IT Governance for SME

This IT Governance framework is tailored for the application within small and medium-sized enterprises. The main purpose of the framework is to improve IT governance activities within small and medium-sized enterprises by providing a generic framework including implementation guidance.

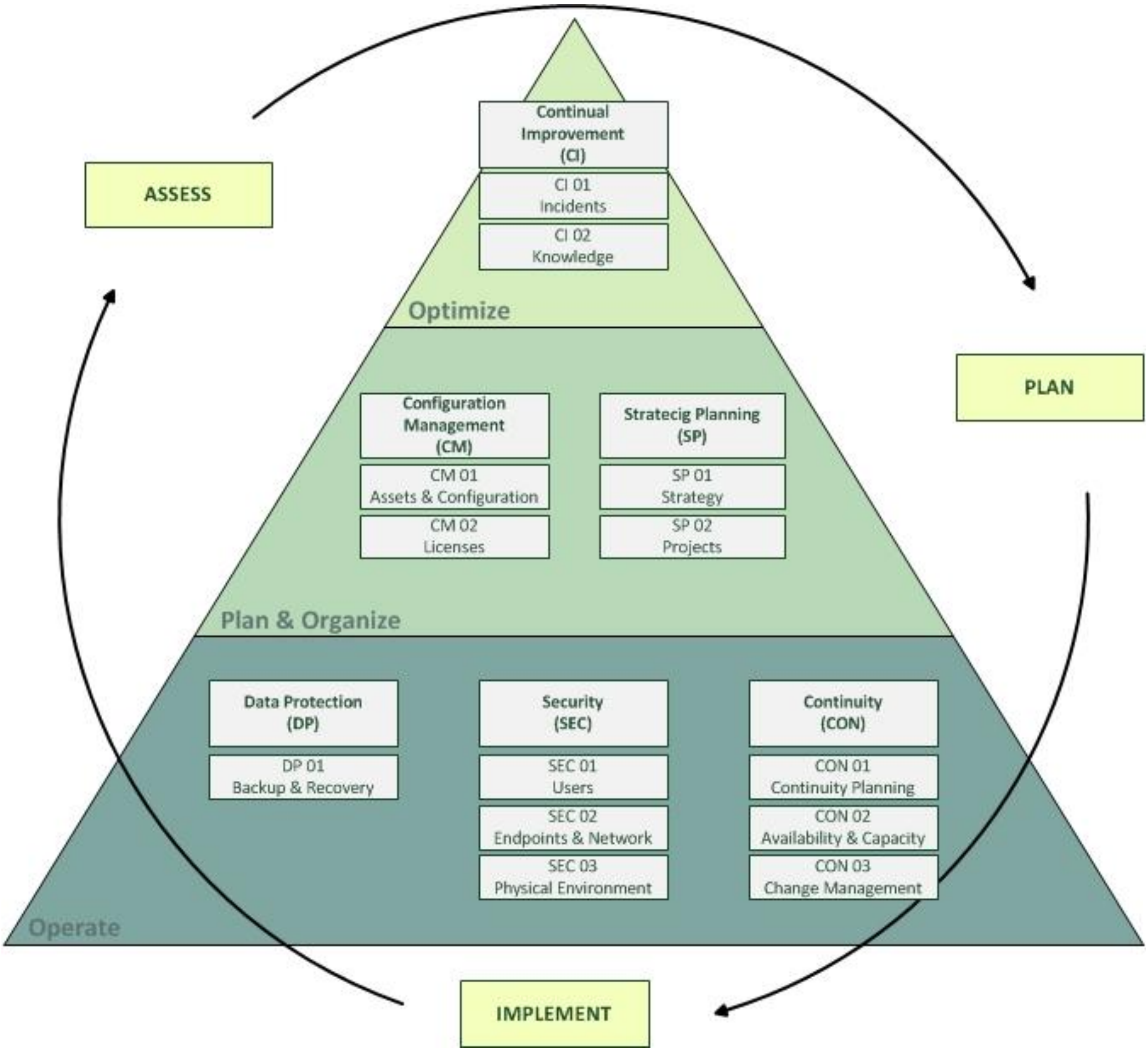

Figure 1: The framework.

Table of Content

1. Principles

The principles outline the characteristics of the framework and determine the scope of the framework regarding the applicability and the operational area.

1.1 Self-Empowerment

The framework is simple and easy to understand. This makes it possible that the implementation can be made by the company on its own, without special knowledge or external consulting necessary. The framework comes with a built-in lifecycle and an assessment which facilitates the implementation process by providing a step-by-step guidance.

1.2 Lightweight Approach

A framework should not be implemented for its own sake but should improve the overall maturity and quality of the related IT processes. Therefore, this framework is based on a lightweight approach meaning that no excessive requirements regarding the deliverables are prescribed.

The design of the framework is structured in a way that it fits well into the existing structures and processes. Although processes are proposed, it does not automatically mean that these processes have to be adopted in order to reach satisfactory results. The main objective of the segmentation into processes is that the described tasks are logically structured and can be assigned to an existing role or person in the company.

1.3 Compatibility

Since there are already numerous frameworks in the area of IT Governance, it is not reasonable to develop a distinct framework. This Framework is based on COBIT 5, but has been tailored for the needs for small and medium-sized enterprises. This approach ensures compatibility and extendibility. Companies that have implemented this framework can easily upgrade to COBIT 5 by consulting the provided COBIT 5 mapping in chapter 5.3. The mapping reveals the COBIT 5 processes that are included in this framework.

2. Components

The framework is divided into three layers, depicted in in a pyramid. The layers separate the domains regarding their importance for a company master the daily business. The form of the pyramid graphically expresses the level of importance that the layer has regarding to master the daily business.

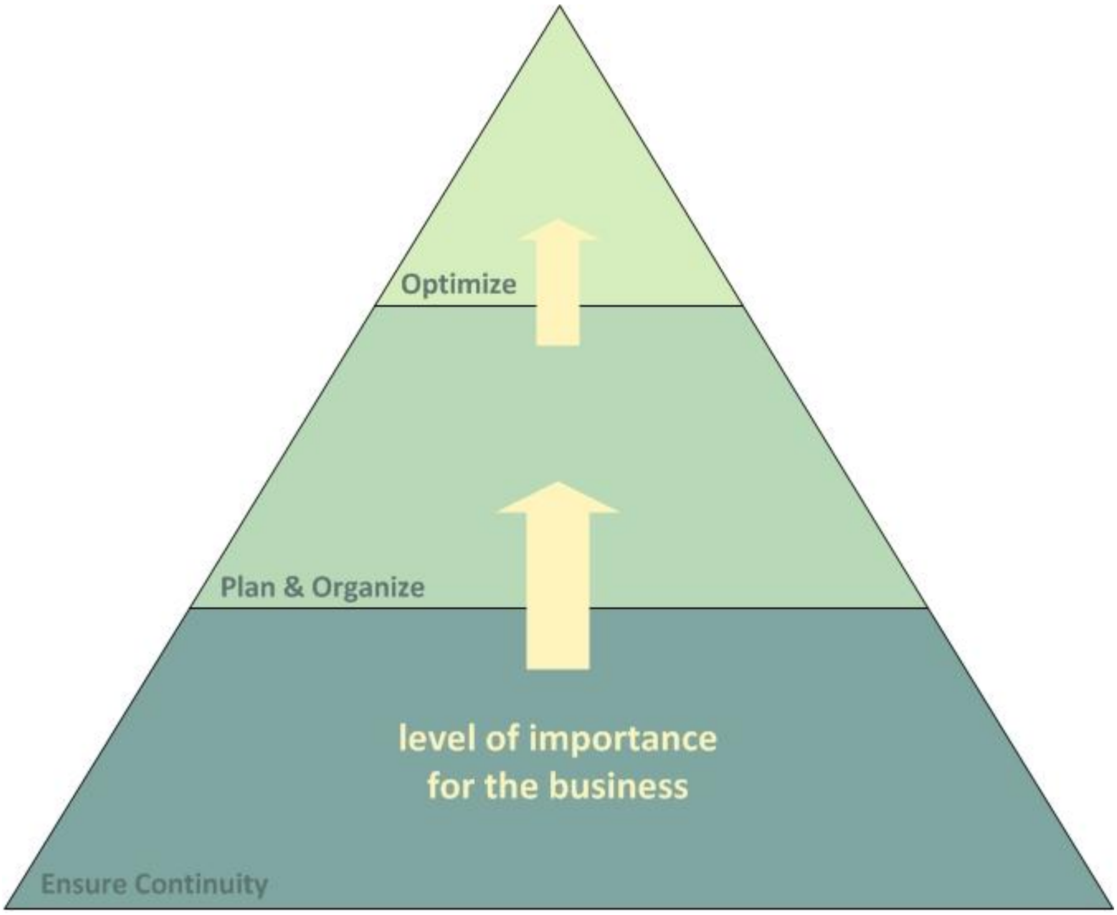

Figure 2: Explanation of layers.

Usually, incidents at the bottom layer have great impact on daily business processes. Running backup and recovery processes or a well-protected infrastructure is vital for the business. The layer Ensure Continuity contains all key processes that are necessary for solid and stable provisioning of IT services. The middle layer consolidates the planning and administrative tasks. Its main purpose is that IT services are effectively managed and that IT divisions move from reactive to proactive management. Optimization within the IT department is the intention of the top layer.

The domains are logically detached and the processes within the domains illustrate real-live processes in a common IT operations department, based on a functional separation.

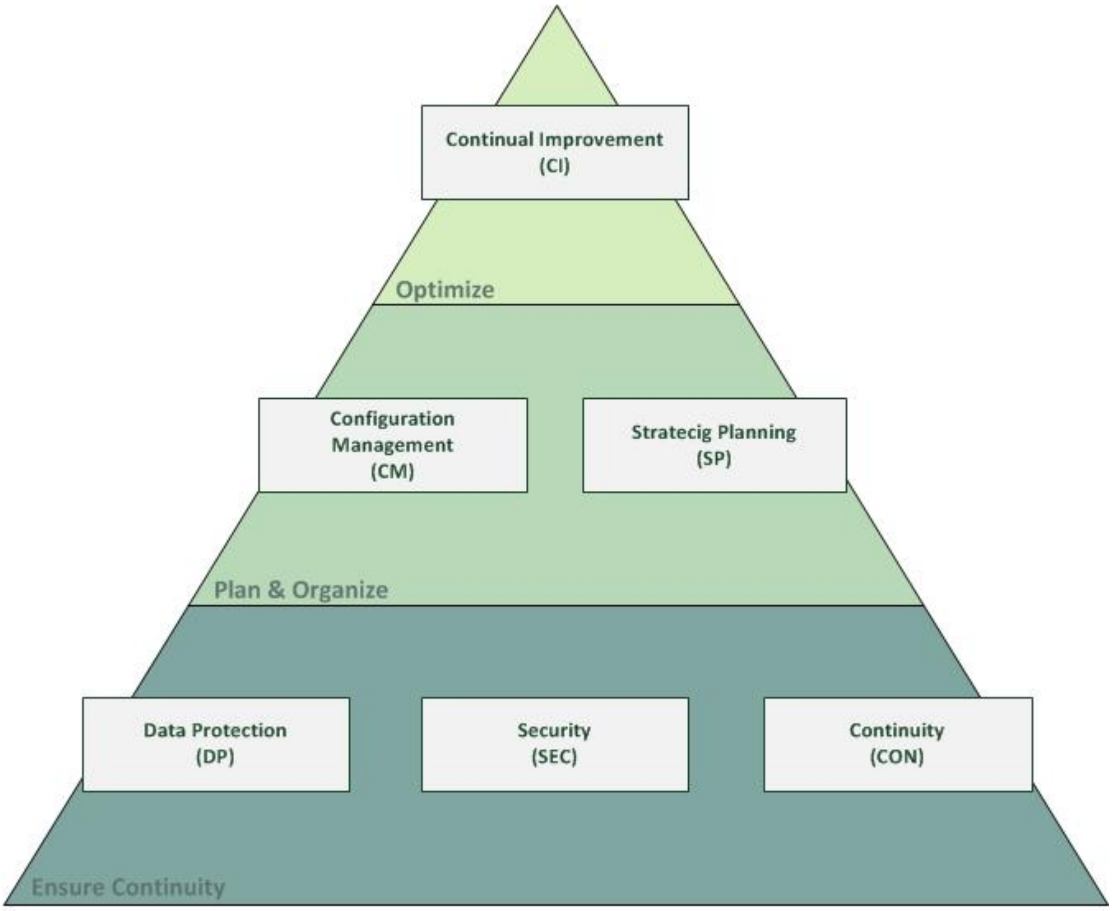

Figure 3: Explanation of domains.

In the following, each process is described in detail. Every process consists of a process goal, enumeration and explanation of tasks and prescribes the necessary attributes that should be produced or maintained. To enable monitoring functionalities, each process provides metrics that can be traced. Additionally, best practices are provided.

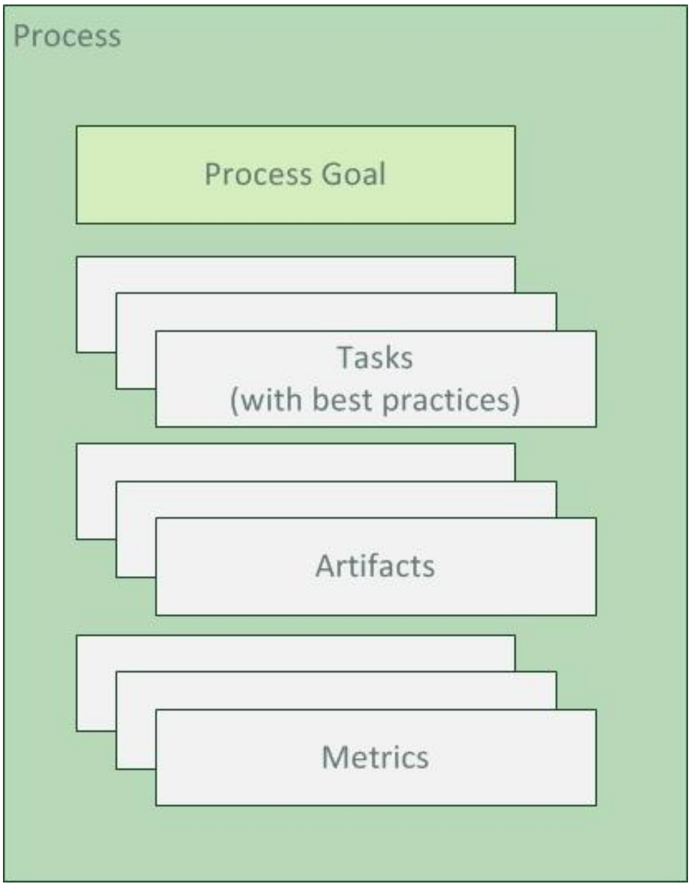

Figure 4: Structure of a process.

3. Processes

As already mentioned, this framework is tailored out of COBIT 5 for the needs of small and medium-sized enterprises. The content of the processes has been mainly taken out of the respective COBIT 5 processes (see the provided mapping in chapter 5.3). Where necessary, some minor changings have been made.

3.1 DP01: Backup and Recovery

3.1.1 Process Goal

Secure corporate data and ensure fast and efficient data recovery

3.1.2 Tasks

DP01.T01 Backup

Backup systems, applications, data and documentation according to a defined schedule. The following considerations should be taken into account:

- Frequency (monthly, weekly, daily etc.)
- Mode of backup (e.g., disk mirroring for real-time backups , DVD for long-term retention)
- Type of backup (e.g., full vs. incremental)
- Type of media
- Creation of logs
- Monitoring and alerting
- Physical and logical location of data sources
- Security and access rights
- Encryption

Best Practice

- Systems are usually backed up by creating images whereas data is backed up with file-based backup routines. It is common to apply a grandfather-father-son backup policy for most backup objects. This backup technique stores full copies of the backup source on a monthly basis, incremental backups on a weekly basis and differential backups on a daily basis. This approach ensures that any state can be restored, depending on the retention policy.
- Backups should be stored on a secure location and ideally not the same location as the data source whilst ensuring a fast recovery processes. It is recommended to use dual-destination backup to encounter this challenge. Dual destination backup allows storing backup objects on two (physically separated) locations. The first location should be quickly accessible in case of recovery and the second location should satisfy the demand of a secure backup location (e.g. backup in the cloud or in another company site).
- Compliance with external laws and regulations must be adhered. Be aware that for some industries (e.g. health) there are special requirements for data retention.

DP01.T02 Test backup objects

Periodically test backup objects through validation and restoration trials.

Best Practice

- Validation and testing is a vital task to ensure the quality of the backup. It may happen that backup objects can't be restored, for what reason ever, and proper and regular testing is essential to perceive this misconduct. Whilst the restoration testing of data is a rather trivial process, restoration testing of systems and applications is difficult because of the required peripheral system that is necessary to check the functionality. The setup of virtual system environments has proven to be an efficient way for restoration testing of systems and applications.

DP01.T03 Establish restoration routines

Ensure that in case of data loss staff is well trained in the recovery process. Minimal system downtime or data leakage should be aimed-at.

3.1.3 Artifacts

DP01.A01 Backup and Recovery Plan

The backup and recovery plan should entail:

- Documentation of the backup process and the backup routines (DP1.T01)
- Testing scenarios and testing plan (DP1.T02)
- Recovery plan (if necessary step-by-step instructions) for each backup object (DP1.T03)

3.1.4 Metrics

DP01.M01 Percent of backup files transferred and stored securely

DP01.M02 Frequency of tests

DP01.M03 Number of recovery exercises and tests that have achieved recovery objectives

3.2 SEC01: Users

3.2.1 Process Goal

Minimize the business impact of information security vulnerabilities and incidents caused by user misconduct.

3.2.2 Tasks

DSS01.T02 User Security

Ensure that all users have information access rights in accordance with their business requirements. Ensure that users are aware of security issues and establish user guidelines.

Best Practice

- Maintain user access rights in accordance with business function and process requirements. Align the management of identities and access rights to the defined roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles.
- Manage user access lifecycle from creation of user account, to modifications and deletion (especially with trainee-accounts) and perform regular management review of all accounts and related privileges.
- Clear policies help to improve the security standard and raise the security awareness. A user policy should provide helpful information for users on how to behave and how to deal with security threats.

3.2.3 Artifacts

SEC01.A01 User Policy

The user policy is an internal document that contains regulations. It should describe the desired behavior with the use of information technology as well as in case of incidents and problems.

3.2.4 Metrics

SEC01.M01 Percent of stakeholders who understand policies

SEC01.M02 Frequency of policies review and update

SEC01.M03 Number of accounts incompliant with the policy

3.3 SEC02: Endpoints and Network

3.3.1 Process Goal

Minimize the business impact of information security vulnerabilities and incidents caused by endpoints or network devices

3.3.2 Tasks

SEC02.T01 Endpoint Security

Implement and maintain preventive, detective and corrective measures in place across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, and spam) and ensure that endpoints are secure. Up-to-date virus software and proper patching on every endpoint are the core security measures.

Best Practice

- The management of malware solutions and system updates is centralized, enabling reporting functionalities that permit better pro- and reactive measures in case of a security incident.
- The hardening of endpoints is another useful security measure. The following reflections should be taken into account (not conclusive):
  - ✓ Configure operating systems in a secure manner (e.g. local administrator rights)
  - ✓ Implement device lockdown mechanisms.
  - ✓ Manage remote access and control. (e.g. VPN)
  - ✓ Provide physical protection of endpoint devices.
  - ✓ Dispose of endpoint devices securely.

SEC02.T02 Network Security

Use security measures and related management procedures to protect information over all methods of connectivity.

Best Practice

- Nowadays, network devices offer a wide range of possibilities to face cyber security. Unified Thread Management (UTM) has proven to be an efficient measure to protect the local network and has become affordable not only for large enterprises. The following principles should be adopted:
  - ✓ Allow only authorized devices to have access to corporate information and the enterprise network. Configure these devices to force password entry.
  - ✓ Implement network filtering mechanisms such as firewalls and intrusion detection software with appropriate policies to control inbound and outbound traffic.
  - ✓ Encrypt information in transit according to its (implicit or explicit) classification.
  - ✓ Apply approved security protocols to network connectivity.
  - ✓ Configure network equipment in a secure manner.
  - ✓ Carry out periodic penetration testing to determine adequacy of network protection.
  - ✓ Carry out periodic testing of system security to determine adequacy of system protection.

3.3.3 Artifacts

SEC02.A01 Security Plan for Endpoints and Network

The security plan should cover:

- The management of Endpoint Security (SEC02.T01)
- The management of Network Security (SEC02.T02)

3.3.4 Metrics

SEC02.M01 Number of vulnerabilities discovered

SEC02.M02 Number of outstanding patches at a point in time

SEC02.M03 Number of incidents involving endpoint devices

SEC02.M04 Number of security incidents causing business disruption

3.4 SEC03: Physical Environment

3.4.1 Process Goal

Protect the physical infrastructure against unauthorized access.

3.4.2 Tasks

SEC02.T01 Physical Security

Define and implement procedures to grant, limit and revoke access to IT systems according to business needs, including emergencies. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.

Best Practice

- Manage the requesting and granting of access to the computing facilities. Formal access requests are to be completed and authorized by management of the IT site, and the request records retained. The forms should specifically identify the areas to which the individual is granted access.
- Ensure that access profiles remain current. Base access to IT sites (server rooms, buildings, areas or zones) on job function and responsibilities.
- Require visitors to be escorted at all times while onsite by a member of the IT operations group. This is hard to implement in small and medium-sized enterprises and depends on several factors (e.g. level of trust to the visitor, purpose of the task).
- Conduct regular physical security awareness training.

3.4.3 Artifacts

SEC03.A01 Security Plan for physical Security

The security plan for physical security should cover:

- The management of Physical Security (SEC03.T01)

3.4.4 Metrics

SEC03.M01 Number of physical-security related incidents

3.5 CON01: Continuity Planning

3.5.1 Process Goal

Ensure continuity of critical business operations.

3.5.2 Tasks

CON01.T01Develop and implement a business continuity response

Identify it services that are critical to the business operations and implement rational continuity measures.

Best Practice

- Identify potential scenarios likely to give rise to events that could cause significant disruptive events. These events should then be classified regarding the time of disruption in case of failure and their importance. The importance is often determined through the maximal tolerable outage. The time required to recover should also be taken into consideration.
- Identify measures that will reduce the likelihood through prevention and determine cost-effective measures that are to be taken in case of an incident. These procedures should be well documented so that in case of a disruptive event, a structured course of action can be taken.
- Clear roles and responsibilities for each measure must exist.

CON01.T02Exercise, test and review the business continuity plan

Test the continuity arrangements on a regular basis.

Best Practice

- The testing of the continuity plan has multiple purposes. First you want to be sure that the defined measures work as desired (verification). Secondly, staff is getting trained in dealing with exceptional situations (learning) and last but not least, the procedures can be optimized by accomplishing continuity tests (optimization).

3.5.3 Artifacts

CON01.A01 Continuity Plan

The continuity plan should contain:

- A business impact analysis with potential scenarios (CON01.T01)
- Incident response actions based on the continuity requirements(CON01.T01)
- Testing plan, containing the test objects and a time plan (CON01.T02)

3.5.4 Metrics

CON01.M01	Number of critical business systems not covered by the continuity plan
CON01.M02	Percent of successful business continuity incidents
CON01.M03	Number of planned business continuity exercises
CON01.M04	Percent of executed business continuity exercises that have achieved its objectives

3.6 CON02: Availability and Capacity

3.6.1 Process Goal

Maintain service availability, efficient management of resources and optimization of system performance through prediction of future performance and capacity requirements.

3.6.2 Tasks

CON02.T01Identify availability and capacity requirements

Balance current and future needs for availability, performance and capacity with cost-effective service provisioning.

Best Practice

- Assess availability, performance and capacity of it services and resources and determine the baselines. The assessment should consider the current and forecasted requirements. The following criteria should be considered:
  - ✓ Customer requirements
  - ✓ Business priorities and objectives
  - ✓ Budget impact
  - ✓ Resource utilization
  - ✓ IT capabilities and industry trends
- Ensure periodic monitoring (or where possible automated) and implement appropriate alerting functionalities (e.g. free disk space).
- Plan, prioritize availability, performance and capacity implications of changing business needs and service requirements.

3.6.3 Artifacts

CON02.A01 Availability and Capacity Plan

The availability and capacity plan should contain:

- Availability, performance and capacity baselines
- Monitoring and alerting configuration
- Action plan concerning availability and capacity for the next couple of years (depending on industry and procurement strategy)

3.6.4 Metrics

CON02.M01 Percent of unplanned capacity, performance or availability upgrades versus planned upgrades

CON02.M02 Number of availability incidents

CON02.M03 Number of events where capacity has exceeded planned limits

3.7 CON03: Change Management

3.7.1 Process Goal

Enable fast and reliable delivery of change to the business and mitigation of the risk of negatively impacting the stability or integrity of the changed environment.

3.7.2 Tasks

CON03.T01Manage Changes

Evaluate, prioritize and authorize change requests. Implement standard change procedures and ensure proper monitoring and control mechanisms.

Best Practice

- Ensure that all changes are conducted in a structured way. The following considerations should be taken into account (a simple form is enough):
  - ✓ Impact assessment
  - ✓ Prioritization and authorization
  - ✓ Emergency changes,
  - ✓ Tracking
  - ✓ Reporting
  - ✓ Closure and documentation
- All changes should be coordinated centrally through one consistent person, so that holistic overview is ensured. This is vital to recognize possible dependencies.

CON03.T02Prepare and execute Testing

Establish a test plan and required environments to test individual or integrated solution components, including the business processes and supporting services, applications and infrastructure. Execute testing continually based on the change plan.

Best Practice

- Suitable testing of scheduled changes helps to verify that the solution will operate successfully in the live environment and delivers the intended results.
- Create a test plan and ensure that the test procedures should simulate real-world conditions.
- For critical applications it is recommended to temporarily set up mirrored environments where the real environment can be simulated at a very high degree of similarity. Note that not everything can be simulated and that a certain residual risk will remain.
- Make sure that the test results are logged.

3.7.3 Artifacts

CON03.A01 Change Plan

The change plan should contain:

- Description of the change management process
- Overview about scheduled changes
- Reference to the required respectively demanded forms (change request, test plan)

3.7.4 Metrics

CON03.M01	Percent of unsuccessful changes due to inadequate impact assessments
CON03.M02	Percent of total changes that are emergency fixes
CON03.M03	Number of executed tests

3.8 CM01: Assets & Configuration

3.8.1 Process Goal

Account for all IT assets and optimize the value provided by these assets. Provide sufficient information about service assets to enable the service to be effectively managed

3.8.2 Tasks

CM01.T01 Identify and Manage Assets

Manage IT assets though their life cycle. Make sure that their use delivers value at optimal cost, they remain operational and physically protected.

Best Practice

- Identify all assets and maintain alignment with the change- and configuration management.
- Verify the existence of all owned assets by performing regular physical and logical inventory checks and reconciliation.
- Source, receive, verify, test and record all assets in a controlled manner, including physical labeling, as required.

CM01.T02 Manage the Configuration

Define and maintain descriptions and relationships between key resources and capabilities required to deliver IT-enabled services.

Best Practice

- Define and agree on the scope and level of detail for configuration management.
- Establish and maintain a logical model of the services, assets and infrastructure and how to record configuration items and the relationships amongst them. A good point to start is a drawing of the system landscape that proves a good overview by naturally selecting the level of detail.
- Periodically verify live configuration items against the configuration repository by comparing physical and logical configurations.

3.8.3 Artifacts

CM01.A01 Asset Register

The asset register should cover:

- List of all IT assets with information about procurement, maintenance and disposal (e.g. warranty information).

CM01.A02 Configuration Repository

The configuration repository should cover:

- Graphical abstraction of the system landscape
- Actual configuration of the selected configuration items
- Description of the relationship among the configuration items.

3.8.4 Metrics

CM01.M01	Number of assets not utilized
CM01.M02	Number of deviations between the configuration repository and live configuration

3.9 CM02: Licenses

3.9.1 Process Goal

Ensure that licenses are procured in the right quantity.

3.9.2 Tasks

CM02.T01 Manage Licenses

Manage software licenses to ensure that the optimal number are acquired, retained and deployed in relation to required business usage.

Best Practice

- Maintain a register of all purchased software licenses and associated licenses agreements.
- On a regular basis, conduct an audit to identify all instances of installed licensed software. Decide whether there is a need to retain or terminate licenses in case of dissimilarities.

3.9.3 Artifacts

CM02.A01 License Register

The license register should cover:

- The management of software licenses (contact information, license keys and agreements)
- An actual overview about the current status

3.9.4 Metrics

CM02.M01	Percent of used licenses against paid-for licenses

3.10 SP 01: Strategy

3.10.1 Process Goal

Align IT with business objectives.

3.10.2 Tasks

SP01.T01 Determine IT direction

Provide a holistic view of the current business and IT environment and the future direction.

Best Practice

- Consider the current enterprise environment and business processes, as well as the external environment of the enterprise (industry drivers, relevant regulations, basis for competition) for the future direction.
- Identify key stakeholders and obtain insight on their requirements. Then, identify and analyze sources of change in the enterprise and ascertain priorities.
- Make sure that the future direction is controlled / revised regularly

SP01.T02 Define and communicate road map

Develop initiatives and communicate to the stakeholders.

Best Practice

- Define a road map based on the results of SP01.T01. Determine dependencies, overlaps, synergies and impacts amongst initiatives.
- Identify resource requirements, schedule budgets for each of the initiatives.

3.10.3 Artifacts

SP01.A01 Road Map

The road map is the strategy document regarding IT decisions. The road map should cover:

- Statement about the future direction
- Initiatives to be performed embedded in a chronology

3.10.4 Metrics

SP01.M01	Percent of projects that can be directly traced back to the strategy
SP01.M02	Frequency of updates to the road map

3.11 SP02: Projects

3.11.1 Process Goal

Optimize the performance of IT-projects in response to changing enterprise priorities and demands.

3.11.2 Tasks

SP02.T01 Maintain the IT-Portfolio

Maintain portfolio of projects, IT services and IT assets.

Best Practice

- Create and maintain portfolios of IT-enabled investment programs, IT services and IT assets, which form the basis for the current IT budget and support the road map.
- On a regular basis, monitor and optimize the performance of the IT-portfolio to exploit synergies, eliminate duplication between programs and identify and mitigate risk.

SP02.T02 Manage projects

Maintain a standard approach for project management. Plan and monitor IT projects.

Best Practice

- Enforce a standard approach for project management (e.g. Hermes (Schweizerische Eidgenossenschaft, 2005), PMBoK (Project Management Institute, 2009)). Ensure that the approach covers the full life cycle.
- Establish and maintain project planning to guide project execution and control throughout the life of the project.
- Ensure that milestones are accompanied by significant deliverables requiring review and sign-off.

3.11.3 Artifacts

SP02.A01 IT-Portfolio

The IT-Portfolio should cover:

- Consolidation of all current IT initiatives
- Guidelines for projects (e.g. procedure model)
- Monitoring and control mechanisms for projects

3.11.4 Metrics

SP02.M01	Number of running initiatives
SP02.M02	Percent of successful initiatives
SP02.M03	Percent of projects undertaken without approved business cases
SP02.M04	Percent of deviations from the project plan

3.12 CI01: Incidents

3.12.1 Process Goal

Achieve increased productivity and minimize disruptions through quick resolution of user queries and incidents. Increase availability, reduce costs and improve customer convenience and satisfaction by reducing the number of operational problems.

3.12.2 Tasks

CI01.T01 Manage Incidents

Provide timely and effective response to user requests and resolution of all types of incidents.

Best Practice

- Implement an incident register (e.g. ticketing system)
- Define incident and service request classification and prioritization schemes to ensure consistent approaches for handling, informing users about and conducting trend analysis.
- Define appropriate support groups to assist with identification, root cause analysis and solution determination. Define priority levels through consultation with the business and report the status of identified incidents.
- Make sure that known-errors are recorded and communicated.

3.12.3 Artifacts

CI01.A01 Incident Register

The incident register should cover:

- Incident management procedures
- All incident requests
- Known errors

3.12.4 Metrics

CI01.M01 Number of incidents causing disruption to business-critical processes

3.13 CI 02: Knowledge

3.13.1 Process Goal

Provide the IT-related knowledge required to support all staff in their work activities and for informed decision making and enhanced productivity.

3.13.2 Tasks

CI02.T01 Manage IT-Knowledge

Maintain the availability of relevant, current, validated and reliable knowledge to support all process activities and to facilitate decision making. Plan for the identification, gathering, organizing, maintaining, use and retirement of knowledge.

Best Practice

- Establish and maintain a knowledge database (e.g. Wiki). Define documentation standards.
- Ensure user training and increase user awareness through training and sensitization.

3.13.3 Artifacts

CI02.A01 Knowledge Database

The Knowledge Data base must be able to:

- Document unstructured information and transform it to knowledge.
- Publish and make knowledge accessible to relevant stakeholders.

3.13.4 Metrics

CI02.M01	Level of satisfaction of users
CI02.M02	Frequency of updates in the knowledge database
CI02.M03	Percent of knowledge repository used

4. Lifecycle

The lifecycle provides good guidance for implementing the framework. It is based on a continual improvement process where first, the current situation is assessed, then the desired state is defined and the necessary measures are taken. In the last step of the cycle, the defined initiatives are implemented.

The following premises should be taken into consideration.

- IT governance cannot be implemented within a big-bang approach but needs to emerge slow and steadily.
- A governance-aware enterprise culture is the foundation for successful implementation.
- Management support is vital for the success.
- Provided that these preconditions are covered, implementation proposals can begin.

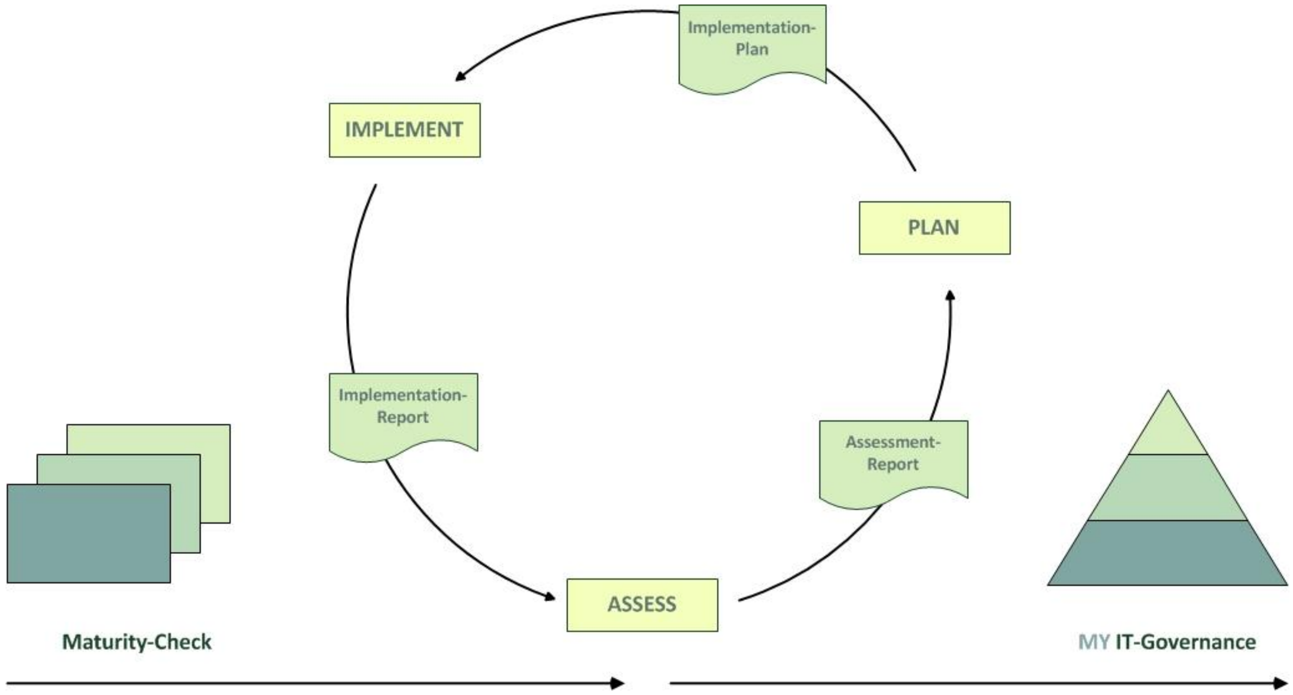

Figure 5: Lifecycle.

4.1 Assess

The primary goal of the assessment phase is to conduct an analysis of the current maturity regarding IT governance tasks. The maturity-check provided within the framework (it-governance-for-sme.ch/maturity-check) offers an easy way to initially assess the current situation. It is also helpful because by replying the questionnaire all relevant IT topics pop up and the assessor automatically becomes confronted with practically relevant interrogations. In the best case the accomplishment of the maturity-check not only helps to determine the actual state but already sensitizes the company regarding the most important IT governance topics. Another advantage of the maturity-check is that the assessor already starts working with the framework and thereby learns to know the structure of the framework from the bottom. The following picture illustrates the result of an example assessment. Each process is filled with the respective color that was calculated from the indications of the questionnaire. Red means that the assessed process maturity is insufficient, orange indicates a little better process maturity and the light green states that the process maturity is sufficient but there is still some room for improvement. The dark green means that the process is implemented with a high process maturity.

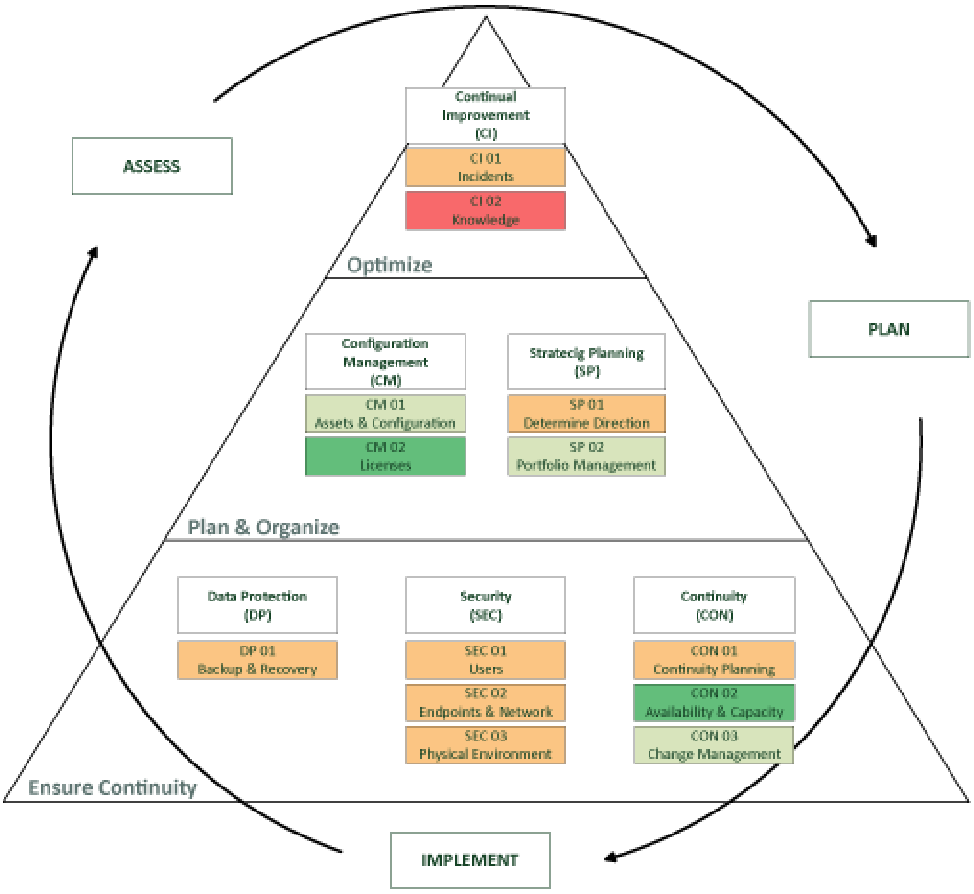
ASSESS
PLAN
IMPLEMENT
Continual Improvement (CI)
CI 01 Incidents
CI 02 Knowledge
Optimize
Configuration Management (CM)
CM 01 Assets & Configuration
CM 02 Licenses
Strategic Planning (SP)
SP 01 Determine Direction
SP 02 Portfolio Management
Plan & Organize
Data Protection (DP)
DP 01 Backup & Recovery
Security (SEC)
SEC 01 Users
SEC 02 Endpoints & Network
SEC 03 Physical Environment
Continuity (CON)
CON 01 Continuity Planning
CON 02 Availability & Capacity
CON 03 Change Management
Ensure Continuity

Figure 6: Result of example assessment (on it-governance-for-sme.ch).

Once the maturity-check is done, the results must be analyzed. It is therefore vital to study the framework and the proposed tasks, artifacts and metrics and already trying to make some linkage between the framework and the real-life situation.

An assessment-report is the final delivery of this phase. It contains the findings from the maturity-check as well as the subsequent analysis. The main purpose of this document is that the weaknesses are clearly addressed so that it can serve as a base for decision making.

4.1.1 Artifact

Assessment-Report

4.2 Plan

In the planning phase, the desired state is defined and, with help of the assessment-report, an implementation plan is set up. It is of great importance that the desired result is clear to everyone. The desired result can be expressed with help of the assessment-report and the described artifacts in the framework.

The implementation plan should consolidate all scheduled activities. For all activities, the following information must be provided:

- Goal
- Priority
- Result (e.g. process or artifact)
- Time horizon
- Responsible person(s)
- Estimated implementation cost
- Estimation of required manpower

This proceeding ensures a structured approach and enables monitoring and control of the implementation progress. Prioritization should be with regards to the severity of the discovered weakness during the assessment phase and the estimated overall expenditures. After the implementation-plan is elaborated, it must be reviewed and approved by the management.

4.2.1 Artifact

Implementation-Plan

4.3 Implement

The implementation consists of the three main steps execute, monitor and review. The execution of the activities happen according to the implementation plan and regular monitoring activities ensure the implementation success. After completion, the result of the activity is reviewed and an overall implementation-report concludes the implementation phase.

4.3.1 Artifact

Implementation-Report

5. Benefits

This chapter lists the benefits for small and medium-sized enterprises of using this framework.

5.1 Usability

This framework has been specifically developed for small and medium-sized enterprises. Whereas the content within the prescribed processes is tailored from COBIT 5 and therefore does not differ much (where an equivalent process is existent in this framework), organizational recommendations such as roles and responsibilities or the implementation guidance have not been adopted. Just from a rational perspective it would not be reasonable to apply the provided roles and responsibilities from COBIT. The organization of small and medium-sized enterprises simply does not allow such a setup. This framework does not provide any role or responsibility. The company is absolutely free in deciding its organizational structure and the framework can be implemented regardless of the organizational and operational structure. Although COBIT does not prescribe an organizational structure by defining the roles and responsibilities, the quantity of the described roles make an implementation within a small and medium-sized enterprise nearly impossible. The lightweight design of this framework enables maximal flexibility.

As described in the framework's principles, self-empowerment is another important factor that determines the usability of the framework. The framework is structured in a simple and reasonable way and is easily understandable. The simplicity of the structure is necessary for ensuring this self-empowerment approach. A company should be able to set up this IT governance framework without external help. Furthermore, the company should feel equal to manage the prescribed processes after successful implementation. An IT governance initiative should not be started for its own sake but for the sake of improving the IT processes. Therefore it is vital for any enterprise that the processes of this framework become an integral part of the IT organization.

5.2 Compliance

Compliance with external laws and regulations can be improved by applying this framework. It does not mean that the framework solves all challenges regarding compliance but the better each process is implemented, the more probable it is that the compliance requirements are fulfilled. According to Grünendahl et al. (Das IT-Gesetz: Compliance in der IT-Sicherheit, 2012, p. 13), IT governance helps to improve the awareness regarding IT compliance issues. Additionally, clearly structured IT processes provide a good overview across the IT landscape which eases to address compliance topics.

5.3 Compatibility with COBIT 5

The framework is based on COBIT 5. Although compliance with COBIT 5 is not a direct advantage that argues for the application of this framework, it may be beneficial to first adopt this framework than directly applying COBIT 5. The implementation of COBIT 5 takes much more personal, organizational and financial resources. The advantage emerges when an enterprise that actually has this framework in place wants to upgrade to COBIT 5. All processes in this framework can be mapped to the COBIT 5 enabling processes (ISACA, 2012) assuring upwards compatibility.

The following figure maps the processes within this framework with COBIT 5.

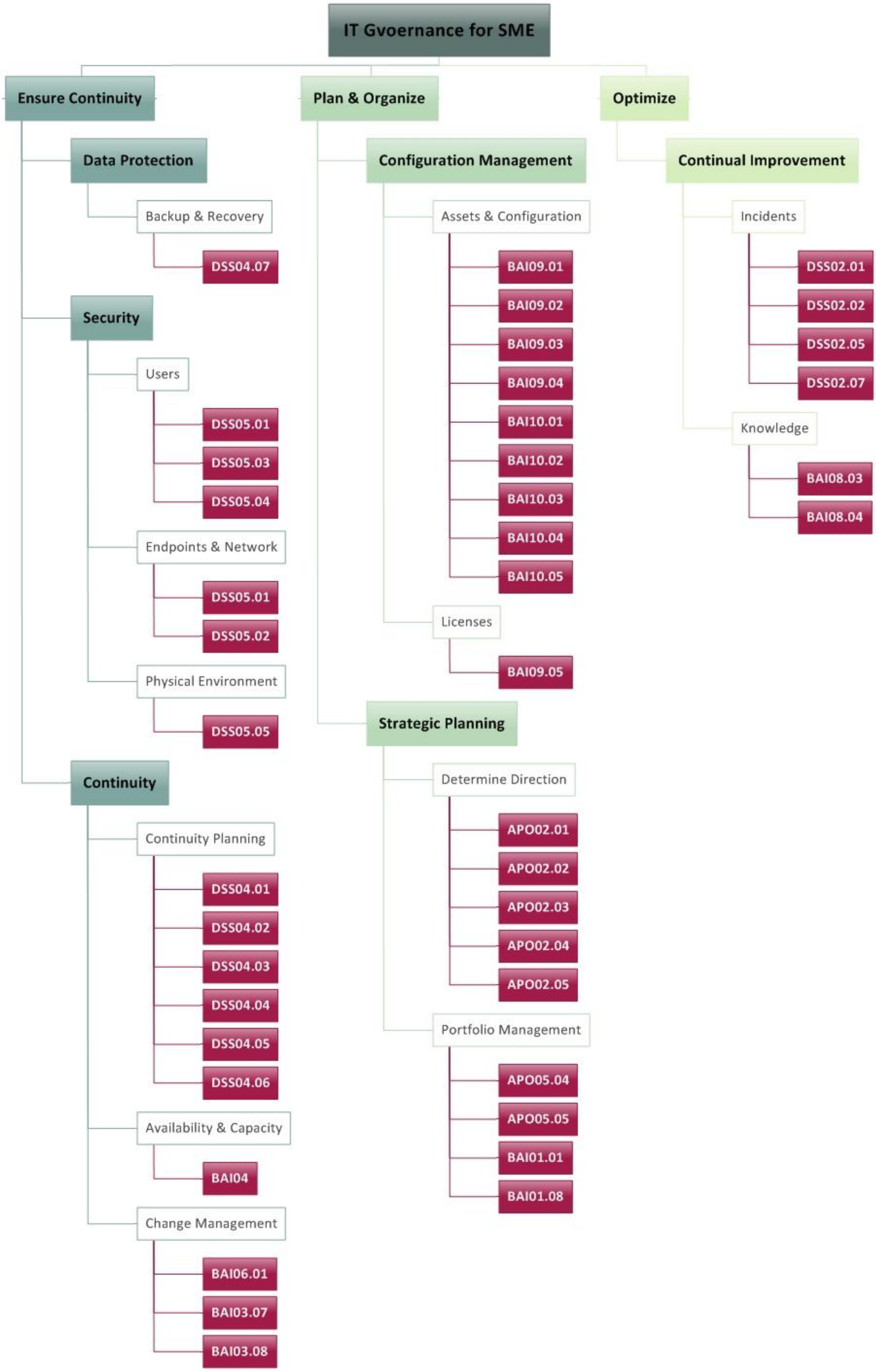

Figure 7: Mapping to COBIT 5.

5.4 Holism

IT governance can be considered to be the rooftop of all IT processes within the enterprise. It is therefore important that an IT governance initiative covers all relevant aspects of IT.

The IT governance focus areas defined by the IT Governance Institute (IT Governance Institute & KPMG, 2003) provide a solid overview by enlisting the relevant parts of IT governance. The following table contains a mapping between the processes prescribed in the framework and the IT governance focus areas.

The respective color indicates the level of affiliation of the process to the IT governance focus area. Grey means that there is no substantial coherence; the bright green indicates that the area is partially or indirectly covered and the dark green signifies direct coverage of the focus area.

	Strategic Alignment	**Value Delivery**	**Risk Management**	**Resource Management**	**Performance Measurement**
DP01 **Backup & Recovery**		Solid backup and recovery policies fasten disaster recovery.	Risk management process is part of the backup and recovery plan.	Data and Applications are crucial IT key factors.	
SEC01 **Users**		Good user security provides indirect value through prevented incidents.	The security plan implies the risk management for user security.	Staff is affected by the security plan.	
SEC02 **Endpoints & Network**		Good endpoint and network security provides indirect value through prevented incidents.	The security plan implies the risk management for endpoint and network security.	Endpoints and Network devices (Technology) are securely configured and managed.	
SEC03 **Physical Environment**		A well protected physical infrastructure prevents from theft and misconfiguration.	The security plan implies risk management for the physical infrastructure.	Facilities are properly managed.	

	Strategic Alignment	Value Delivery	Risk Management	Resource Management	Performance Measurement
CON01 **Continuity Planning**		Disruptive events are reduced.	Risk management practices are applied by establishing the business impact.		
CON02 **Availability & Capacity**	Future needs regarding availability and capacity are taken into account.	Optimal and cost-effective service provisioning.	Proactive risk management through monitoring and alerting.		
CON03 **Change Management**		Improved flexibility and agility.	Risk is reduced through proper testing		
CM01 **Assets & Configuration**		Rational sourcing		All IT assets are properly managed and configured.	
CM02 **Licenses**		Effective and efficient procurement		Software licenses are centrally managed	
SP01 **Strategy**	Optimal alignment with business objectives and long-term IT goals	Future direction is clear which leads to a concentration of resources to the determined direction			
SP02 **Projects**		Exploit synergies and reduce redundancies		IT Portfolio management of programs, projects, services and assets	
CI01 **Incidents**		Optimal end-user support increases productivity			

	Strategic Alignment	Value Delivery	Risk Management	Resource Management	Performance Measurement
CI02 Knowledge		Knowledge-Database enhances productivity		Transformation of information into knowledge.	

Table 1: Coverage of IT governance focus areas.

The table states that all focus areas are covered by the framework, except performance measurement. Although performance measurement is not directly addressed, the defined metrics within the processes provide the foundation for setting up concrete measures for assessing the performance. However, a direct coverage of this focus area is indeed inexistent. This is due to the fact that performance measurement was not rated to be that important in the interviews so that it should have been integrated in the framework. A reason for this may be that the ability to measure the performance requires a certain process maturity (repeatability) and, at most of the interview partners, this maturity level was still far away.

This framework should enable small and medium-sized enterprises to govern their IT in a simple and pragmatic manner. By looking at the table, this statement can be confirmed. Rather strategic topics have been reduced to an adequate minimum and special emphasis has been placed to operational topics. To summarize, the framework covers all relevant IT processes for small and medium-sized enterprises and its implementation is a good step towards IT governance.