hoonartek

Introduction to QMS, ISMS and BCMS standards

Liberating Data • Empowering People

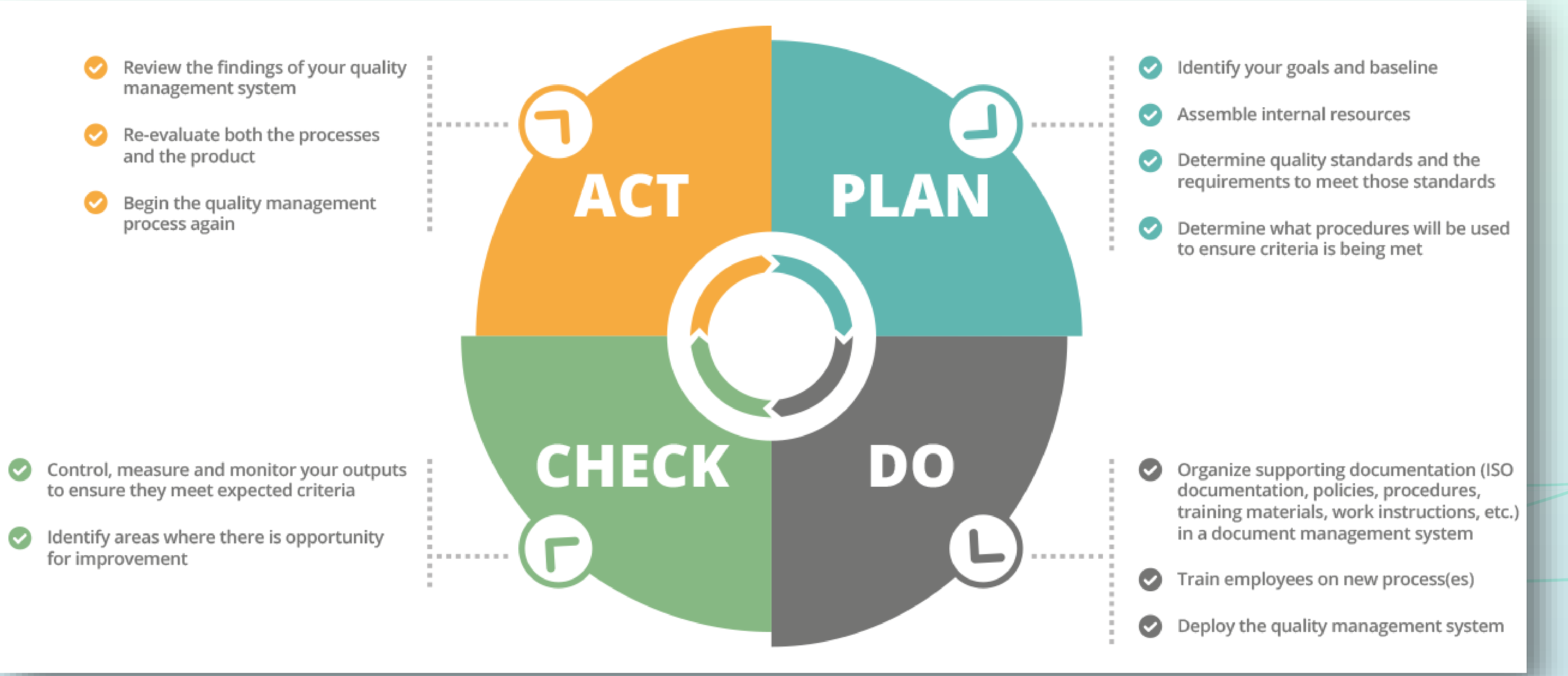
ISO 9001 I **ISO 27001** I **ISO 22301** I **ISO 31000** I IT SOC II Certified

Table of Content

Quality Management System (QMS - ISO 9001:2015)

A quality management system (QMS) is defined as a formalized system that documents processes, procedures, and responsibilities for achieving quality policies and objectives. A QMS helps coordinate and direct an organization’s activities to meet customer and regulatory requirements and improve its effectiveness and efficiency on a continuous basis.

ISO 9001:2015, the international standard specifying requirements for quality management systems, is the most prominent approach to quality management systems. While some use the term "QMS" to describe the ISO 9001 standard or the group of documents detailing the QMS, it refers to the entirety of the system.



ACT
- Review the findings of your quality management system
- Re-evaluate both the processes and the product
- Begin the quality management process again

PLAN
- Identify your goals and baseline
- Assemble internal resources
- Determine quality standards and the requirements to meet those standards
- Determine what procedures will be used to ensure criteria is being met

CHECK
- Control, measure and monitor your outputs to ensure they meet expected criteria
- Identify areas where there is opportunity for improvement

DO
- Organize supporting documentation (ISO documentation, policies, procedures, training materials, work instructions, etc.) in a document management system
- Train employees on new process(es)
- Deploy the quality management system

Benefits of QMS (ISO 9001:2015)

Implementing a quality management system affects every aspect of an organization's performance. Benefits of a documented quality management system include:

1. Meeting the customer’s requirements, which helps to instill confidence in the organization, in turn leading to more customers, more sales, and more repeat business.
2. Meeting the organization's requirements, which ensures compliance with regulations and provision of products and services in the most cost- and resource-efficient manner, creating room for expansion, and growth.

These benefits offer additional advantages, including:

I. Defining, improving, and controlling processes

II. Reducing waste

III. Preventing mistakes

IV. Lowering costs

V. Facilitating and identifying training opportunities

VI. Engaging Resources

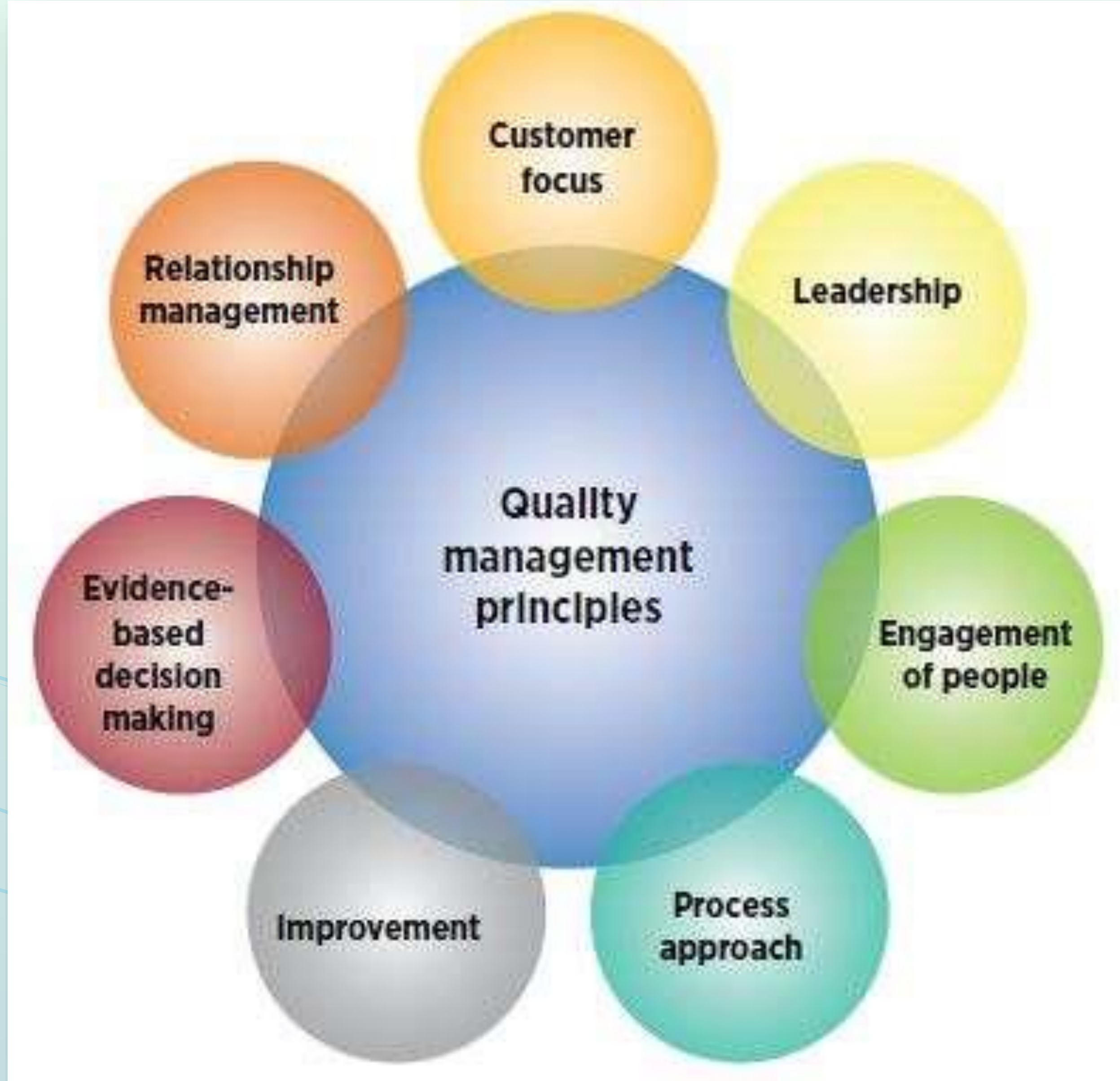
VII. Setting organization-wide direction

VIII. Communicating a readiness to produce consistent results

Elements of QMS (ISO 9001:2015)

Each element of a quality management system helps achieve the overall goals of meeting the customers' and organization's requirements. Quality management systems should address an organization's unique needs; however, the elements all systems have in common include -

1. The organization's quality policy and quality objectives
2. Quality manual
3. Procedures, instructions, and records
4. Data management
5. Internal processes
6. Customer satisfaction from product quality
7. Improvement opportunities
8. Quality analysis



Establishing and Implementing QMS (ISO 9001:2015)

- Before establishing a quality management system, HoonarTek has identified and managed various connected, multifunctional processes to help ensure customer satisfaction. The QMS design is influenced by Hoonartek' s objectives, needs, and products and services provided. This structure is based largely on the plan-do-check-act (PDCA) cycle and allows for continuous improvement to both the product and the QMS. The basic steps to implementing a quality management system are as follows:

1. **Design and Build** - The design and build portions serve to develop the structure of a QMS, its processes, and plans for implementation. This stage would include:-
   i. Requirement gathering and assessment
   ii. Creation of requirement traceability matrix (essential for Development and Testing)
   iii. Creation of Project Charter and SOW for the project
   iv. High Level Design of the solution
   v. Development Tasks (for the developer)
   vi. Unit Testing (performed by the developer)
   vii. Technical Review and Feedback (from Tech Lead)
   viii. Testing by the Quality Team (Testing in higher environments like QA and SIT)
   ix. Defect Lifecycle (Bugs resolved by the developer based on guidance from BA and Client Feedback)

Establishing and Implementing QMS (ISO 9001:2015)

2. **Deploy** - The deployment portions serve to develop the structure of a QMS, its processes, and plans for implementation. This stage would include:-
   I. Confirmation on Sanity of Code (performed by Developer) to the Platform Administrator and Project Manager.
   II. Risk Analysis of Code (by the Platform Administrator)
   III. Roll Back plan (in the event of Code Failure)
   IV. Sign off from the client for the Risk Analysis and Roll Back Plan
   V. Project Manager to ensure availability of Developer should the code fail and must be rolled back.
   VI. Failure Analysis (performed by Developer, Tech Lead and BA)
3. **Control and Measure** - Control and measurement are two areas of establishing a QMS that are largely accomplished through routine, systematic audits of the quality management system. The specifics vary greatly from organization to organization depending on size, potential risk, and environmental impact. This stage includes:-
   I. Efficient Defect Management - Quickest resolution of Defects found within the solution. (QA >> BA >> Developer)
   II. Defect Analysis using various methods (most popular – Pareto’s Analysis)
   III. Change Management (change requests in solution requested by the client)
   IV. Mitigation of Risks (identified during the project)
   V. Client Feedback (after successful deployments)

Establishing and Implementing QMS (ISO 9001:2015)

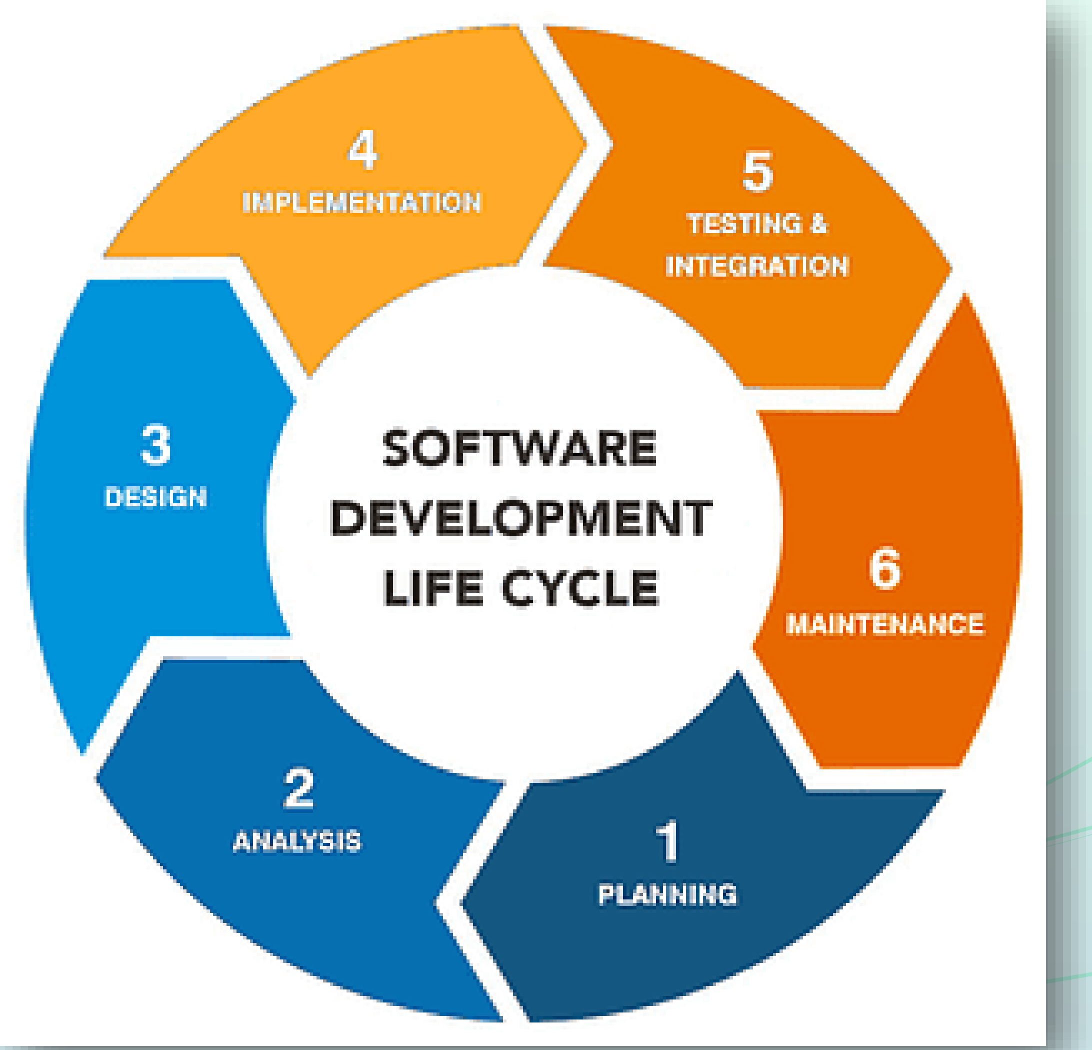
4. **Review and Improve** - Review and improve detail how the results of an audit are handled. The goals are to determine the effectiveness and efficiency of each process toward its objectives, to communicate these findings to the employees, and to develop new best practices and processes based on the data collected during the audit.

   I. Lessons Learned during the project

   II. Update and upgrades in Best Practices based on lessons learned.

Often Lessons learned by project teams are lost if they remain undocumented. Capturing Lessons learned at various stages of a project later becomes a valuable repository of knowledge not just for the project managers, delivery heads and top management but also for all team members working collectively.

As part of a continuous improvement at Hoonartek, Project Managers, Tech Leads, QA Teams, Members of the development teams are encouraged to document their experience on the project from time to time.



QMS (ISO 9001:2015) at Hoonartek

Hoonartek has always believed in providing high quality solutions to its clients. The quality goals set by Hoonartek are as below –

1. Quality improvement - Reduce defects in system during testing – Target <12%
2. Enhanced Customer Satisfaction – Reduce Customer Complaints – Target < 5 Complaints
3. On Time Project Deliveries – Target > 95%
4. Trainings – Conducting Training as per plan – Target 100%

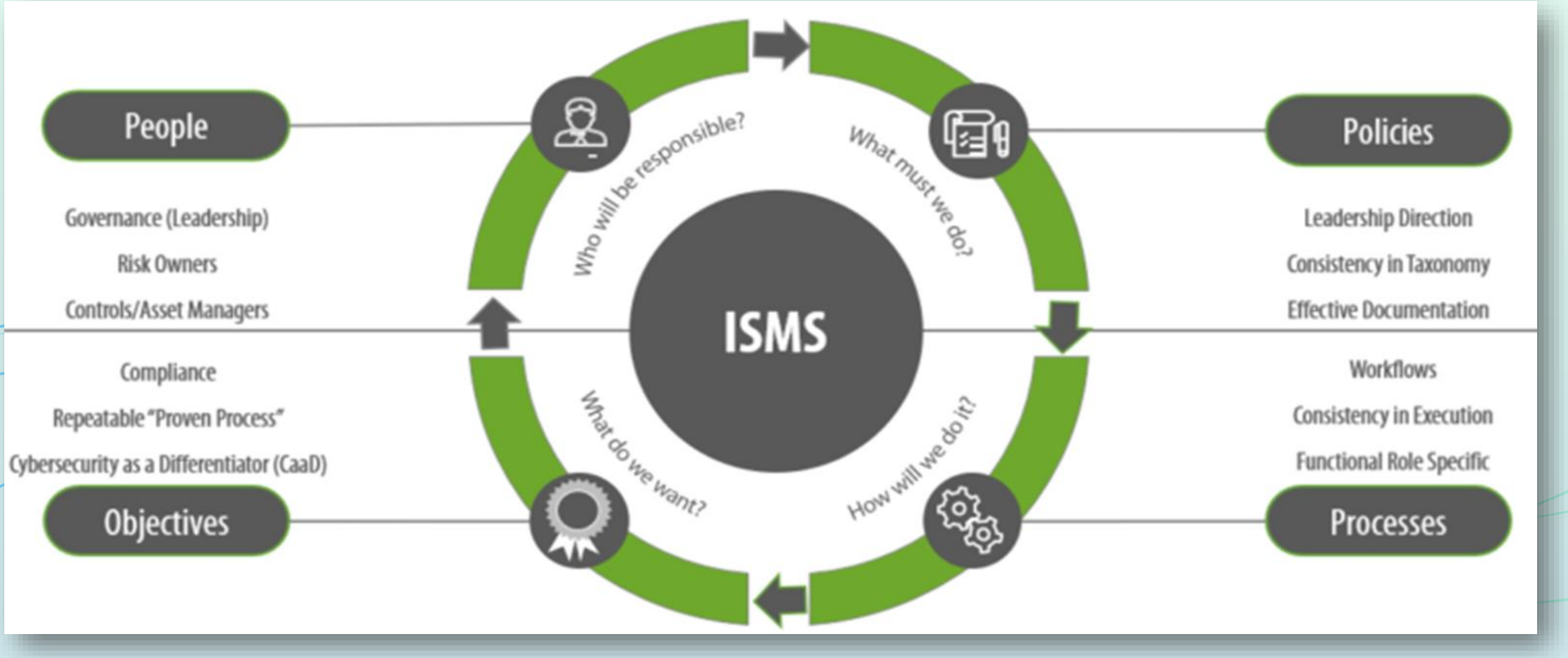
For creating Awareness -

1. Annual Mandatory Trainings for all Resources
2. Policy is used as screensavers on all laptops at Hoonartek for all users
3. Policy displayed on screens in reception areas

Information Security Management System (ISMS - ISO 27001:2022)

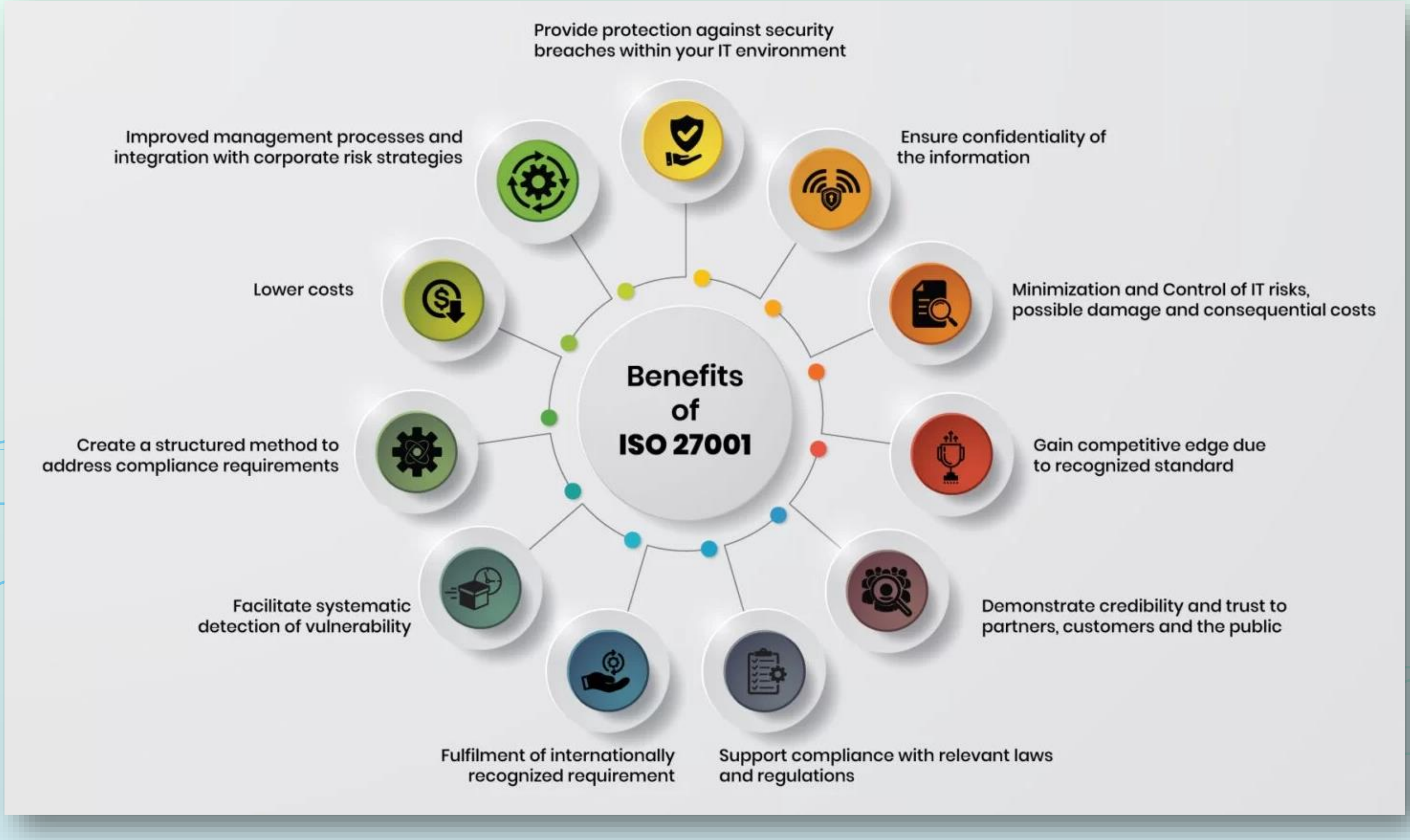
An information security management system (ISMS) is a framework of policies and controls that manage security and risks systematically and across an entire Organization's information security.

The framework for ISMS is usually focused on risk assessment and risk management. We can think of it as a structured approach to the balanced tradeoff between risk mitigation and the cost (risk) incurred.



Benefits of ISMS (ISO 27001:2022)

Information Security Management System is the international standard that provides the specification and requirements for implementing an ISMS which is a system of processes, documents, technology and people that helps to manage, monitor, audit and improve your organization's information security.


Benefits of ISO 27001
Provide protection against security breaches within your IT environment
Ensure confidentiality of the information
Minimization and Control of IT risks, possible damage and consequential costs
Gain competitive edge due to recognized standard
Demonstrate credibility and trust to partners, customers and the public
Support compliance with relevant laws and regulations
Fulfilment of internationally recognized requirement
Facilitate systematic detection of vulnerability
Create a structured method to address compliance requirements
Lower costs
Improved management processes and integration with corporate risk strategies

Elements of ISMS (ISO 27001:2022)

ISMS security controls span multiple domains of information security as specified in the ISO 27001 standard. However, the applicability of the specified controls in the standard is entirely based on the selection of the organization. Most prominent controls applied are as below –

1. **Information security policies** - An overall direction and support help establish appropriate security policies. The security policy is unique to an organization, devised in context to the changing business and security needs.
2. **Organization of information security** - This addresses threats and risks within the corporate network, including cyberattacks from external entities, inside threats, system malfunctions, and data loss.
3. **Asset management** - This component covers organizational assets within and beyond the corporate IT network., which may involve the exchange of sensitive business information.
4. **Human resource security** - Policies and controls pertaining to personnel, activities, and human errors, including measures to reduce risk from insider threats and workforce training to reduce unintentional security lapses.
5. **Physical and environmental security** - These guidelines cover security measures to protect physical IT hardware from damage, loss, or unauthorized access. While many organizations are taking advantage of digital transformation and maintaining sensitive information in secure cloud networks off-premise, security of physical devices used to access that information are to be considered.
6. **Communications and operations management** - Systems must be operated with respect and maintenance to security policies and controls. Daily IT operations, such as service provisioning and problem management, should follow IT security policies and ISMS controls.

Elements of ISMS (ISO 27001:2022)

7. **Access control** - This policy domain deals with limiting access to authorized personnel and monitoring network traffic for anomalous behavior. Access permissions relate to both digital and physical mediums of technology. The roles and responsibilities of individuals should be well defined, with access to business information available only when necessary.

8. **Information system acquisition, development, and maintenance** - Security best practices should be maintained across the entire lifecycle of the IT system, including the phases of acquisition, development, and maintenance.

9. **Information security and incident management** - Identify and resolve IT issues in ways that minimize the impact to end users. In complex network infrastructure environments, advanced technology solutions are required to identify insightful incident metrics and proactively mitigate potential issues.

10. **Cryptography** - Among the most important and effective controls to protect sensitive information, however this not being a complete solution in itself. Therefore, ISMS govern how cryptographic controls are enforced and managed.

11. **Supplier relationships** - Third-party vendors and business partners may require access to the network and sensitive customer data. It may not be possible to enforce security controls on some suppliers. However, adequate controls should be adopted to mitigate potential risks through IT security policies and contractual obligations.

ISMS (ISO 27001:2022) at Hoonartek

Hoonartek has implemented ISMS controls to protect its information assets against all internal, external, deliberate or accidental threats. –

Hoonartek will implement and have in place controls, processes, and mechanisms to ensure:

1. Information will be protected against any unauthorized access.
2. Confidentiality of information must be assured.
3. Integrity of information must be maintained.
4. The availability of information for business processes will be maintained.
5. Legislative and regulatory requirements will be met.
6. Information security training will be provided for all employees.
7. All actual or suspected information security breaches must be reported to the Chief Information Security Officer and will be thoroughly investigated.
8. The objectives will be monitored at regular frequency for continual improvement.

For Creating Awareness –

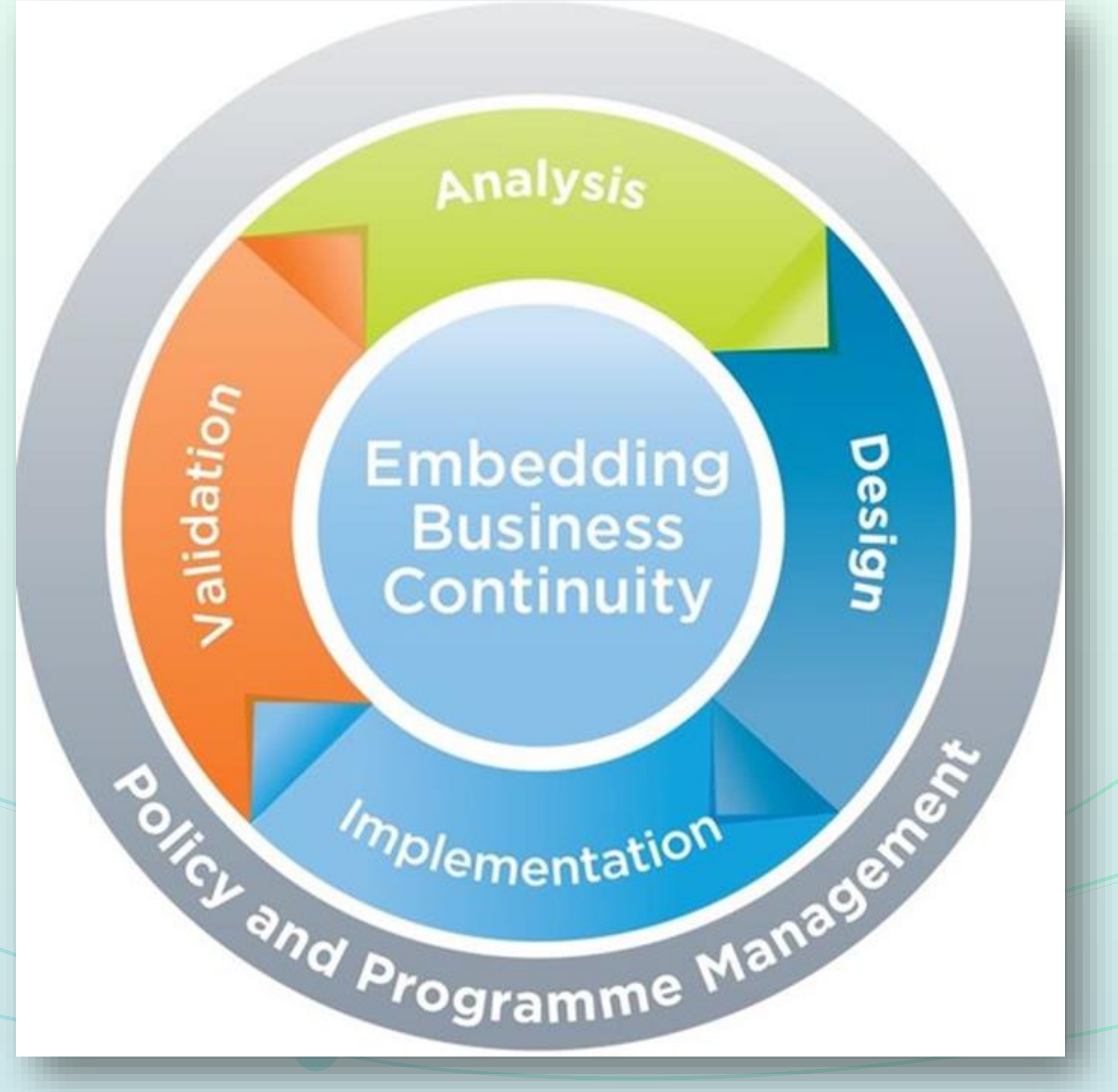
1. Annual Mandatory Trainings for all Resources
2. Policy is used as screensavers on all laptops at Hoonartek for all users
3. Policy displayed on screens in reception areas

Business Continuity Management System (BCMS - ISO 22301:2019)

BCMS is a set of interrelated elements that organizations use to establish, implement, operate, monitor, review, maintain, and improve their business continuity capabilities. These elements include -

1. People
2. Policies
3. Plans
4. Procedures
5. Processes
6. Structures
7. Resources

All these elements are used to ensure that operations continue, and products and services are delivered at predefined levels, the brands and value-creating activities are protected, and the reputations and interests of key stakeholders are safeguarded whenever disruptive incidents occur.


Analysis
Design
Implementation
Validation
Embedding Business Continuity
Policy and Programme Management

Benefits of BCMS (ISO 22301:2019)

BCMS is critical because it looks beyond dealing with the emergency itself. It considers what will be required to get the business up and running as soon as possible and keep it and its dependents working and contributing to the economy for the long term.

To make it work, stakeholders across the business and its value chain all must be involved: managers, process owners, strategic planners, project and procurement teams, key suppliers and directors all must be involved in managing risk. It goes much deeper than just preparing for a major event e.g., a flood, a terrorist attack but of preparing the business and its employees for anything.

1. Minimize the effect of a disruption on an organization
2. Reduce the risk of human and financial loss.
3. Retain company image and give staff, clients and suppliers confidence in the organization's services.
4. Enable the recovery of critical systems within an agreed timeframe.
5. Meet legal and statutory obligations.

Elements of BCMS (ISO 22301:2019)

The key elements for BCMS are as below –

1. **Business Impact Analysis** – Identify the critical activities and resources required to support the business during a disruption.
2. **Risk Assessment** – Identify threats and vulnerabilities of its critical business functions and resources needed to support the client's SLA.
3. **Business Continuity Strategy** – A conceptual summary of preventive (mitigation) strategies, crisis response strategies and recovery strategies that must be carried out between the occurrence of a disaster and the time when normal operations are restored. The strategy should always be relevant to the project's / function's Business Impact Analysis.
   a) **Establish Resource Requirements** – A strategy will include details of resources to be considered while implementing a continuity strategy for various disruptive scenarios. These will include people, IT applications, systems and infrastructure, Critical Non-IT infrastructure as facilities, equipment and consumables, Vital records, transportation, finance and suppliers.
   b) **Incident Response Plan** – A conceptual plan on how should the team members respond and communicate while facing any disruptive event based on their assigned duties and responsibilities within the team.
4. **Business Continuity Plans** – Establish mitigation plans to manage and minimize the impact of a disruptive event on the business ensuring continuity of critical activities. The BC Plans must be aligned to the Risks identified while performing Risk Assessment for the project / function.
5. **Business Recovery Plans** – A summary on how to proceed with restoration of business operations after a disruptive event. This will include all IT and Non-IT critical functions, systems and infrastructure, equipment and consumables, finance and supplier chains. The Recovery Plans should always be based on the recovery of activities identified under the Business Impact Analysis for the project / function.

BCMS (ISO 22301:2019) at Hoonartek

Hoonartek has implemented BSMS controls to protect its resources, assets against all internal, external, deliberate or accidental threats –

1. Minimizing disruptions and loss of customer business.
2. Strive to continuously meet customer requirements.
3. Protection of company assets.
4. Mitigating Service Level, Contractual, Financial, Reputational, Legal & Regulatory and Health & Safety loss.
5. Health and safety of its personnel and other stake holders before, during and after an event.

For Creating Awareness –

1. Annual Mandatory Trainings for all Resources
2. Policy is used as screensavers on all laptops at Hoonartek for all users
3. Policy displayed on screens in reception areas

Your Responsibility – QMS (ISO 9001:2015)

1. Closely monitors defects found in the system to minimize defects within the solution
2. Actively follows up with the client to gauge their satisfaction levels after planned deliveries
3. Emphasizes on quick resolution to any client complaints raised, also have a root cause analysis done for the complaint and use it as a lessons learned to avoid repetition of such mistakes.
4. Projects are internally audited frequently to ensure compliance to the set QMS standard by Hoonartek

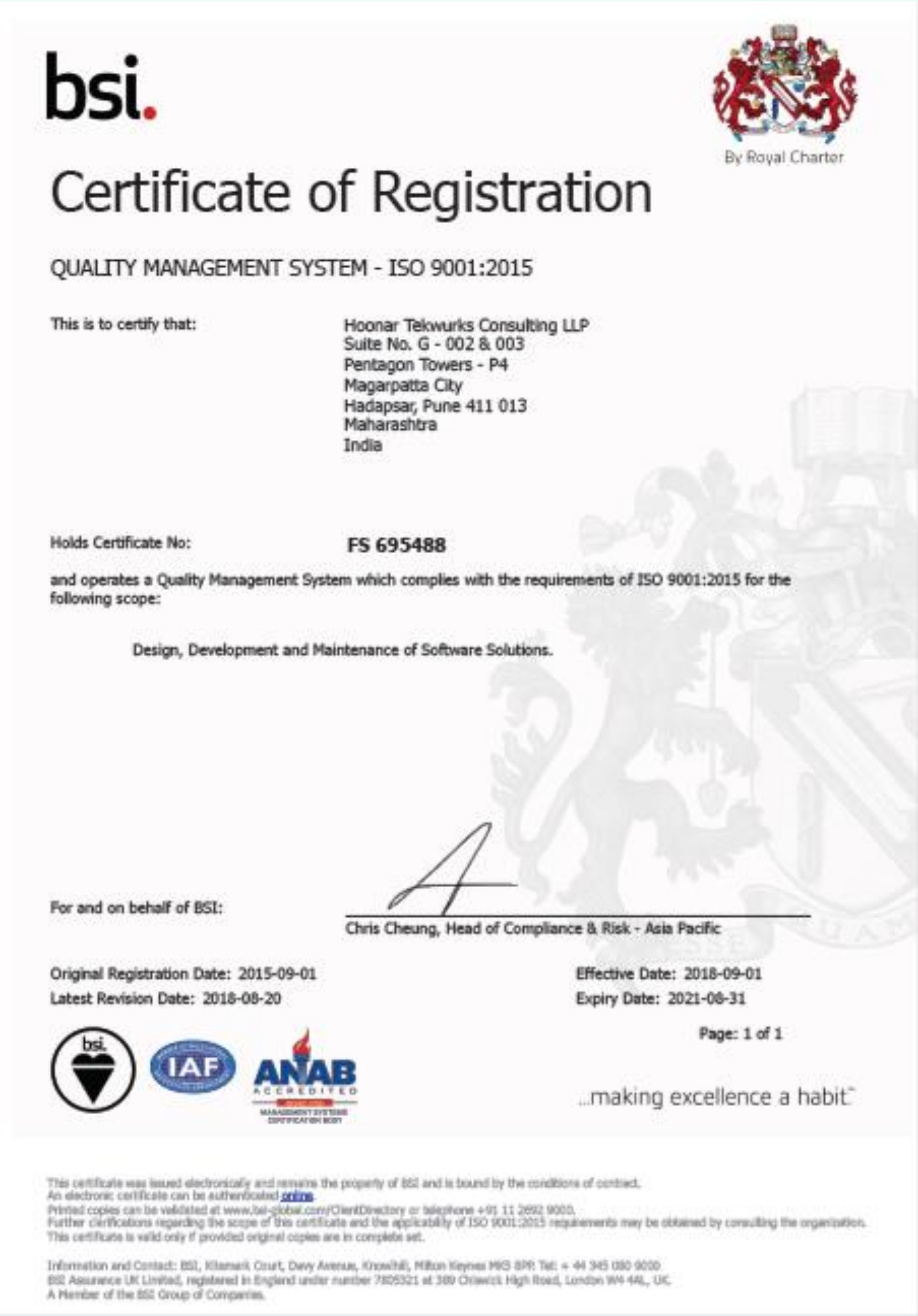
Your Responsibility – ISMS (ISO 27001:2022)

1. Have designated Project operations areas with restricted accesses to unauthorized personnel.
2. Ensures awareness amongst project team members on information security policies followed at Hoonartek.
3. Show Zero tolerance to credentials and password sharing, saving any client data on private drives etc.
4. Discourage shoulder surfing while working on client data.
5. Implement and follow clean desk and clear desktop policy.
6. Be vigilant, refrain from responding to spam messages from imposters posing as members from Hoonartek Senior Management. Always check with IT Helpdesk in such instances.
7. While using your cellphones, always follow the guidelines as per the acceptable use of cellphones on premises policy of Hoonartek.
8. Use of personal devices (laptops) while on Hoonartek premises is strictly prohibited which will result in a disciplinary action against the resource.
9. All actual or suspected information security breaches are reported to Information Security Manager and are thoroughly investigated followed by Disciplinary action if found guilty.
10. Projects are internally audited frequently to ensure compliance to the set ISMS standard by Hoonartek.

Your Responsibility – BCMS (ISO 22301:2019)

1. Ensures awareness amongst project team members on business continuity policies followed at Hoonartek.
2. Create Business continuity strategies based on business impact analysis and risk analysis to ensure protection of resources along with ways to minimize impact on business operations during any disruptive event.
3. Create mitigation plans at project level and involve team members in the testing of disruptive scenarios to gauge the preparedness and success levels of the documented plan.
4. Draw up learnings and shortfall analysis to overcome delayed responses and avoid confusions.
5. Projects are internally audited frequently to ensure compliance to the set BCMS standard by Hoonartek.

ISO Certifications of Hoonartek



By Royal Charter

Certificate of Registration

QUALITY MANAGEMENT SYSTEM - ISO 9001:2015

This is to certify that: Hoonar Tekwurks Consulting LLP
Suite No. G - 002 & 003
Pentagon Towers - P4
Magarpatta City
Hadapsar, Pune 411 013
Maharashtra
India

Holds Certificate No: FS 695488

and operates a Quality Management System which complies with the requirements of ISO 9001:2015 for the following scope:

Design, Development and Maintenance of Software Solutions.

For and on behalf of BSI: Chris Cheung, Head of Compliance & Risk - Asia Pacific

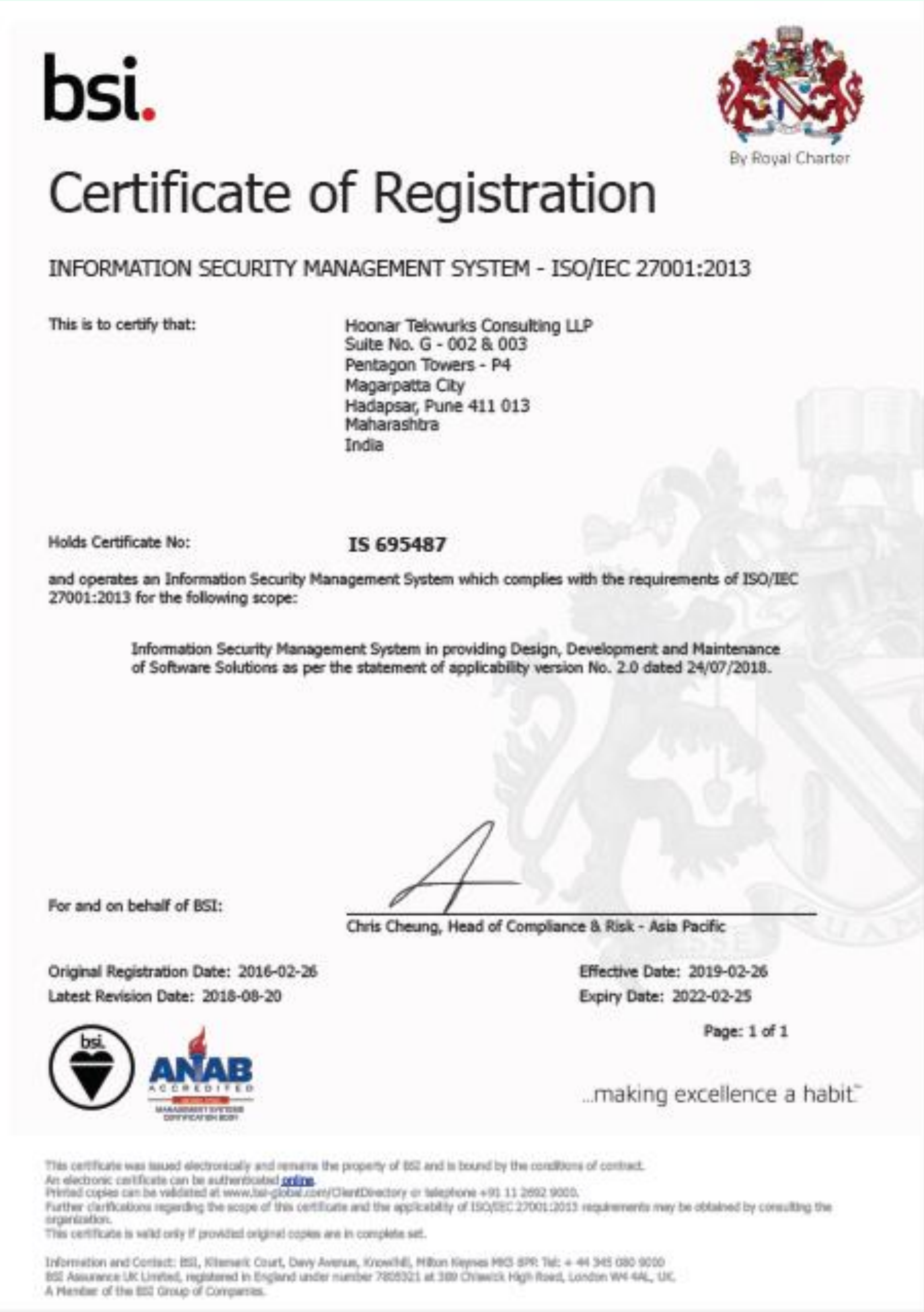
Original Registration Date: 2015-09-01
Latest Revision Date: 2018-08-20
Effective Date: 2018-09-01
Expiry Date: 2021-08-31

Page: 1 of 1

...making excellence a habit™

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsi-global.com/ClientDirectory or telephone +91 11 2692 9000.
Further clarifications regarding the scope of this certificate and the applicability of ISO 9001:2015 requirements may be obtained by consulting the organization.
This certificate is valid only if provided original copies are in complete set.

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.



By Royal Charter

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that: Hoonar Tekwurks Consulting LLP
Suite No. G - 002 & 003
Pentagon Towers - P4
Magarpatta City
Hadapsar, Pune 411 013
Maharashtra
India

Holds Certificate No: IS 695487

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

Information Security Management System in providing Design, Development and Maintenance of Software Solutions as per the statement of applicability version No. 2.0 dated 24/07/2018.

For and on behalf of BSI: Chris Cheung, Head of Compliance & Risk - Asia Pacific

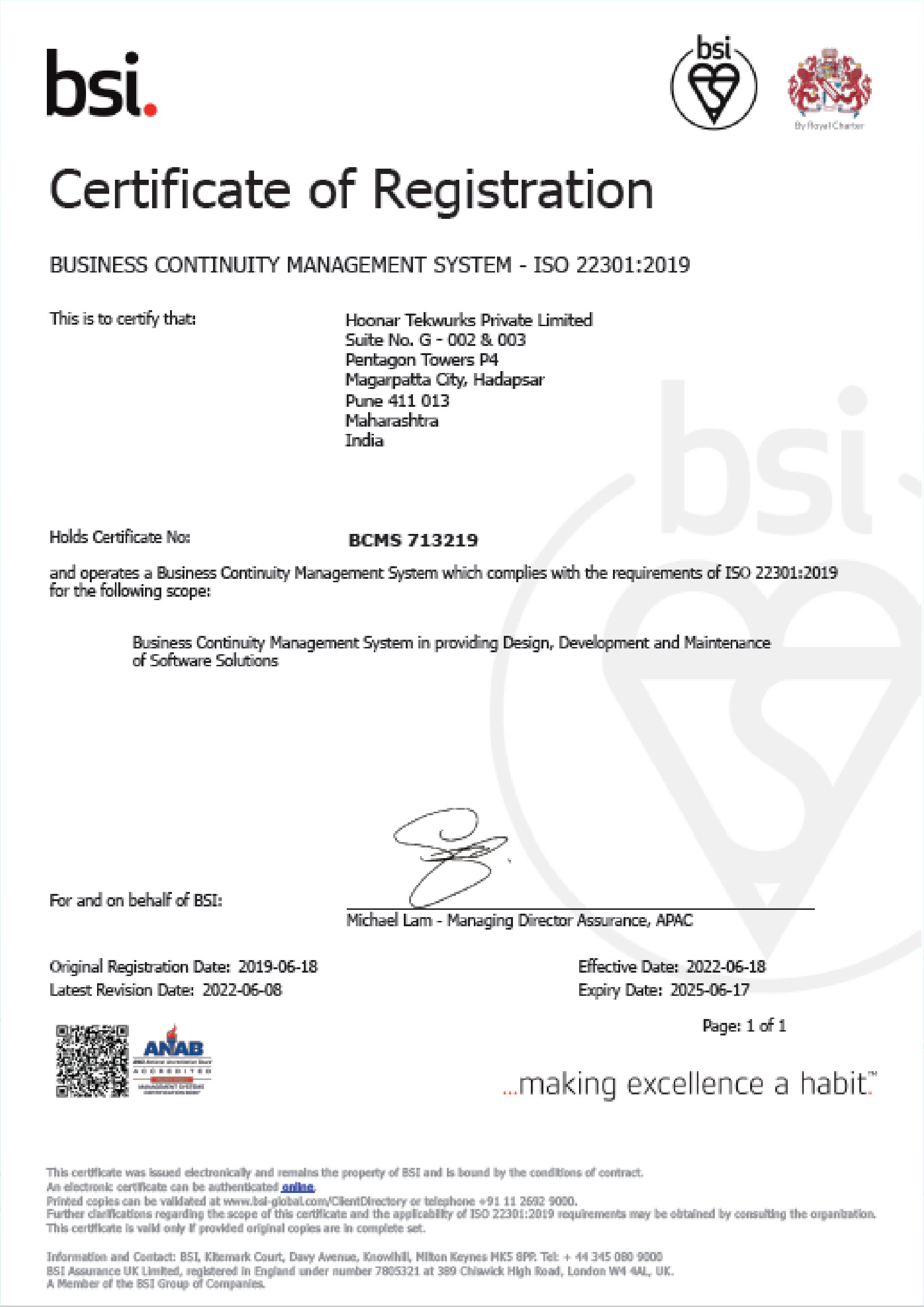
Original Registration Date: 2016-02-26
Latest Revision Date: 2018-08-20
Effective Date: 2019-02-26
Expiry Date: 2022-02-25

Page: 1 of 1

...making excellence a habit™

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsi-global.com/ClientDirectory or telephone +91 11 2692 9000.
Further clarifications regarding the scope of this certificate and the applicability of ISO/IEC 27001:2013 requirements may be obtained by consulting the organization.
This certificate is valid only if provided original copies are in complete set.

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.



By Royal Charter

Certificate of Registration

BUSINESS CONTINUITY MANAGEMENT SYSTEM - ISO 22301:2019

This is to certify that: Hoonar Tekwurks Private Limited
Suite No. G - 002 & 003
Pentagon Towers P4
Magarpatta City, Hadapsar
Pune 411 013
Maharashtra
India

Holds Certificate No: BCMS 713219

and operates a Business Continuity Management System which complies with the requirements of ISO 22301:2019 for the following scope:

Business Continuity Management System in providing Design, Development and Maintenance of Software Solutions

For and on behalf of BSI: Michael Lam - Managing Director Assurance, APAC

Original Registration Date: 2019-06-18
Latest Revision Date: 2022-06-08
Effective Date: 2022-06-18
Expiry Date: 2025-06-17

Page: 1 of 1

...making excellence a habit.™

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsi-global.com/ClientDirectory or telephone +91 11 2692 9000.
Further clarifications regarding the scope of this certificate and the applicability of ISO 22301:2019 requirements may be obtained by consulting the organization.
This certificate is valid only if provided original copies are in complete set.

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.

hoonartek

Thank you!

Hoonartek is the world's leading data solutions company. Founded in 2010, we've helped more than 200 enterprises successfully leverage data and insights to drive transformation, create innovative business models, and generate new monetisation avenues. Hoonartek's three offerings – data products and monetisation, digital banking and lending, and digital engineering – make Hoonartek a partner of choice for businesses in BFSI, Telecom, ISVs, Healthcare and Manufacturing. With headquarters in Pune, India, we are present in the US, UK and Europe. We proudly serve Korn Ferry, ASI, L&T, Experian, NSE, IDFC, and Airtel to name a few.

To learn more, visit www.hoonartek.com | in 🐦 f