Prüfungsvorbereitung Teil 1

Frühjahr 2024

Inhalt

1 Fachkompetenz

1.1 Projektmanagement - DIN 69901

1.1.1 Definitionen

Projekt Ein Projekt ist ein Vorhaben, in dem etwas erreicht werden soll. Dieses Vorhaben muss bestimmte Kriterien/Eigenschaften erfüllen.

- Zielorientiert
- Zeitlich begrenzt
- Begrenzte Ressourcen
- Einzigartig
- Komplex
- Organisiert

Zur Definition der Zielvorgaben wird oftmals das **SMART** Konzept verwendet. Dabei handelt es sich um ein Kriterium zur eindeutigen Formulierung von Zielen. Diese sind dadurch messbar und überprüfbar.

(S) **Specific** spezifisch → Ziele müssen eindeutig definiert sein

(M) **Measurable** messbar → Ziele müssen messbar sein

(A) **Achievable** erreichbar, attraktive, akzeptiert → Ziele müssen ansprechend bzw. erstrebenswert sein

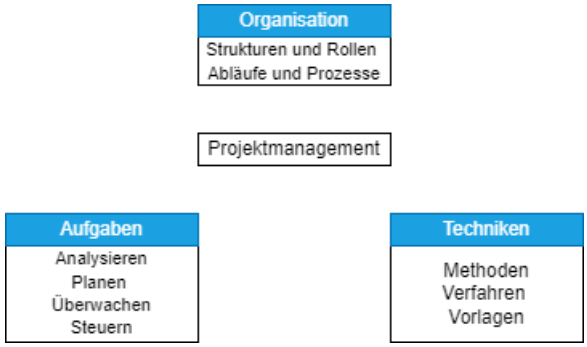
(R) **Reasonable** realistisch → Zeile müssen realistisch sein

(T) **Time-bound** terminiert → Ziele müssen mit einem fixen Datum festgelegt werden können

Projektmanagement Projektmanagement hat die Aufgabe das Projekt erfolgreich zum Ziel zu führen. Das Ziel des Projektmanagements ist es eine Leistung/Ziel zu erbringen unter Einhaltung von Zeit und Kosten (magisches Dreieck).

Magische Dreieck

Daraus ergibt sich die Definition: **Projektmanagement: "Gesamtheit von Führungsaufgaben, -organisation, -techniken und -mitteln" für die Abwicklung eines Projekts"**



Proejktmanagement

Je nach Projekttyp, Vorgehensweise (Projektmanagementsystem) können diese Bereiche auf verschiedene Personen, Personengruppen und Berufsgruppen unterschiedlich verteilt werden. *(Beispielsweise: Projektleiter, Entwicklerteam usw.)*

Agiles Projektmanagement "Agiles Projektmanagement beschreibt eine Form des Projektmanagements, bei der auf unvorhergesehene Ereignisse, neue Anforderungen und Veränderungen flexibel und proaktiv reagiert wird. Das betrifft nicht nur die Struktur von Prozessen, sondern auch Organisationen und handelnde Personen selbst." *https://scolution.de/was-ist-agiles-projektmanagement/*

1.1.2 Weitere Grundlagen

Phasen eines Projekts Ein Projekt durchläuft in der Regel vier Phasen.

- Initiierung (Projektauftrag/Projektdefintion)
- Projektplanung
- Projektdurchführung
- Projektabschluss

Initiierung: Hier werden Ziele, Umfang, Zweck und Stakeholder des Projekts identifiziert und definiert.
Mögliche Schritte sind: Machbarkeitsstudie, Identifizieren des Umfangs, Identifizieren von Projektbeteiligten, Stakeholder-Analyse, Entwickeln eines Business Case, Entwicklung eines Aufgabenbeschreibung (Dokumentation als Arbeitsvereinbarung)

Projektplanung: In dieser Phase werden Aufgaben, Ressourcen, Zeitpläne und Budgets erstellt, um das Projekt effektiv umzusetzen.
Mögliche Schritte: Projektplan, Netzplan, Gant-Diagramm, Planung von Meilensteinen, Ist- und Soll-Analyse

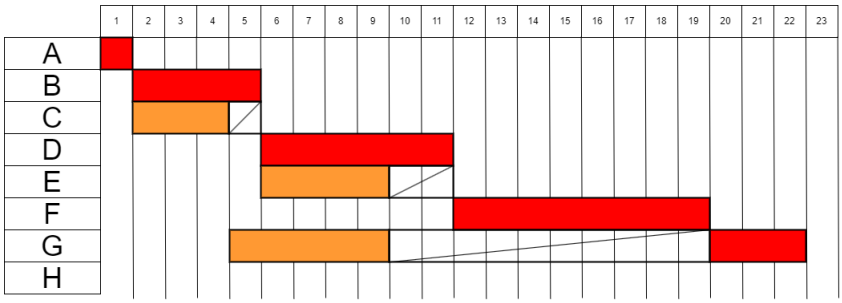
Projektdurchführung: Die Umsetzung des Projekts findet in dieser Phase statt, und die Teams setzen die im Plan festgelegten Aktivitäten um.
Mögliche Schritte: Realisierung, Testung, Erstellung detaillierter Aufgaben (Gant-Diagramm, Kanban Board), Tests

Abschluss: Die Umsetzung des Projekts findet in dieser Phase statt, und die Teams setzen die im Plan festgelegten Aktivitäten um.
Mögliche Schritte: Abschlussbericht, Analyse der Teamleistung, Abrechnung

1.1.3 Instrumente/Modelle des Projektmanagement

Gantt-Diagramm Das Gantt-Diagramm ist ein Instrument, das die zeitliche Abfolge von Aktivitäten in Form von Balken darstellt.

Nr.	Phase	Dauer	Vorgänger
A	Analyse	1	
B	Planung	4	A
C	Design 1	3	A
D	Modul 1	6	C, B
E	Design 2	4	B
F	Modul 2	8	E, D
G	Testphase Design 1	5	C
H	Übergabe	3	F, G



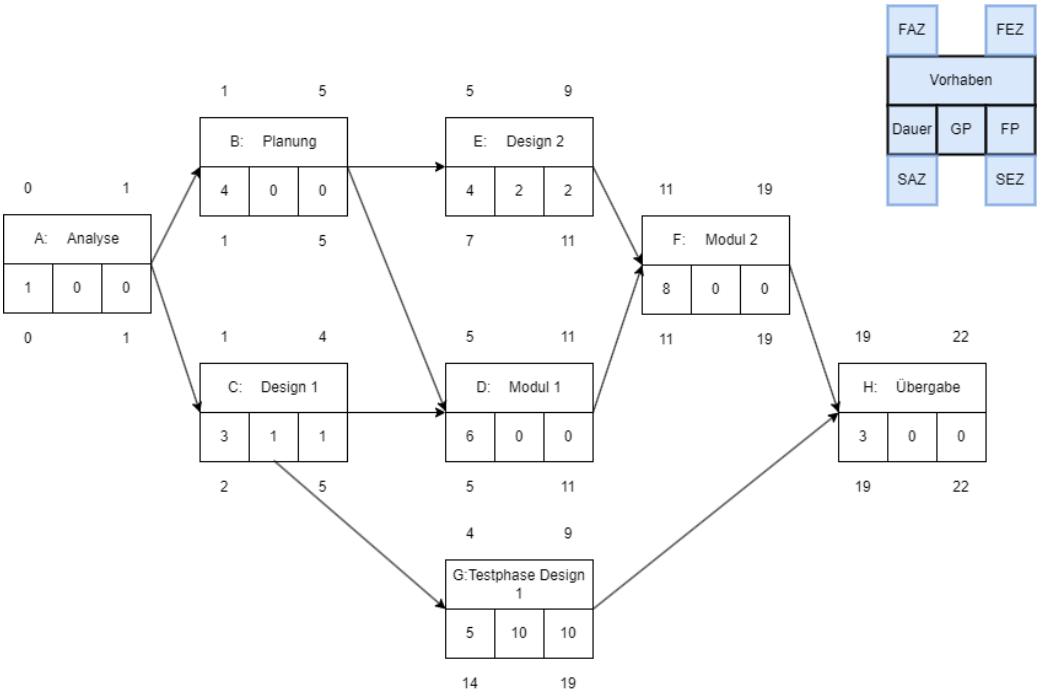
Gantt-Diagramm

Netzplan Ein Netzplan ist eine grafische Darstellung eines Projektablaufs, die die Abhängigkeiten zwischen verschiedenen Aufgaben und Aktivitäten zeigt. Er wird verwendet, um den zeitlichen Ablauf eines Projekts zu planen, zu visualisieren und zu steuern. Ein Netzplan besteht aus Knoten, die die verschiedenen Aktivitäten repräsentieren, und Pfeilen, die die logischen Abhängigkeiten zwischen den Aktivitäten darstellen.

Nr.	Phase	Dauer	Vorgänger
A	Analyse	1	
B	Planung	4	A
C	Design 1	3	A
D	Modul 1	6	C, B
E	Design 2	4	B
F	Modul 2	8	E, D
G	Testphase Design 1	5	C
H	Übergabe	3	F, G

Vorgehensweise:

1. Dauer einzeichnen
2. FAZ und FEZ ermitteln → FAZ = das letzte FEZ der Vorgänger (Zu Beginn 0), FEZ = FAZ + Dauer
3. SAZ und SEZ-Ermitteln → SEZ = SAZ des Nachfolgers (Bei letzten Vorhaben FEZ des letzten Vorhabens), SAZ = SEZ - Dauer
4. FP ermitteln = FAZ des Nachfolgers − FEZ des Vorhabens
5. GP ermitteln = SEZ - FEZ oder SAZ - FAZ
6. ggf. Kritischen Pfad ermitteln. (Pfad, bei dem es zu keiner Verzögerung kommen darf)



Netzplan
Kritischer Pfad: A → B → D → F → H

- FAZ = Frühester Anfangszeitpunkt
- FEZ = Frühester Endzeitpunkt
- SAZ = Spätester Anfangszeitpunkt
- SEZ = Spätester Endzeitpunkt
- FP = freier Puffer
- GP = Gesamtpuffer

Wasserfallmodell Das Wasserfallmodell gehört zu den klassischen Methoden im Projektmanagement. Es ist ein lineares Planungsmodell, das in aufeinanderfolgende Projektphasen unterteilt ist. Das neue Projekt startet mit der ersten Phase und läuft strikt nach der zu Beginn definierten Reihung ab. Sobald eine Phase abgeschlossen ist, geht es in eine Neue über.

1. **Initiierung:** In dieser Phase werden die Ziele und der Umfang des Projekts definiert. Es beinhaltet die Identifizierung der Stakeholder, Festlegung von Zielen und die Klärung von Erwartungen.

2. **Planung:** Die Planungsphase beinhaltet die detaillierte Festlegung von Aufgaben, Ressourcen, Zeitplänen und Budgets. Es können auch Risiken identifiziert und bewertet werden.

3. **Implementierung:** Die eigentliche Programmierung oder Entwicklung des Systems findet in dieser Phase statt.

4. **Test/Überwachung:** In der Testphase wird das Produkt das erste Mal im Ganzen getestet. Überprüft wird, ob die gesetzten Anforderungen erfüllt sind. Ziel ist es Fehler aufzudecken und diese zu beseitigen.

5. **Abschluss/Inbetriebnahme:** Sobald alle Tests abgeschlossen sind wird das fertige Produkt in den Betrieb aufgenommen und schließlich an den Kunden ausgeliefert. In dieser letzten Phase kann das Produkt immer wieder optimiert und aktualisiert werden.

Im Wasserfallmodell markieren **Meilensteine** entscheidende Punkte im Projektverlauf, wie zum Beispiel den Abschluss von Entwicklungsphasen. Jeder Meilenstein repräsentiert einen klaren Fortschritt und dient der Überprüfung, ob das Projekt im Zeitplan liegt und den Anforderungen entspricht. Meilensteine werden in der Planungsphase geplant.

Das Wasserfallmodell ist **dokumentgetrieben**. Das bedeutet nach jeder Phase muss dokumentiert werden. Beispiele hierfür: Lastenheft, Pflichtenheft, Abschlussbericht.

1.1.4 Agiles Projektmanagement

Agile Entwicklung Agile Entwicklung zielt darauf ab, schnell und flexibel auf sich ändernde Anforderungen zu reagieren, um Softwareprodukte effizient zu liefern. Sie betont enge Zusammenarbeit im Team, regelmäßige Anpassung an Änderungen, Kundenorientierung und inkrementelle Fortschritte. Sie basiert auf **Agilen Modellen.**

Agile Modelle Agile Modelle sind Rahmenwerke oder Ansätze. Sie bieten eine allgemeine Struktur für die Organisation von Projekten und betonen flexible und iterative Vorgehensweisen. Beispiele für agile Modelle sind Scrum, Kanban und Extreme Programming (XP). Agile Modelle werden durch **agile Methoden** und **agile Prozesse** unterstützt.

Agile Methoden Agile Methoden sind konkrete Techniken und Praktiken, die innerhalb eines agilen Modells angewendet werden, um den Entwicklungsprozess zu unterstützen. Zum Beispiel beinhaltet Scrum bestimmte Meetings wie Sprint Planning, Daily Standups und Sprint Reviews, die als agile Methoden betrachtet werden können.

Agile Prozesse Agile Prozesse beziehen sich auf die Gesamtheit der Aktivitäten und Abläufe, die in einem agilen Modell implementiert werden. Diese Prozesse sind darauf ausgerichtet, auf Veränderungen zu reagieren, die Anforderungen flexibel zu gestalten und inkrementelle Fortschritte zu ermöglichen. Ein Beispiel für einen agilen Prozess könnte der Scrum-Prozess sein, der Sprints, Backlog-Management und regelmäßige Retrospektiven umfasst.

Agiles Manifest Das Agile Manifest erklärt grundlegende Werte und Prinzipien der agiles Softwareenwicklung. Die zentralen vier Werte sind:

1. Individuen und Interaktionen mehr als Prozesse und Werkzeuge
2. Funktionierende Software mehr als umfassende Dokumentation
3. Zusammenarbeit mit dem Kunden mehr als Vertragsverhandlung
4. Reagieren auf Veränderung mehr als das Befolgen eines Plans

Scrum Scrum ist ein agiles Model und ist sehr verbreitet. Scrum bietet eine strukturierte Methode für die Zusammenarbeit in selbstorganisierten Teams. Das Scrum Modell umfasst 3 unterschiedliche Rollen.

1. Product Owner
2. Scrum Master
3. Entwicklerteam

Der Product Owner pflegt das *Product Backlog*. Das *Product Backlog* ist eine übersichtliche Anordnung von Anforderungen.

Grundsätzlich wird in sogenannten **Sprints** gearbeitet. Ein **Sprint** ist ein agiler Prozess mit dem Ziel effizient entwickeln zu können. Er soll eine Woche bis 4 Wochen dauern, wobei 2 Wochen üblich sind und wird grundsätzlich nicht unterbrochen. Dieser ist aufgeteilt in 4 Phasen.

1. **Sprint Planning** → Ein Meeting am Anfang eines Sprints, bei dem das Entwicklungsteam gemeinsam mit dem Product Owner die zu erledigenden Aufgaben auswählt und plant.
2. **Entwicklungsphase**
3. **Sprint Review** → Ein Meeting am Ende eines Sprints, bei dem das Entwicklungsteam die abgeschlossenen Arbeiten präsentiert und Feedback sammelt.
4. **Sprint Retrospective** → Ein Meeting am Ende eines Sprints, bei dem das Team darüber reflektiert, was gut gelaufen ist und wie es sich verbessern kann.

Der Sprint wird durch **Daily Scrums** begleitet. Das ist ein tägliches, kurzes Meeting, bei dem das Entwicklungsteam den Fortschritt bespricht, Herausforderungen identifiziert und den Tag plant. Der Scrum Master sollte dabei sein, der Product Owner kann dabei sein.

Nach Abschluss eines Sprints wird meist, sofern der Product Owner zufrieden ist deployed. Ein deploy während eines Sprints findet in der Regel nicht statt.

1.1.5 Glossar

Machbarkeitsstudie: Die Machbarkeitsstudie oder Machbarkeitsanalyse ist ein Instrument und Grundlage für die Entscheidung, ob ein Projekt durchgeführt und auf welche Art und Weise werden kann.

Stakeholder: Als Stakeholder wird eine Person oder Gruppe bezeichnet, die ein berechtigtes Interesse am Verlauf oder Ergebnis eines Prozesses oder Projektes hat.

Product Owner: Der Product Owner setzt sich für die Interessen der Stakeholder ein und achtet darauf, den maximalen und wirtschaftlichen Mehrwert eines zu entwickelnden Produktes/Software herauszuholen.

Stakeholderanalyse: Die Stakeholderanalyse oder auch Projektumfeldanalyse ist ein Instrument zur Ermittlung, welche Personen- oder Interessengruppen mögliche Stakeholder sind und welchen Einfluss diese auf die Entwicklung haben. Ebenfalls wird analysiert welche Zeile/Erwartungen die Stakeholder haben.

Scrum Master Verantwortlich für die Umsetzung von Scrum-Prinzipien, das Entfernen von Hindernissen für das Team und die Förderung einer effektiven Zusammenarbeit.

1.2 Qualitätmanagement DIN EN ISO 9000ff.

Qualitätsmanagement bezieht sich auf die systematische Planung, Steuerung und Überwachung aller Tätigkeiten und Prozesse in einer Organisation, die darauf abzielen, die Qualität ihrer Produkte oder Dienstleistungen sicherzustellen und kontinuierlich zu verbessern. Das Ziel des Qualitätsmanagements ist es, die Kundenzufriedenheit zu erhöhen, die Effizienz der Abläufe zu steigern und die Wettbewerbsfähigkeit der Organisation zu stärken.

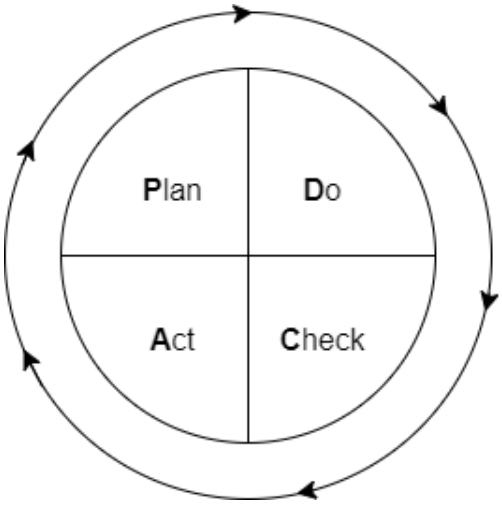
1.2.1 DIN EN ISO 9000ff.

Die Normenreihe DIN EN ISO 9000ff. bildet die Grundlage für die Planung und Umsetzung eines Qualitätsmanagementsystems. In den verschiedenen Normen werde unterschiedliche Bereiche abgedeckt. Unternehmen, die diese Normen erfüllen können von sogenannten Auditoren zertifiziert werden. Solch eine Zertifizierung nennt man auch Audit und diese kann bei Verhandlungen und Partnern Vorteile bringen.

DIN EN ISO 9000 Diese Norm definiert Grundbegriffe der Norm und nennt auch die sieben Grundsätze des Qualitätsmanagements.

1. **Kundenorientierung** → Erfüllung der Kundenanforderungen
2. **Verantwortlichkeit der Führung** → Führungskräfte auf allen Ebenen der Organisation, die sich für die Erreichung der Qualitätsziele engagieren
3. **Einbeziehung der beteiligten Personen** → Kompetente, befugte und engagierte Personen auf allen Ebenen der Organisation
4. **Prozessorientierter Ansatz und Systemorientierter Managementansatz** → Ergebnisse werden wirksamer und effizienter erzielt, wenn Tätigkeiten als zusammenhängende Prozesse verstanden werden
5. **Kontinuierliche Verbesserung** → fortlaufende Verbesserungen
6. **Sachbezogener Entscheidungsfindungsansatz** → Entscheidungen auf Basis der Analyse und Auswertungen der Daten und Informationen
7. **Beziehungsmanagement** → Nachhaltiger Erfolg durch führen und steuern der Beziehungen zu relevanten interessierte Parteien.

DIN EN ISO 9001 In dieser Norm werden Mindestanforderungen an ein QMS (Qualitätsmanagementsystem) beschrieben. Diese Norm ist somit auch Grundlage für eine Zertifizierung. Diese Mindestanforderung lassen sich anhand eines PDCA-Zyklus darstellen.



PDCA - Zyklus

DIN EN ISO 9004 Diese Leitlinien für die kontinuierliche Verbesserung der allgemeinen Leistungsfähigkeit einer Organisation. Deswegen knüpft sie an das **Total Quality Management *(TQM)*** an.

Total Quality Management TQM steht für Total Quality Management, zu Deutsch "umfassendes Qualitätsmanagement". Es handelt sich um einen systematischen Ansatz zur kontinuierlichen Verbesserung der Qualität in allen Aspekten einer Organisation. Ein Modell des TQM ist das EFQM-Modell (European Foundation for Quality Management).

Der Unterschied zwischen Qualitätsmanagement (QM) und Total Quality Management (TQM) liegt darin, dass beim QM das Unternehmen sich auf die Verbesserung der Produkte und Dienstleistungen fokussiert, während TQM alle Abteilungen und Aspekte eines Unternehmens oder Organisation umfasst.

1.2.2 Kano Modell

Das Kano-Modell ist ein Konzept, das von Professor Noriaki Kano entwickelt wurde, um die Kundenzufriedenheit zu verstehen und zu verbessern. Es basiert auf der Idee, dass verschiedene Produktmerkmale unterschiedliche Auswirkungen auf die Zufriedenheit der Kunden haben.

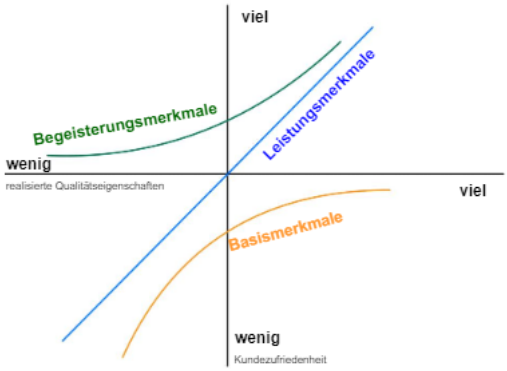
1. **Basismerkmale:** Grundlegende Funktionen oder Eigenschaften eines Produkts, die erwartet werden und als selbstverständlich gelten. Kunden werden unzufrieden, wenn diese fehlen, sind jedoch nicht besonders zufrieden, wenn sie vorhanden sind, da sie diese als selbstverständlich betrachten.

2. **Leistungsmerkmale:** Diese beeinflussen die Kundenzufriedenheit direkt. Je besser diese Faktoren erfüllt sind, desto zufriedener sind die Kunden. Allerdings gibt es hier eine lineare Beziehung: mehr Leistung führt zu mehr Zufriedenheit, weniger Leistung zu weniger Zufriedenheit.

3. **Begeisterungsmerkmale:** Diese überraschen die Kunden positiv, auch wenn sie nicht unbedingt erwartet werden. Das Hinzufügen dieser Merkmale steigert die Zufriedenheit, während ihr Fehlen die Zufriedenheit nicht unbedingt beeinträchtigt.

4. **Unerhebliche Merkmale:** Dies sind Merkmale, die die Kundenzufriedenheit **nicht signifikant beeinflussen**, unabhängig davon, ob sie vorhanden sind oder nicht. Kunden sind in Bezug auf diese Faktoren gleichgültig.

5. **Rückweisungsmerkmale:** Hin und wieder gibt es Merkmale, die direkt zur **Unzufriedenheit** des Kunden führen. Im Kano Modell werden sie als Rückweisungsmerkmale bezeichnet.



Kano-Modell - Diagramm

1.2.3 Softwarequalität

Softwarequalität bezieht sich auf die Gesamtheit der Merkmale und Eigenschaften einer Software, die ihre Fähigkeit bestimmen, bestimmte Anforderungen zu erfüllen und die Kundenerwartungen zu erfüllen. Es handelt sich um einen umfassenden Begriff, der verschiedene Aspekte der Softwareentwicklung und Nutzung abdeckt.

- **Zuverlässigkeit** → Zuverlässigkeit bezieht sich auf die Fähigkeit der Software, konsistente und genaue Ergebnisse unter verschiedenen Bedingungen und über einen bestimmten Zeitraum hinweg bereitzustellen. *Reife, Fehlertoleranz (funktioniert auch bei Fehlern), Wiederherstellbarkeit*

- **Funktionalität** → Funktionalität ist ein grundlegendes Merkmal, das sicherstellt, dass die Software die gewünschten Aufgaben korrekt ausführt. *Angemessenheit, Interoperabilität, Sicherheit*

- **Benutzbarkeit**→ Eine gute Softwarequalität beinhaltet auch eine benutzerfreundliche Schnittstelle, die leicht verständlich und einfach zu bedienen ist. *Verständlichkeit, Erlernbarkeit, Bedienbarkeit*

- **Effizienz**→ Die Software sollte Ressourcen effizient nutzen, um ihre Aufgaben mit minimalen Systemressourcen (CPU, Speicher, etc.) zu erledigen. *Zeitverhalten, Verbrauchsverhalten*

- **Wartbarkeit**→ Wartbarkeit bezieht sich darauf, wie einfach es ist, die Software zu pflegen und zu aktualisieren. Eine wartbare Software ermöglicht es Entwicklern, Änderungen vorzunehmen, Fehler zu beheben und neue Funktionen hinzuzufügen, ohne unerwünschte Seiteneffekte zu verursachen. *Analysierbarkeit, Änderbarkeit*

- **Portabilität**→ Eine portable Software kann ohne größeren Aufwand auf unterschiedlichen Systemen eingesetzt werden. *Anpassbarkeit, Austauschbarkeit, Installierbarkeit*

Softwaretest Ein Softwaretest prüft und bewertet Software auf Erfüllung der für ihren Einsatz definierten Anforderungen und misst ihre Qualität. Die gewonnenen Erkenntnisse werden zur Erkennung und Behebung von Softwarefehlern genutzt. Tests während der Softwareentwicklung dienen dazu, die Software möglichst fehlerfrei in Betrieb zu nehmen. Man unterscheidet zwischen **White-Box-Testing** (Tests mit Kenntnissen, auch auf Code Ebene) und **Black-Box-Testing** (Ohne Kenntnis über die Funktionalität und ohne Code). Dafür gibt es unterschiedliche Testverfahren. Es gibt 4 grundsätzliche Testverfahren.

1. **Komponententest (Unittest)** Einzelne Komponenten und Module werden überprüft. Dies ist ein White-Box-Test und wird vom Entwickler durchgeführt. Dies kann mit gewissen Frameworks automatisiert werden.

2. **Integrationstest** Diese Tests überprüfen, ob mehrere Bestandteile des Gesamtsystems reibungslos und fehlerfrei miteinander zusammenspielen.

3. **Systemtest** Hierbei wird das ganze System zum ersten mal als Ganzes getestet. Dies geschieht meistens auf einem Testsystem, welches das Produktivsystem des Kunden darstellen soll.

4. **Abnahmetest** Das ist der entgültige Test vor der auslieferung and die Geräte der Kunden. Hierbei testet der Auftraggeber die Funktionalität. Es handelt sich um einen Black-Box-Test.

1.2.4 Barrierefreiheit

Die Barrierefreiheit ist durch verschiede Richtlinien geregelt. Durch die EU-Richtline EU 2016/2102 und das BITV 2.0. Ziel dieser Richtlinien ist eine **grundsätzlich uneingeschränkt barrierefreie Gestaltung moderner Informations- und Kommunikationstechnik zu ermöglichen.**

Im IT-Bereich ist die Barrierefreiheit folgendermaßen definiert: Barrierefreiheit im IT-Bereich bezieht sich auf die Gestaltung von Informationstechnologien und digitalen Diensten, um sicherzustellen, dass Menschen mit unterschiedlichen Fähigkeiten und Einschränkungen sie effektiv nutzen können. Dies umfasst Menschen mit Behinderungen, aber auch ältere Menschen oder solche mit vorübergehenden Einschränkungen.

Es gibt verschiede Beispiele der Umsetzung

- Eindeutige Überschriften verwenden, durch Anpassung von Styles *<h1> in HTML*
- Bei Bildern auch Alternativtexte verwenden
- Skalierbarkeit der Texte
- Navigation ohne Maus ermöglichen
- Sinnvoller Aufbau von Websiten für Text-To-Speech

1.2.5 Begriffsklärungen

Qualität: "Grad, in dem ein Satz inhärenter Merkmale eines Objekts Anforderungen erfüllt" (DIN EN ISO 9000) inhärent → innewohnend

DIN: Deutsches Institut für Normung

EN: Europäischen Normungsinstitut

ISO: International Organization for Standardization

IEC: International Electrotechnical Commission

Qualitätsspolitik Die Qualitätspolitik ist eine formale Erklärung eines Unternehmens, die seine Verpflichtung zur Qualität und Kundenzufriedenheit festlegt.

Qualitätsprüfung Die Qualitätsprüfung bezeichnet den Prozess der systematischen Überprüfung von Produkten oder Dienstleistungen, um sicherzustellen, dass sie den festgelegten Qualitätsstandards entsprechen.

Qualitätslenkung Qualitätslenkung bezieht sich auf die Umsetzung von Maßnahmen, um sicherzustellen, dass die Ergebnisse der Qualitätsprüfung den festgelegten Standards entsprechen.

Qualitätsplanung Die Qualitätsplanung bezieht sich auf den Prozess, bei dem Ziele und Anforderungen an die Qualität eines Produkts oder einer Dienstleistung festgelegt werden.

Qualitätssicherung Qualitätssicherung umfasst alle geplanten und systematischen Maßnahmen, die in einem Qualitätsmanagementsystem implementiert werden, um sicherzustellen, dass ein Produkt oder eine Dienstleistung die festgelegten Qualitätsanforderungen erfüllt.

Bedarfsanalyse Eine Bedarfsanalyse ist ein Verfahren zur Ermittlung des Bedarfs, also der Lücken zwischen den derzeitigen und den angestrebten Ergebnissen. Bei richtiger Anwendung bietet diese Analyse wertvolle Einblicke in die Prozesse Ihres Teams und zeigt Bereiche für Effizienzsteigerungen auf. Es gibt drei Methoden.

1. **Fragebögen** Fragebögen und Befragungen sind die beliebtesten Methoden zur Erhebung von Bedarfsdaten. Ein Fragebogen ist ein einfaches Formular mit allgemeinen Fragen, die mit Ja oder Nein beantwortet werden können. Damit lassen sich schnell Informationen ermitteln, wenn Sie beispielsweise die Wirksamkeit Ihrer Markenidentität bewerten wollen.

2. **Befragungen** Viele Teams nutzen Befragungen, um externe Informationen zur Kundenerfahrung zu sammeln. Befragungen enthalten oft offene Fragen, sodass sie detailliertere Informationen liefern als Fragebögen. So können Sie schnell genaue Informationen erhalten, etwa wenn Sie das Kundenerlebnis nach dem Kauf aus Sicht des Kunden bewerten möchten.

3. **Fokusgruppe** Eine Fokusgruppe ist ein Gespräch mit einer kleinen Anzahl von Teilnehmern, die ähnliche Eigenschaften oder Erfahrungen mitbringen. Sie erfordern zwar erheblich mehr Zeit als die beiden anderen Methoden, dafür liefern Fokusgruppen umfassende Informationen über den Bedarf und das Kundenerlebnis. So können Sie zum Beispiel herausfinden, wie die Kunden Ihre Marke erleben und was ihrer Meinung nach verbessert werden könnte.

1.3 Datenschutz

Unter Datenschutz kann man den Schutz vor Missbrauch personenbezogener Daten verstehen. Grundsätzlich sollte jeder Mensch selbst entscheiden was mit seinen persönlichen Daten geschieht. Dieses Recht wird aber regelmäßig gebrochen, da personenbezogene Daten oft wirtschaftlich verwendet werdet. Aber auch Geheimdienste verarbeiten diese Daten.

1.3.1 DSGVO und BDSG

Ein Schutz gegen Missbrauch der persönlichen Daten ist der eigene Verantwortungsvolle Umgang mit seinen Daten. Zusätzlich gibt es Richtlinien und Gesetze, die den Datenschutz regeln. In Unternehmen oder Behörden wird zusätzlich ein Datenschutzbeauftragter implementiert. In Deutschland ist der Datenschutz durch die DSGVO und der BDSG geregelt.

DSGVO Die Datenschutz-Grundverordnung ist eine EU-Verordnung, die am 25. Mai 2018 in Kraft getreten ist. Ihr Hauptziel ist es, den Schutz personenbezogener Daten innerhalb der Europäischen Union zu stärken und einheitliche Datenschutzstandards in allen Mitgliedsstaaten zu etablieren. Die DSGVO betrifft nicht nur Unternehmen innerhalb der EU, sondern auch solche außerhalb, wenn sie personenbezogene Daten von EU-Bürgern verarbeiten.

1. Transparenz und Modalitäten
2. Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten
3. Berichtigung und Löschung
4. Widerspruchsrecht
5. Beschränkungen

BDSG Das Bundesdatenschutzgesetz ist das nationale Datenschutzgesetz in Deutschland und regelt den Umgang mit personenbezogenen Daten auf nationaler Ebene. Das BDSG wurde im Zuge der Einführung der DSGVO angepasst, um diese zu ergänzen und nationale Besonderheiten zu berücksichtigen.

1.3.2 Rechte betroffener Personen

Die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union ist eine umfassende Datenschutzregelung, die die Rechte betroffener Personen stärkt. Hier sind die wichtigsten Rechte, die betroffene Personen gemäß der DSGVO haben:

1. **Recht auf Auskunft (Artikel 15):** Betroffene Personen haben das Recht, von der verarbeitenden Stelle eine Bestätigung darüber zu erhalten, ob personenbezogene Daten über sie verarbeitet werden, und wenn ja, Zugang zu diesen Informationen zu erhalten.

2. **Recht auf Berichtigung (Artikel 16):** Betroffene Personen haben das Recht, die Berichtigung unrichtiger oder unvollständiger personenbezogener Daten zu verlangen.

3. **Recht auf Löschung (Artikel 17):** Unter bestimmten Umständen können betroffene Personen das Recht auf Löschung ihrer personenbezogenen Daten verlangen, zum Beispiel wenn die Daten nicht mehr für die Zwecke, für die sie erhoben wurden, benötigt werden.

4. **Recht auf Einschränkung der Verarbeitung (Artikel 18):** Betroffene Personen haben unter bestimmten Bedingungen das Recht, die Einschränkung der Verarbeitung ihrer personenbezogenen Daten zu verlangen.

5. **Recht auf Datenübertragbarkeit (Artikel 20):** Betroffene Personen haben das Recht, die sie betreffenden personenbezogenen Daten, die sie einer verantwortlichen Stelle bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

6. **Widerspruchsrecht (Artikel 21):** Betroffene Personen können der Verarbeitung ihrer personenbezogenen Daten aus Gründen, die sich aus ihrer besonderen Situation ergeben, widersprechen. Es sei denn, es liegen zwingende schutzwürdige Gründe für die Verarbeitung vor.

7. **Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (Artikel 22):** Betroffene Personen haben das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihnen gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

8. **Beschwerderecht bei einer Aufsichtsbehörde (Artikel 77):** Betroffene Personen haben das Recht, bei einer Datenschutz-Aufsichtsbehörde eine Beschwerde einzureichen, wenn sie der Ansicht sind, dass die Verarbeitung ihrer personenbezogenen Daten gegen die DSGVO verstößt.

1.3.3 Standard-Datenschutzmodell

Das Standard-Datenschutzmodell (SDM) ist ein Modell, das die Sicherheits- und Datenschutzanforderungen für Informationssysteme spezifiziert. Es wurde von der Datenschutzkonferenz (DSK) in Deutschland entwickelt und dient als Orientierung für die Umsetzung von Datenschutz in Informationssystemen.

Die Gewährleistungsziele im Kontext des Standard-Datenschutzmodells (SDM) können sich auf die folgenden Prinzipien beziehen:

1. **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben:** Datenverarbeitung sollte auf einer rechtmäßigen Grundlage erfolgen, und die Verarbeitung sollte fair und transparent sein.

2. **Zweckbindung:** Personenbezogene Daten dürfen nur für vorher festgelegte, eindeutige und legitime Zwecke erhoben werden.

3. **Datenminimierung:** Es sollte nur die für den jeweiligen Verarbeitungszweck notwendige Menge an personenbezogenen Daten erfasst und verarbeitet werden.

4. **Richtigkeit der Daten/Integrität:** Personenbezogene Daten sollten korrekt und aktuell sein, und es sollten Maßnahmen ergriffen werden, um sicherzustellen, dass dies der Fall ist. Speicherbegrenzung und Datenintegrität: Daten sollten nur so lange gespeichert werden, wie es für den Verarbeitungszweck erforderlich ist, und es sollten Maßnahmen ergriffen werden, um die Integrität der Daten zu schützen.

5. **Vertraulichkeit und Datensicherheit:** Schutz vor unbefugtem Zugriff, Verlust oder Zerstörung personenbezogener Daten durch geeignete Sicherheitsmaßnahmen.

6. **Rechenschaftspflicht:** Die verantwortliche Stelle ist dafür verantwortlich, die Einhaltung der Datenschutzgrundsätze nachzuweisen und nachvollziehbar zu dokumentieren.

7. **Datenschutz durch Voreinstellungen (Privacy by Design and by Default):** Datenschutz soll bereits bei der Entwicklung von Informationssystemen berück-sichtigt werden.

1.4 IT-Sicherheit

IT-Sicherheit, auch als Informationstechnologiesicherheit oder kurz IT-Sicherheit bezeichnet, bezieht sich auf den Schutz von Informationstechnologien (IT) und den damit verbundenen Systemen, Daten, Netzwerken und Diensten vor verschiedenen Bedrohungen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen. Das Hauptziel der IT-Sicherheit besteht darin, die IT-Infrastruktur vor unbefugtem Zugriff, Datenverlust, Manipulation, Diebstahl, Virenbefall und anderen potenziellen Schäden zu schützen.

- **Vertraulichkeit:** Sicherstellen, dass sensible Informationen nur von autorisierten Personen oder Systemen zugänglich sind.
- **Integrität:** Garantieren, dass Daten und Systeme vor unbefugten Änderungen oder Manipulationen geschützt sind.
- **Verfügbarkeit:** Gewährleisten, dass Systeme und Daten jederzeit für autorisierte Benutzer verfügbar sind, ohne durch Angriffe oder Ausfälle beeinträchtigt zu werden.

1.4.1 ISMS Informationssicherheitmanagement

Es handelt sich um einen systematischen Ansatz zur Verwaltung und Sicherung von Informationen in einer Organisation. Das ISMS ist auf die Implementierung, Überwachung, Wartung und kontinuierliche Verbesserung von Informationssicherheitsmaßnahmen ausgerichtet.

Ein ISMS basiert in der Regel auf einem definierten Rahmenwerk, wie beispielsweise der internationalen Norm ISO/IEC 27001. Diese Norm legt die Anforderungen für die Einführung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines ISMS fest.

1.4.2 IT-Grundschutz

Der IT-Grundschutz wurde vom BSI (Bundesamt für Sicherheit und Informationstechnik) entwickelt. Dabei handelt es sich um ein Konzept, eine Methodik, die die Informationssicherheit in Behörden und Unternehmen erhöhen soll. Der IT-Grundschutz gilt als Maßstab für Absicherung von Informationen und den Aufbau eines Managementsystems für Informationssicherheit (ISMS). Dies ist kompatibel zur ISO-27001-Norm.

1.4.3 IT-Sicherheitsgesetz

Das IT-Sicherheitsgesetz ist eine deutsche Gesetzgebung, die darauf abzielt, die Sicherheit von Informationstechnologien in kritischen Infrastrukturen zu gewährleisten. Es verpflichtet Betreiber bestimmter Sektoren wie Energie, Telekommunikation und Gesundheit dazu, angemessene Schutzmaßnahmen zu ergreifen, um Cyberangriffe zu verhindern. Zudem **müssen sie Sicherheitsvorfälle** melden und mit den Vorgaben für IT-Sicherheit des Gesetzes konform gehen. Das Ziel ist es, die Widerstandsfähigkeit gegenüber digitalen Bedrohungen zu stärken und die Integrität kritischer Infrastrukturen zu schützen.

1.4.4 IT-Angriffe

- **Phishing:** Phishing bezeichnet den Versuch, durch Täuschung an vertrauliche Informationen zu gelangen, indem beispielsweise gefälschte E-Mails oder Websites verwendet werden, die legitimen Institutionen oder Unternehmen ähneln.

- **Vishing:** Vishing ist eine Form des Phishings, bei dem Angreifer versuchen, durch Telefonanrufe oder VoIP (Voice over Internet Protocol) an sensible Informationen zu gelangen, indem sie sich als vertrauenswürdige Quelle ausgeben.

- **Pharming:** Pharming ist eine betrügerische Technik, bei der die DNS-Einstellungen manipuliert werden, um Benutzer zu gefälschten Websites umzuleiten. Das Ziel ist es, vertrauliche Informationen abzugreifen.

- **Spoofing:** Spoofing bezieht sich auf das Vortäuschen einer falschen Identität oder Herkunft, um Nutzer zu täuschen. Beispiele sind IP-Spoofing, E-Mail-Spoofing oder URL-Spoofing, bei denen die wahre Identität oder Quelle verschleiert wird.

- **Nicknapping:** Der Begriff "Nicknapping" ist weniger gebräuchlich, beschreibt das "Entführen" oder unrechtmäßige Erlangen von Benutzer-IDs oder Nicknames in Online-Plattformen oder sozialen Netzwerken.

- **Spam:** Spam bezeichnet unerwünschte und oft massenhaft versendete Nachrichten, insbesondere in Form von E-Mails. Das Hauptziel von Spam ist oft Werbung oder das Verbreiten schädlicher Links.

- **Spyware:** Spyware ist schädliche Software, die ohne Wissen des Benutzers Informationen über dessen Aktivitäten sammelt. Dies kann das Erfassen von Tastatureingaben, Passwörtern oder persönlichen Daten umfassen.

- **Wurm:** Ein Wurm ist ein selbstreplizierender Schadcode, der sich ohne menschliches Zutun verbreitet. Im Gegensatz zu Viren benötigt ein Wurm keine infizierten Dateien, sondern verbreitet sich eigenständig durch Netzwerke.

- **Ransomware:** Ransomware ist schädliche Software, die die Daten eines Benutzers verschlüsselt und dann Lösegeld fordert, um die Daten wieder freizugeben. Es ist eine Form der Erpressung im digitalen Raum.

- **DDoS (Distributed Denial of Service):** DDoS-Angriffe zielen darauf ab, die Verfügbarkeit eines Dienstes, einer Website oder eines Netzwerks zu beeinträchtigen, indem eine große Anzahl von Anfragen gleichzeitig darauf gerichtet wird, sodass die Ressourcen überlastet werden.

- **Botnetze:** Ein Botnetz ist ein Netzwerk von infizierten Computern, die von einem Angreifer ferngesteuert werden. Diese "Bots" können für verschiedene Zwecke eingesetzt werden, einschließlich DDoS-Angriffen oder dem Versenden von Spam.

- **APT-Angriffe (Advanced Persistent Threats):** APT-Angriffe sind hochentwickelte und gezielte Cyberangriffe, bei denen Angreifer häufig über längere Zeiträume hinweg unbemerkt bleiben, um sensible Informationen zu stehlen oder Systeme zu sabotieren

1.4.5 Informationsschutzbeauftrager - ISB

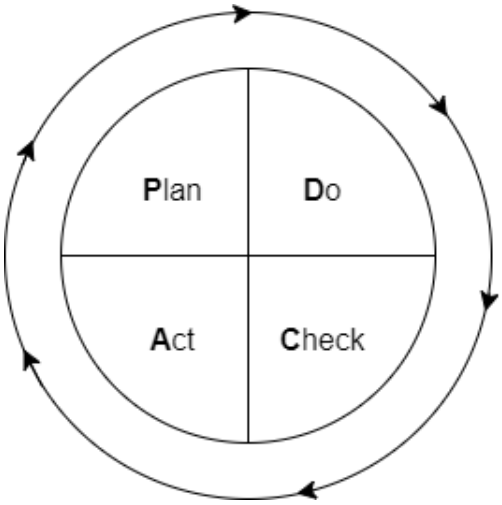
Ein Informationssicherheitsbeauftragter ist für alle Fragen rund um die Informationssicherheit in der Institution zuständig. Zu seinen Aufgaben gehört es,

- den Sicherheitsprozess zu steuern und zu koordinieren,
- die Leitung bei der Erstellung der Sicherheitsleitlinie zu unterstützen,
- die Erstellung des Sicherheitskonzepts und zugehöriger Teilkonzepte und Richtlinien zu koordinieren,
- Realisierungspläne für Sicherheitsmaßnahmen anzufertigen sowie ihre Umsetzung zu initiieren und zu überprüfen,
- der Leitungsebene und anderen Sicherheitsverantwortlichen über den Status der Informationssicherheit zu berichten,
- sicherheitsrelevante Projekte zu koordinieren,
- sicherheitsrelevante Vorfälle zu untersuchen sowie
- Sensibilisierungen und Schulungen zur Informationssicherheit zu initiieren und zu koordinieren.

Ein ISB sollte Erfahrung und Wissen sowohl auf den Gebieten der Informationssicherheit als auch der IT besitzen. Darüber hinaus sollte er die Geschäftsprozesse der Institution kennen.

1.4.6 Sicherheitsprozess

Informationssicherheit ist kein Zustand, der einmal erreicht wird und dann fortbesteht, sondern ein Prozess, der kontinuierlich angepasst werden muss. Geänderte Verfahren und Prozesse in einer Institution, der Wandel in den gesetzlichen Rahmenbedingungen, neue Technik, aber auch bislang unbekannte Schwachstellen und daraus erwachsende Gefährdungen stellen immer wieder neue Anforderungen, so dass die nachhaltige Angemessenheit und Wirksamkeit nicht automatisch gewährleistet sind. Der gesamte Sicherheitsprozess unterliegt daher einem Lebenszyklus, der sich in folgende Phasen gliedert:



PDCA - Zyklus

In der Praxis

1. Initiierung, Erstellung einer Informationssicherheitsleitlinie und Aufbau einer Sicherheitsorganisation
2. Erstellung eines Sicherheitskonzepts
3. Umsetzung des Konzepts
4. Aufrechterhaltung und Verbesserung

1.4.7 Vorgehensweise

Die **Basis-Absicherung** ist für Institutionen interessant, die einen Einstieg in den IT-Grundschutz suchen und schnell alle relevanten Geschäftsprozesse mit Basismaßnahmen absichern möchten.

Die **Kern-Absicherung** lenkt die Sicherheitsmaßnahmen auf die Kronjuwelen einer Institution, also besonders wichtige Geschäftsprozesse und Assets. Diese Variante zielt damit auf die vertiefte Absicherung der kritischsten Bereiche ab.

Die **Standard-Absicherung** entspricht der empfohlenen IT-Grundschutz-Vorgehensweise (vgl. früherer BSI-Standard 100-2). Sie hat einen umfassenden Schutz für alle Prozesse und Bereiche der Institution als Ziel.

1. Analyse des IT-Zustandes
2. Schutzbedarfsfestellung
3. Auswahl der Sicherheitsanforderungen
4. Realisierung der Maßnahmen
5. Aufrechterhaltung und kontinuierliche Verbesserung

1.4.8 Schutzbedarfsfestellung

Die "Schutzbedarfsfeststellung" ist ein Prozess in der Informationssicherheit, bei dem ermittelt wird, welche Informationen oder Systeme innerhalb einer Organisation welchen Schutzbedarf haben. Dieser Schutzbedarf hängt von verschiedenen Faktoren ab, darunter die Sensibilität der Informationen, ihre Bedeutung für die Geschäftsprozesse und die potenziellen Auswirkungen eines Sicherheitsvorfalls. Die Feststellung des Schutzbedarfs bildet die Grundlage für die Implementierung angemessener Sicherheitsmaßnahmen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen