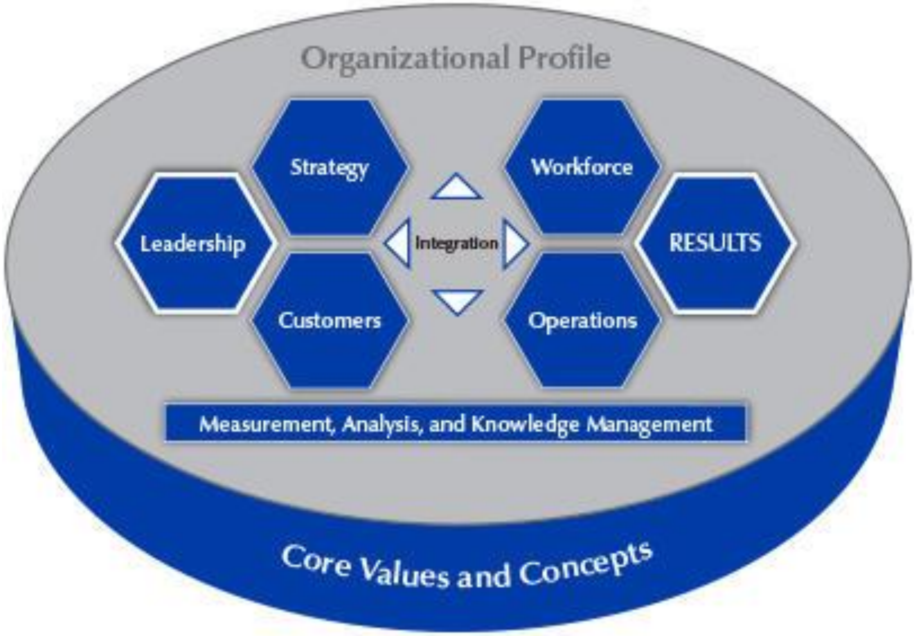
Develop design, test/optimise design components and complete design.

BUSINESS EXCELLENCE FRAMEWORKS

MBNQA

Malcolm Baldrige National Quality Award - Performance Excellence Award

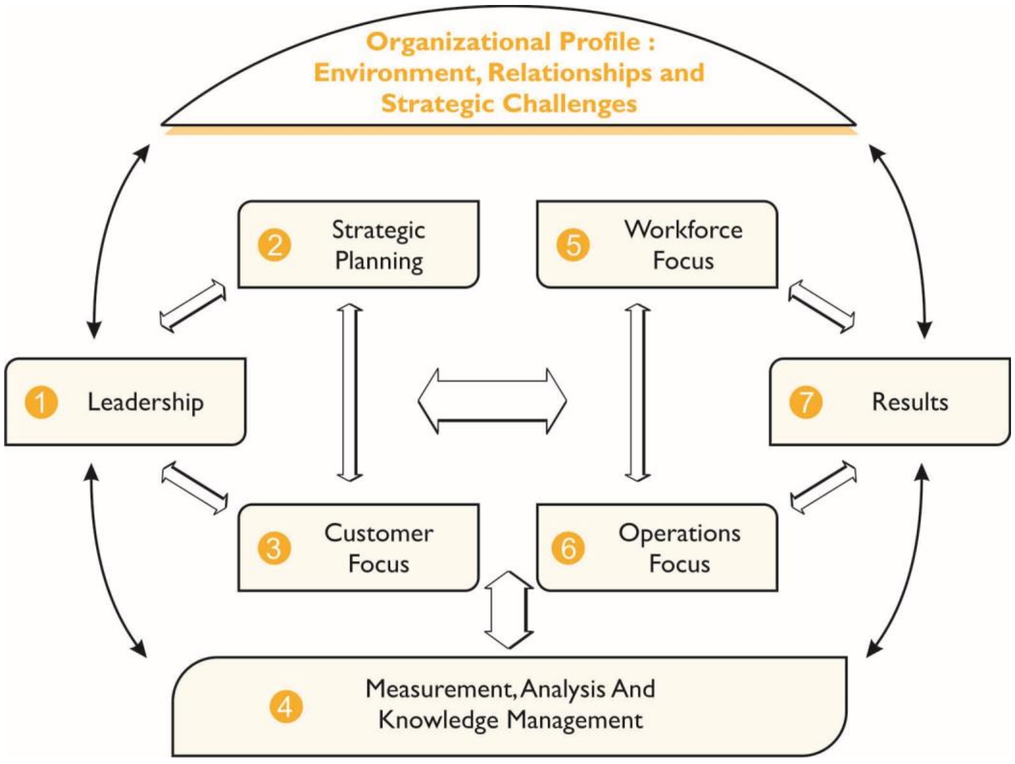
- An integrated approach to organizational performance management.
- Delivery of increasing value to customers and stakeholders, contributing to organizational sustainability.
- Improvement of overall organizational effectiveness and capabilities.
- Organizational and personal learning.
- The NIST, Department of Commerce, USA administers the award.



Reference:
https://www.nist.gov/baldrige

Ramkrishna Bajaj National Quality Award - Performance Excellence Award

- The IMC Ramkrishna Bajaj National Quality Award (IMC RBNQA) Trust to administer the Award with a purpose of spreading awareness for quality and fostering competitiveness in Indian Industry.



Reference:
http://imcrbnqa.com/index.html

BENEFITS OF PROCESS FRAMEWORKS

Benefits of Process Frameworks

Benefits of Process Frameworks

1. Discipline in execution of business processes.
2. Harmony of business processes and their interactions.
3. Removes person-dependency.
4. Predictability of outcomes.
5. Enables internal benchmarking.
6. Enables external benchmarking.
7. Improved customer satisfaction.
8. Improved quality and productivity.
9. Reduced cost.
10. Improved employee satisfaction.

TOP 10

BEST PRACTICES

Top 10 Best Practices for Implementation

Top 10 Best Practices for Implementation of Process Frameworks

1. ISO 9001 is the best to start with as a base framework.
2. When ISO 9001 is implemented, it is easy to achieve CMMI Level 3 by filling the gaps.
3. Adopt the motto of "simplify-standardize-automate".
4. Integrate the processes into day-to-day management of projects and services.
5. Encourage metrics based management of projects and services.
6. Focus on strong implementation of Measurement and Analysis at CMMI Level 2 for smooth implementation of Level 4 processes.
7. Leverage tools to the maximum.
8. Identify and mitigate risks for implementation early and effectively.
9. Be sensitive to the culture of the organization for successful change management.
10. Recognize and reward the champions.

Q & A

THANK YOU

RAMESH VENKATRAMAN

Associate Professor (Off-Campus) - Management Group

E-Mail: Ramesh.Venkatraman@pilani.bits-pilani.ac.in
Mob: +91-9176625725