IT Service Continuity Management

Prävention, IT-Notfallvorsorge, Resilienz

Kapitel 4

Die Policy schreiben: Der Arbeitsauftrag

Mit der Policy (auch »Richtlinie«, »Leitlinie« oder »Strategie« genannt) werden der eigentliche Arbeitsauftrag, die Organisation, die Rollen und der Nutzen/Zweck eines ITSCM definiert, beschrieben und durch das Top-Management freigegeben. Diese Policy muss unbedingt mit der BCM- und der ISM-Policy abgestimmt sein (sofern diese existieren). Sie dürfen sich nicht widersprechen und müssen sich idealerweise ergänzen.

»Freude an der Arbeit lässt das Werk trefflich geraten.« (Aristoteles)

In einer Policy wird der eigentliche Arbeitsauftrag des ITSCM definiert. *Und nur dort!*

In der Policy haben Sie die Möglichkeit, *Inhalte zu definieren* und für *Transparenz* und *Abgrenzung* zu sorgen. Daher sollten Sie unbedingt die notwendige Zeit investieren und diese Richtlinie klar ausarbeiten. Ein unklarer Arbeitsauftrag ist nämlich kein Arbeitsauftrag! Und ohne klaren Auftrag machen Sie nichts im ITSCM. 😉

Das ist etwas, was ich aus über 30 Jahren praktischer Erfahrung im Projektmanagement gelernt und für das ITSCM adaptiert habe. Oft wird nämlich aus Unwissenheit vieles wild durcheinandergeworfen. Das geschieht, weil Ihr Gegenüber nicht so tief in der Materie steckt und die Gedankengänge, die Ihnen offensichtlich erscheinen, nicht so einfach nachvollziehen kann.

Legen Sie in der Policy also den Grundstein für ein gemeinsames Verständnis und für den Sinn, Zweck und Mehrwert eines ITSCM. In diesem Dokument grenzen Sie sich deutlich ab. Hier werden Erwartungshaltungen dokumentiert und die Ergebnisse vordefiniert.

Sie sehen: Die Policy ist das mit Abstand wichtigste Dokument für Ihr ITSCM.

Tipp aus der Praxis

Fangen Sie bei der ersten Policy mit wenigen konkreten Vorgaben an und erweitern Sie diese sukzessive im Laufe der nächsten Jahre. Es nützt nichts, eine erste Policy von 45 Seiten zu haben, die Vorgaben und Erwartungshaltungen beinhaltet, die sich zum gegebenen Zeitpunkt unmöglich realisieren lassen.

Das sorgt nur für Frust auf ganzer Linie und auf allen Seiten. Hier ist weniger definitiv mehr. Sonst »verbrennen« Sie sich Ihr ITSCM (inklusive dessen Mitarbeiter), noch bevor es richtig losgeht. Und eine unnötige Fluktuation von Mitarbeitern verzögert Ihren ITSCM-Aufbau und -Betrieb noch weiter.

Damit fokussieren Sie sich und sichern sich gleichzeitig gegen falsche Erwartungshaltungen ab. Nutzen Sie eine Policy daher zum offenen Informationsaustausch und auch als Diskussionsgrundlage.

Die Policy sollte definitiv kein Geheimpapier sein, das im Hochsicherheitstresor unter Verschluss liegt und nur mit einer 128-stelligen Zahlenkombination am Montagmittag um 12.12 Uhr zugängig ist. Dann macht man etwas falsch.

Ich habe das Schreiben der Policy daher bewusst an dieser frühen Stelle platziert. Jetzt haben Sie schon die ersten Erfahrungen gesammelt, und die Mitarbeiter oder wenigstens der ITSC-Manager wurde geschult. Sie haben angefangen, sich zu vernetzen; die ersten Überlegungen, wie das ITSCM weiter aufgebaut werden soll, wurden ausgetauscht etc. Nun sollten Sie unbedingt genau festlegen, worum es in »Ihrem« ITSCM gehen soll.

Vorgabe oder selbst aktiv werden?

Natürlich kann es sein, dass Sie die Policy vorab vom ITSCM-Owner erstellen lassen oder sie vom Mutterkonzern oder von der Firmenzentrale vorgegeben bekommen. Ich gehe hier aber davon aus, dass es noch keine fertige Policy oder Vorgaben gibt und dass Sie alles neu aufbauen müssen. So wissen Sie auch, wie man das Ganze aufbaut, was in eine Policy gehört und wie der spätere Weg zur Offizialisierung aussieht.

Mit den Templates beim Downloadmaterial stelle ich Ihnen eine Policy mit Beispieltexten zur Verfügung. Vielleicht können Sie dort die eine oder andere Anregung für Ihre Organisation mitnehmen.

Policys sollten in etwa 10 bis 15 Seiten umfassen. Auf ihnen wird alles nur sehr grob und oberflächlich beschrieben. Eine detailliertere Beschreibung findet in anderen Dokumenten statt. Schreiben Sie diese Policy in einfacher Sprache. Hier müssen Sie niemandem etwas beweisen, niemanden mit Fachvokabular oder fancy Buzzwords beeindrucken. Je einfacher, desto verständlicher. Das sollte Ihr Ziel sein.

4.1 Den Zweck und die Ziele eines ITSCM definieren

Als Erstes geht es darum, den Arbeitsauftrag und die strategischen Vorgaben für das ITSCM so genau wie möglich zu beschreiben. Planen Sie genügend Zeit ein. Denn oft ist es gar nicht mal so einfach, alles auf den Punkt zu bringen, detailliert und verständlich zu beschreiben – vor allem, wenn Sie gerade erst mit dem ITSCM anfangen und Ihnen noch der Gesamtüberblick fehlt.

Stellen Sie sich folgende Fragen: Was erwartet man von einem ITSCM? Nur die Erhöhung der Resilienz einer Organisation ist wohl etwas zu wenig. Sollen z. B. IT-Notfallvorsorgemaßnahmen mit den technischen Bereichen erarbeitet und umgesetzt werden? Sollen technische Übungen und Tests stattfinden, die vom ITSCM koordiniert werden? Soll eine

organisationsweite Awareness-Kampagne geplant und durchgeführt werden? Soll ein ITSCM die IT auf »Herz und Nieren« prüfen? Das heißt, soll das ITSCM auf Schwachstellen- und Fehlersuche gehen? Soll ein ITSCM das vorhandene BCM intensiv unterstützen? Soll ein ITSCM IT-Risiken definieren und bewerten? Soll das ITSCM nützliche KPIs erzeugen?

Vermeiden Sie Unklarheiten und Blackboxes!

In der Policy sollten Sie die ganzen Anforderungen an ein ITSCM detailliert aufführen. Achten Sie bei allen Inhalten auf eine einfache Sprache bzw. einfache Formulierungen, denn schließlich wird diese Policy auch von allen Mitarbeitern der Organisation gelesen. Und Sie möchten ja alle Mitarbeiter bestmöglich mit auf die gemeinsame Reise nehmen und ihnen keine Blackbox vorsetzen.

Eine *Blackbox* ist etwas, bei dem man nur sieht, was hineingeht und was herauskommt – aber nicht, was drinnen passiert. Das ist für viele Menschen sehr ungewöhnlich, und viele bauen angesichts dessen spontan eine innere Abwehrhaltung auf.

Schrecken Sie auch niemanden mit unnötigem Fachchinesisch oder akademischer Prosa und unverständlichen Schachtelsätzen ab. Sie suchen Verbündete und keine Gegner! 😉

4.2 Den Geltungsbereich bestimmen

Wenn Sie festgelegt haben, was vom ITSCM erwartet wird, geht es an den Geltungsbereich. Mit einem Geltungsbereich definieren Sie genau, wofür Ihr ITSCM zuständig sein soll und wofür nicht. Das bedeutet, hier setzen Sie einen örtlichen Fokus für das ITSCM. Sie können es z. B. organisationsweit definieren oder auch nur lokal bzw. sehr eingegrenzt einsetzen, also beispielsweise:

- für einen Kontinent
- für ein Land
- für ein Bundesland
- für eine Stadt
- für einen Standort (oder Teile des Standortes)
- für einen festgelegten Bereich innerhalb Ihrer Organisation
- für alle RZ-Standorte
- für einen RZ-Standort
- für einen Teil des RZ (z. B. für den hochsicheren Bereich)
- etc.

Dabei sind Sie vollkommen frei. Oft gibt es auch eine (Konzern-)Zentrale oder einen Mutterkonzern bzw. ein Headquarter, das für alle angeschlossenen oder nachgeordneten Bereiche Vorgaben erstellt, die dann nur noch lokal angepasst werden müssen (an andere Gesetze, Normen, Vorschriften etc.).

Ein solcher Aufbau könnte wie folgt aussehen:

> Diese ITSCM-Policy ist für »Name der Organisation« in:
>
> - »alle Standorte« (Länder)
> - »Name der Standorte« (Land)
> - »Name der Lokation« (Ort)
> - »Name der Abteilung« (Ort)
> - »nur ein bestimmter Bereich« (Ort) gültig.
>
> Das ITSCM bezieht sich auf alle **Prozesse, (IT-)Services** sowie auf die gesamte **IT-Infrastruktur** mit allen **Informationen**, **Anwendungen** und **Systemen**. Sie gilt für alle Mitarbeiter sowie für alle Personen, die
>
> - Zugang zur IT-Infrastruktur,
> - Zugriff auf Informationen,
> - Zugang zu IT-Anwendungen oder IT-Systemen haben, die für die Aufgabenerfüllung genutzt werden.
>
> Diese Policy muss von allen Mitarbeitern wie auch von allen externen Dienstleistern beachtet werden. Alle Verträge mit Dienstleistern, die Dienstleistungen mit Relevanz für das ITSCM betreffen, müssen mögliche Vorgaben aus dieser Policy berücksichtigen und erfüllen …

4.3 Allgemeine Definitionen

4.3.1 Das »Big Picture« (Vorgehensmodell)

In Abbildung 4.1 sehen Sie das »Big-Picture« zum ITSCM mit allen wichtigen Stationen und deren Abhängigkeiten. Es ist quasi das ganze ITSCM auf einen Blick.[1]

So ein »Big Picture« können Sie in die Policy aufnehmen, denn so sehen alle Beteiligten sofort, wie hochkomplex ein ITSCM ist und dass man ein ITSCM nicht mit einer Person mal so »nebenbei« machen kann. Gehen Sie ruhig ein wenig taktisch vor und präsentieren Sie Ihren Arbeitsbereich auch entsprechend. Dann kann niemand sagen, er hätte nicht gewusst, wie zeitaufwendig der Aufbau und Betrieb eines ITSCM sein kann.

1 Ich habe die Grafik vom Team der *BCM Academy GmbH* erhalten und finde, dass es Bände spricht. Es ist in meinen Augen die beste grafische Zusammenfassung eines ITSCM, die ich gefunden habe. Sie finden die Grafik beim Downloadmaterial zum Buch. Danke, Birthe! 😊

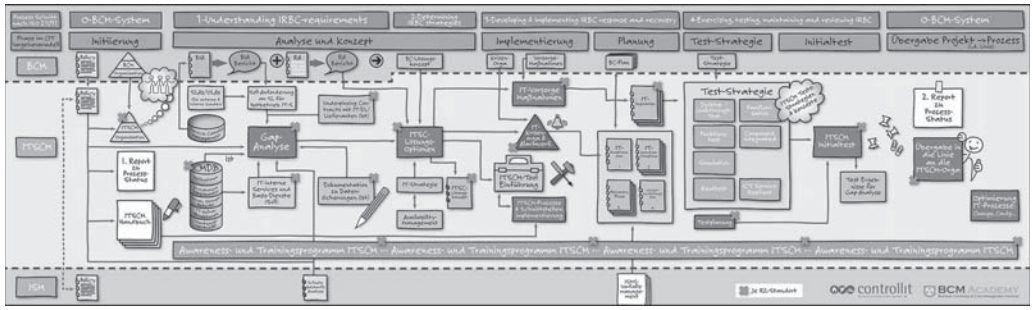

Abbildung 4.1: ITSCM-»Big Picture« (Quelle: BCM Academy GmbH, Lehrgang »Certified IT Service Continuity Manager, CITSCM«, https://www.bcmacademy.de/de/citscm)

In Abbildung 4.1 können Sie schon sehen, wie viel Fleißarbeit notwendig ist und dass eine sehr gute Vernetzung, Verzahnung und viel Durchhaltevermögen in der eigenen Organisation unumgänglich ist.

4.3.2 Rollenbeschreibungen in Kurzform

Als Nächstes werden in der Policy die ITSCM-Rollen erklärt. Dazu möchte ich die Rollen kurz beschreiben, die im direkten ITSCM-Umfeld zu finden sind und die maßgeblich das ITSCMS steuern bzw. beeinflussen. Eine ausführliche Beschreibung folgt später in Kapitel 7. Wichtig ist, dass nicht alle Rollen zwingend vorhanden sein müssen.

Betrachten Sie diese Liste und ihre Visualisierung in Abbildung 4.2 daher als mögliche und optimale Gesamtaufstellung. Dazu müssen Ihre Organisation und das ITSCM aber schon einen sehr hohen Reifegrad aufweisen. Auch haben manche Organisationen diese ITIL-Rollenbezeichnungen oder das entsprechende Wording nicht. Es ist wieder ein *Kann* und kein *Muss*. Daher sehen Sie es als unverbindlichen Vorschlag an.

Beschreiben Sie in Ihrer Policy kurz und knapp alle Rollen, am besten mit namentlicher Nennung der aktuellen Rolleninhaber (wenn es schon welche gibt):

- **ITSCM-Sponsor**

  Der ITSC-Sponsor ist für die dauerhafte Finanzierung eines ITSCMS verantwortlich. »Aktuell ist *Herr/Frau NN, (Vorstand),* aus dem Top-Management dazu benannt.«

- **ITSCM-Owner**

  Der ITSCM-Owner ist der Gesamtverantwortliche für das ITSCM. Diese Verantwortung kann nicht delegiert werden. Der ITSCM-Owner untersteht dem ITSCM-Sponsor und gibt Anforderungen an den oder die ITSC-Manager weiter. Er entwickelt eine ITSCM-Strategie. »Aktuell ist *Herr/Frau NN* dazu benannt.«

- **ITSC-Manager**

  Der ITSC-Manager ist umsetzungsverantwortlich für den Aufbau, Betrieb und die permanente Weiterentwicklung eines ITSCMS. Er untersteht direkt dem ITSCM-Owner. Er

gibt taktische Anforderungen (die aus dem Top-Management kommen) an die ITSC-Koordinatoren (operative Ebene) weiter. »Aktuell ist *Herr Frank M. Marks* dazu benannt.«

- **ITSC-Koordinator**

  Die ITSC-Koordinatoren unterstützen den oder die ITSC-Manager. Sie setzen die taktischen Anforderungen in ihren technischen und operativen Bereichen, Fachbereichen oder Arbeitseinheiten um. Der ITSC-Koordinator fungiert dabei als der zentrale Eingangs- und Ausgangskanal zu seinem Bereich und gleichzeitig als Multiplikator für das ITSCM. »Aktuell sind *[Liste mit Namen einfügen]* dazu benannt.« Hier werden meist mehrere ITSC-Koordinatoren benannt – je nach Größe Ihrer Organisation. Man kann aber auch hier erst mal mit einem ITSC-Koordinator anfangen und dann sukzessive erweitern. Die ITSC-Koordinatoren sind für ihren Bereich umsetzungsverantwortlich. Sie koordinieren und kontrollieren sämtliche Arbeiten in dem direkten Arbeitsumfeld, für das sie zuständig sind.

- **IT-Notfallteam(s) oder Reaktionsteam(s)**

  IT-Notfallteams bzw. Reaktionsteams unterstützen mit ihrem technischen Fachwissen den oder die ITSC-Koordinatoren z. B. bei:

  – Übungen und Tests
  – Vorbereitungen, Durchführungen, Nachbearbeitungen
  – IT-Notfällen und (IT-)Krisen, während der gesamten Dauer
  – der Umsetzung von IT-Notfallvorsorgemaßnahmen

  »Aktuell sind hier folgende Personen der Organisation benannt: *[Hier eine vollständige Liste aller Rolleninhaber anhängen]*.«

- **IT-Spezialist oder externe Spezialisten**

  IT-Spezialisten oder externe Spezialisten sind Fachkräfte mit außergewöhnlichem theoretischen und langjährigem praktischen Wissen. Diese Personen werden nur in wichtigen Situationen hinzugezogen, in denen das eigene Fachpersonal nicht mehr weiterkommt und Unterstützung braucht. Sie unterstützen den ITSC-Koordinator mit ihrem technischen Fachwissen bei z. B.:

  – Übungen und Tests
  – Vorbereitungen, Durchführungen, Nachbearbeitungen
  – bei IT-Notfällen und (IT-)Krisen während der gesamten Dauer
  – bei der Umsetzung von IT-Notfallvorsorgemaßnahmen

  »Aktuell sind hier folgende Personen/Firmen benannt *[Hier eine vollständige Liste aller Rolleninhaber anhängen]*.«

- **ITSCM-Team**

  Das ITSCM-Team unterstützt den oder die ITSC-Manager bei allen anfallenden Tätigkeiten im Tagesgeschäft. Die Größe des Teams sollte sich an der Anzahl der ITSC-Manager

orientieren. Als Standardwert würde ich pro ITSC-Manager einen ITSCM-Mitarbeiter ansetzen. Bei größeren Organisationen, in denen es etwa zwei ITSC-Manager und zwei ITSCM-Mitarbeiter gibt, könnte zudem ein kleines Backoffice mit einer oder zwei Personen als administrative Unterstützung durchaus sinnvoll sein. Aber dies ist natürlich auch von Ihrem verfügbaren Budget und Ihren personellen Rahmenbedingungen abhängig.

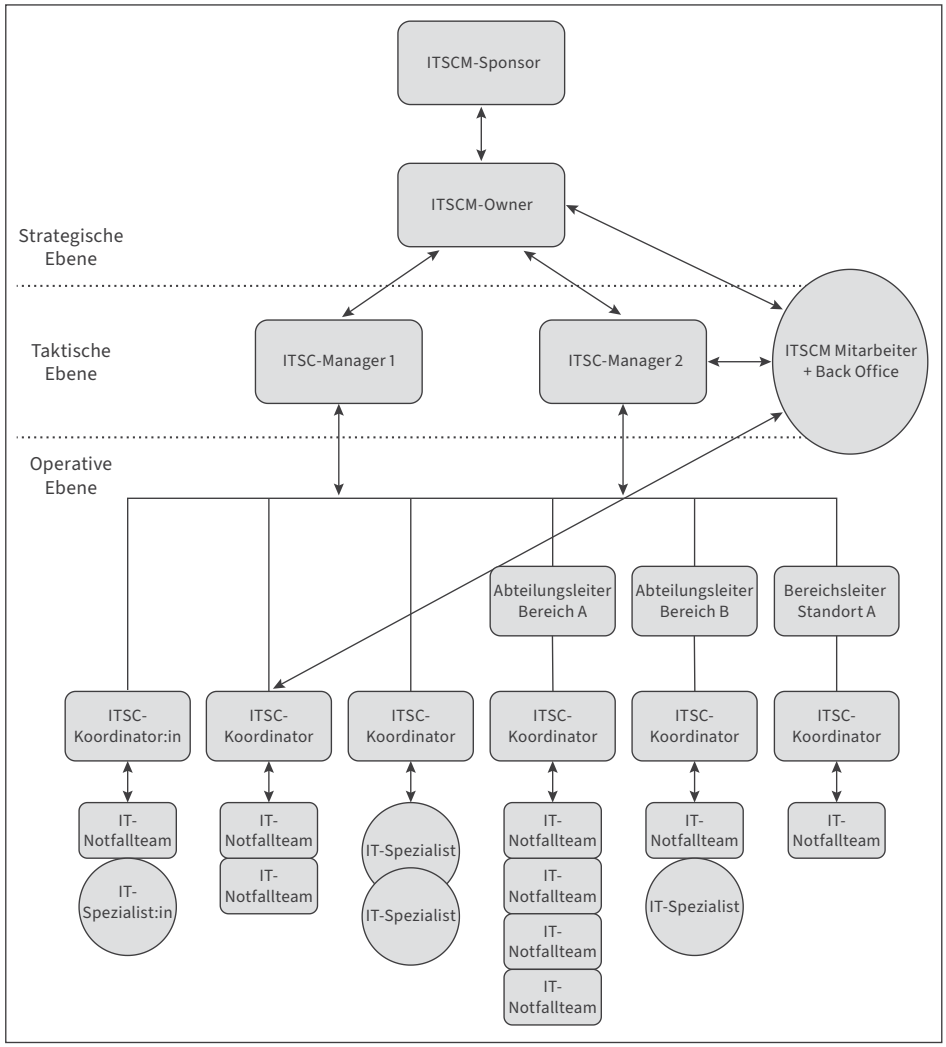

Abbildung 4.2: Übersicht der Rollen im voll ausgebauten ITSCM-Umfeld

4.3.3 Störungskategorien definieren

Um zu verdeutlichen, welche Schadensereignisse im Rahmen eines ITSCM betrachtet werden, folgt in der Policy eine kurze allgemeine Erläuterung der Ereignisse, die organisationsweit bei Ihnen vorab definiert werden muss.

Unter »notfallrelevanten Ereignissen« sind nur die Eskalationsstufen »IT-Notfall«, und »(IT-)Krise« zu verstehen. »Incidents« und »Major-Incidents« zählen dagegen zum allgemeinen Tagesgeschäft und werden durch die *Allgemeine Aufbauorganisation (AAO)* bearbeitet. Die AAO wird später noch genauer in Abschnitt 4.5 erklärt. Abbildung 4.3 bietet Ihnen einen Überblick über diese Stufen. Passen Sie diese Tabelle für Ihre Organisation an.

Incident (oder Minor-Incident)

Ein *Incident* (also eine interne Störung oder einfache Störung) ist eine Situation, in der Prozesse oder IT-Services (inklusive IT-Ressourcen) nicht wie vorgesehen funktionieren oder zur Verfügung stehen. Die dadurch entstehenden Schäden sind als gering einzustufen: Ein *geringer Schaden* ist ein Schaden, der im Verhältnis zum gesamten Haushaltsbudget zu vernachlässigen ist oder der die Aufgabenerfüllung nur unwesentlich beeinträchtigt. Eine *Störung* liegt vor, wenn unabhängig von der Ursache eine Größe sich nicht innerhalb des Sollbereichs bewegt bzw. wenn eine Abweichung vom Sollzustand auftritt. (Zur Definition des Soll-Zustands unbedingt die SLA-Vorgaben beachten!)

Incidents werden durch die im Tagesgeschäft integrierte Störungsbehebung beseitigt. Störungen können sich jedoch zu einem IT-Notfall oder einer (IT-)Krise ausweiten und sind deshalb genau zu beobachten, sorgfältig zu dokumentieren und zeitnah zu beheben. Dies ist jedoch nicht die Aufgabe eines ITSCM, sondern eines Störungsmanagements (*Incident-Managements*).

Incidents passieren bei der heutigen hochkomplexen IT jeden Tag zigfach, sind also kein Grund zur Panik. 😉

Bei einem IT-Dienstleister können sogar einige Hundert kleinere Incidents an der Tagesordnung sein. Auch das ist normal und abhängig davon, wie fein Sie ihre (Störungs-)Detektion oder ihre Schwellenwerte eingestellt bzw. definiert haben.

Beispiel: Ein kurzes Timeout (ein »Ruckler« oder eine zeitliche Verzögerung) kann schon ein vollautomatisiertes Incident-Ticket auslösen, das später wieder automatisiert auf »gelöst« gesetzt wird, wenn die Antwortzeit wieder stimmt. Das kann innerhalb von Sekunden oder Minuten passieren. Der Anwender bekommt davon normalerweise nichts mit.

Major-Incident (oder Großstörung)

Ein *Major-Incident* ist ein schwerwiegender und ungeplanter Incident, der gravierende Unterbrechungen der Geschäftstätigkeiten (auch beim Kunden) verursacht und mit höherer Dringlichkeit von der AAO gelöst werden muss.

IT-Notfall (oder auch kritischer Vorfall)

Ein kritischer Vorfall bzw. ein IT-Notfall ist ein Schadensereignis, bei dem (Geschäfts-) Prozesse oder (IT-)Ressourcen nicht wie vorgesehen funktionieren oder zur Verfügung stehen. Der Geschäftsbetrieb ist sehr stark beeinträchtigt. Es entstehen hohe bis sehr

hohe Schäden, die sich signifikant und in nicht akzeptablem Rahmen auf die Aufgabenerfüllung der Organisation auswirken. Der Schwerpunkt des IT-Notfalls liegt zwar auf der Verfügbarkeit, jedoch muss auch der Verlust der Integrität oder der Vertraulichkeit von schutzbedürftigen Daten als IT-Notfall angesehen werden. IT-Notfälle können nicht mehr im normalem Tagesgeschäft abgewickelt werden, sondern erfordern eine besondere Notfallbewältigungsorganisation, mit entsprechenden Sonderberechtigungen, z. B. eine *Besondere Aufbauorganisation (BAO)* mit einem Krisenstab und einem (IT-)Lagezentrum.

Definitionen anpassen

Sie können den IT-Notfall auch mit Ihren zeitkritischen Geschäftsprozessen bzw. zeitkritischen IT-Services verbinden. Das heißt, ist z. B. einer dieser zeitkritischen Geschäftsprozesse bzw. zeitkritischen IT-Services gestört, wird das automatisch als IT-Notfall deklariert und ausgerufen.

Ein IT-Notfall ist:

- ein Ereignis, das den Geschäftsbetrieb stark beeinträchtigt und somit einen länger andauernden Ausfall von (Geschäfts-)Prozessen und/oder IT-Ressourcen verursacht
- eine eskalierte Störung, die von der AAO nicht gelöst werden kann
- eine massive Störung wichtiger (IT-)Anwendungen bzw. des Geschäftsbetriebs oder ein Sicherheitsvorfall mit massiven Auswirkungen auf die Sicherheitsziele (Hier könnte aber auch schon die Informationssicherheit aktiv werden.)
- die Störung eines zeitkritischen Geschäftsprozesses oder eines zeitkritischen IT-Service
- *[Ihre Definition von IT-Notfall]*

Für die IT-Notfallbewältigung liegen idealerweise aktuelle und in der Praxis geprobte IT-Notfallpläne vor. Ein IT-Notfall, der mehr als 14 Wochentage andauert, wird automatisch zu einer (IT-)Krise hochgestuft. Auch dies können Sie anhand Ihrer Organisationsvorgaben natürlich ganz anders definieren oder regeln.

Beispiele für IT-Notfälle sind:

- **Ein Brand im Serverraum**, der eine aufwendige Sanierung wesentlicher Bereiche der Nutzfläche im Rechenzentrum sowie IT-Ersatzbeschaffungen erfordert
- **Mehrere IT-Systeme** sind aufgrund von Brand, Wasser, Vandalismus, Sabotage oder technischen Defekten ausgefallen. Dieser Ausfall kann mehrere Wochen dauern.
- Das **Kühlsystem für den Serverraum** fällt voraussichtlich für mehrere Wochen aus.
- **Massiver Ausfall des IT-Fachpersonals** für mehrere Monate wegen Pandemie, Unfall o. Ä. – insbesondere vor wichtigen Meilensteinen mit Außenwirkung
- Ein Defekt von mehr als der Hälfte der zentralen IT-Systeme durch z. B. **fehlerhafte Stromversorgung (Spannung/Frequenz)**

- Die **Vertraulichkeit** von Daten, IT-Anwendungen und IT-Systemen mit **hohem Schutzbedarf** bezüglich ihrer Vertraulichkeit ist nicht sicher gegeben. Das heißt, es liegen Hinweise auf einen unbefugten Zugriff vor.
- Die **Integrität** von Daten, IT-Anwendungen und IT-Systemen mit hohem Schutzbedarf ist nicht sicher gegeben. Das heißt, es liegen Hinweise auf Manipulation(en) vor. Die Integrität kann innerhalb der durch den Schutzbedarf vorgegebenen *maximal tolerierbaren Ausfallzeit (MTPD)* nicht wiederhergestellt bzw. verifiziert werden.
- Durch **Virenbefall** müssen IT-Systeme im größeren Umfang erneut installiert oder sogar ausgetauscht werden (für forensische Untersuchungen).

(IT-)Krise (beinhaltet auch Katastrophe)

Eine IT-Krise ist entweder:

- ein **eskalierter IT-Notfall oder mehrere parallele IT-Notfälle**
- ein Fall, für den **keine IT-Notfallpläne** vorhanden sind oder in dem vorhandene Pläne **nicht funktionieren**
- ein IT-Notfall, der mehr als **14 Wochentage** andauert (Er wird »automatisch« zu einer (**IT-)Krise hochgestuft**.)
- oder die Störung mehrerer (mehr als 2) zeitkritischer Geschäftsprozesse bzw. zeitkritischer IT-Services

Diese vom Normalzustand extrem abweichende und über die IT-Notfälle hinausgehende Situation kann – trotz vorbeugender Maßnahmen – jederzeit eintreten. Die (IT-) Krise konzentriert sich auf die eigene Organisation und beeinträchtigt nicht breitflächig die Umgebung oder das öffentliche Leben. Sie kann, zumindest größtenteils, innerhalb der eigenen Organisation selbst behoben werden.

Ein typisches Merkmal einer (IT-)Krise ist die Einmaligkeit des Ereignisses. Für die Bewältigung einer (IT-)Krise existieren keine Pläne, sondern lediglich Rahmenanweisungen und -bedingungen bzw. Leitlinien und Empfehlungen auf Basis eines etablierten BCM, ITSCM oder ISM (siehe BCPs/GFPs des BCM oder den Reaktionsplan und die Koordinationspläne des ITSCM).

Definitionen anpassen

Sie können die Definition der (IT-)Krise auch mit Ihren zeitkritischen Geschäftsprozessen bzw. zeitkritischen IT-Services verbinden. Sind z. B. zwei oder mehr zeitkritische Geschäftsprozesse oder zeitkritische IT-Services gestört, wird automatisch die (IT-)Krise ausgerufen.

Es werden nur IT-Notfälle und (IT-)Krisen betrachtet. Nicht betrachtet werden »allgemeine« *Katastrophen*, da diese nicht planbar sind und die eigene Organisation hier oft nicht federführend und verantwortlich tätig ist.

Man ist sozusagen nicht mehr »Herr des Geschehens«, da im Katastrophenfall beispielsweise das *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)* und andere Organisationen (THW, Feuerwehr, Polizei, Bundeswehr etc.) vorrangig die Leitung und Koordination übernehmen.

Katastrophe (wird hier nicht betrachtet!)

Eine Katastrophe ist im Sinne von §1 des BHKG (*Gesetz über den Brandschutz, die Hilfeleistung und den Katastrophenschutz*) ein räumlich und zeitlich nicht begrenztes Großschadensereignis, zum Beispiel als Folge von Überschwemmungen, Erdbeben oder Flugzeugabstürzen. Aus der Sicht der eigenen Organisation stellt sich eine Katastrophe intern als Krise dar und wird durch die Krisenstabsarbeit im Zusammenspiel mit den externen Hilfsorganisationen (z. B. Katastrophenschutz, THW, Bundeswehr etc.) bewältigt.

Eine besondere Vorbereitung gibt es hierfür nicht.

Abbildung 4.3 zeigt Ihnen (wie angekündigt) die vier Stufen noch einmal im Überblick. Sie können sich an diesen Beschreibungen und Definitionen orientieren, aber natürlich müssen Sie für Ihre Organisation individuell festlegen, wie Sie die Unterteilung vornehmen wollen:

Bezeichnung	Minor-Incident	Major-Incident	IT-Notfall	(IT-)Krise
Störungsart	Kleinere Störungen von internen Prozessen, IT-Ressourcen oder IT-Basiskomponenten, ohne jeglichen Kundenbezug und ohne größere Auswirkungen. Keine SLA-Verletzung.	Größere Störungen von internen Prozessen, IT-Ressourcen oder IT-Basiskomponenten, mit geringem bis mittlerem Kundenbezug (einzelne IT-Services oder einzelne Kunden-Services) mit spürbaren Auswirkungen. Mögliche SLA-Verletzung.	Größere Störungen von internen Prozessen, IT-Ressourcen oder IT-Basiskomponenten, mit großem Kundenbezug (sehr wichtige oder viele IT-Services und/oder wichtige IT-Infrastrukturen). Praxiserprobte Notfallpläne sind vorhanden und nutzbar. SLA-Verletzung sehr wahrscheinlich.	Sehr große Störung von vielen internen wichtigen oder zeitkritischen Geschäftsprozessen und/oder IT-Infrastrukturen, es sind nahezu alle Kunden betroffen. Notfallpläne fehlen, funktionieren nicht oder es sind mehrere parallele IT-Notfälle zeitgleich vorhanden. Mehrere SLA-Verletzungen sehr wahrscheinlich.

Abbildung 4.3: Mögliche Definition von Incidents, Störungen und Unterbrechungen

Besonderheit (Verknüpfung mit zeitkritischen Geschäftsprozessen möglich)	kein zeitkritischer Geschäftsprozess betroffen	kein zeitkritischer Geschäftsprozess betroffen	ein zeitkritischer Geschäftsprozess betroffen	mehr als ein zeitkritischer Geschäftsprozess betroffen
Wer ist betroffen?	nur intern	intern/ wenige Kunden	intern/ viele Kunden	intern/ alle Kunden
Priorität	niedrig	mittel	hoch	kritisch
Reputationsverlust	nein	eventuell	höchstwahrscheinlich	ja
SLA-Verletzung	nein	nein/ja	ja	ja
OLA-Verletzung	nein/ja	nein/ja	nein/ja	nein/ja
Datenverlust	ja/nein	ja/nein	ja/nein	ja/nein
Auswirkungen	nur lokal und kurzfristig	mit Kundenbezug und kurz- bis mittelfristig	größerer Kundenbezug und mittelfristig bis längerfristig	weitreichend (alle) und andauernder Ausfall (z. B. Totalausfall)
Sicherheitsvorfall	ja/nein	ja/nein	ja/nein	ja/nein
AAO/BAO Beteiligung	nur AAO	nur AAO	AAO, mögliche Übergabe an BAO	nur BAO
Zeitfaktor	im Stundenbereich	bis zu einem Tag	mehrere Tage bis Wochen	nicht bezifferbar
Notfallplan nötig	nein	nein	ja	ja
WAP/WHP nötig	ja/nein	ja/nein	ja/nein	ja

Abbildung 4.3: Mögliche Definition von Incidents, Störungen und Unterbrechungen (Forts.)

4.4 Prozesse beschreiben

Im nächsten Abschnitt haben Sie die Möglichkeit, den Gesamtprozess Ihres ITSCM oder nur einen oder mehrere Teilprozesse kurz zu beschreiben – je nachdem, was Sie schon aufgebaut haben. Denn erfahrungsgemäß kommen die Prozessarbeiten meist erst später, wenn sich das ITSCM in den Vorgängen Ihrer Organisation etabliert hat. (Es sei denn, es gibt in Ihrer Organisation dazu klare Regelungen, die besagen, dass Prozesse schon vor dem Start eines Projekts definiert werden müssen. Dann haben Sie es allerdings mit einem Henne-Ei-Problem zu tun und müssten zunächst sehr theoretisch vorgehen und Prozesse im luftleeren Raum beschreiben und später an die Praxis anpassen.)

Die Übersicht über die Prozesse soll dafür sorgen, dass die Adressaten der Policy schnell die Vorgänge und Wege in Ihrem ITSCM erfassen können. Achten Sie daher darauf, dass Sie sich an einen allgemein gültigen Standard halten, z. B. an die Spezifikationssprache *Business Process Model and Notation (BPMN)*.

Üblicher ist es, dass Sie in der ersten Version der Policy noch keine Prozesse definieren können oder zumindest Teilprozesse offen lassen müssen. Dann sollten Sie einen Verweis in die Policy aufnehmen, dass dies bis zur nächsten Überarbeitung passieren wird. Mit diesem Platzhalter in der Policy verschaffen Sie sich Zeit, alle sind informiert und Sie vergessen diesen Punkt nicht, da er präsent ist.

Wichtig ist: Sie müssen den (Teil-)Prozess wirklich nur benennen und grob beschreiben und nicht für ihn werben.

Wie Sie Ihren ITSCM-Prozess definieren und beschreiben, erläutere ich in Kapitel 9.

4.5 Die Organisation für den Normal- und den Notbetrieb beschreiben

Im nächsten Schritt der Policy-Erstellung geht es darum, die Organisationsformen zu beschreiben. Es wäre aber auch ein Part, den Sie in der ITSCM-Policy streichen könnten, wenn er bereits in der BCM-Policy auftaucht. Dort passt er thematisch eigentlich besser hin.

Ich orientiere mich an den Begriffen *Allgemeine Aufbauorganisation (AAO)* und *Besondere Aufbauorganisation (BAO)*, die im BSI-Standard 200-4 verwendet werden[2], denn in der ISO 27031 finden Sie so etwas nicht.

Die gesamte Organisation muss alle Belange eines (IT-)Notfallmanagements strategisch, taktisch und operativ abdecken. Da sich eine Organisation in zwei grundlegende Bereiche einteilen lässt – die *Vorsorge* (arbeitet proaktiv) und die *Bewältigung* (arbeitet reak-

2 Siehe: *https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html*

tiv) von IT-Notfällen und (IT-)Krisen –, teilt sich auch die Organisationsstruktur in zwei Bereiche auf:

- in die *(IT-)Notfallvorsorgeorganisation* und
- in die *(IT-)Notfallbewältigungsorganisation*.

Die Organisationsstruktur besteht im Bereich der Notfallvorsorgeorganisation im Normalbetrieb durch die *AAO* aus:

- der Betriebsleitung, der Geschäftsleitung, dem Vorstand usw.
- dem BC-Manager (inklusive Team)
- dem ITSC-Manager (inklusive Team)
- den ITSC-Koordinatoren (inklusive Team)
- den IT-Notfallteams oder Reaktionsteams
- dem Resilienz-Manager (wenn vorhanden)

Im Rahmen der *Bewältigung* (Notfallbewältigungsorganisation) durch die *BAO* besteht die Organisationsstruktur aus:

- dem Krisenstab
- dem (IT-)Lagezentrum/Assistenz und Serviceteam (AST)
- den IT-Notfallteams, Reaktionsteams, A-Teams, Spezialisten etc.

Die AAO ist also für den Normalbetrieb (das Tagesgeschäft) zuständig und die BAO für den Notbetrieb bzw. für die aktive Bewältigung von IT-Notfällen und (IT-)Krisen.

4.6 Die wichtigsten Schnittstellen im Tagesgeschäft in Kurzform vorstellen

Nachdem Sie die Organisation für den Normal- und den Notbetrieb definiert haben, sollten Sie die direkten und wichtigsten Schnittstellen in der Policy vorstellen. Aber nur kurz und knapp! Lang, ausführlich und sehr detailliert wird das Ganze im ITSCM-Handbuch beschrieben.

Tipp aus der Praxis

Da meist das ISM, BCM und das ITSCM ein Dreigestirn bilden, kann ein ITSCM-Team die beiden anderen Bereiche mit je zwei bis drei Sätzen in die ITSCM-Policy einfügen. Die anderen beiden Policys können dann ihrerseits einen ITSCM-Zweizeiler einpflegen. Damit kann das Top-Management genau die Abgrenzungen und Hauptaufgaben der drei Bereiche auf einen Blick sehen und nachvollziehen. Das erleichtert ihnen die Einschätzung zu dem jeweiligen Aufgabengebiet, und die Policy wird schneller freigegeben.

In der Praxis kann ein solches Zusammenspiel in der Policy wie folgt beschrieben werden:

- »**ISM:** Das Informationssicherheitsmanagement ist für den Schutz aller Informationen der Organisation verantwortlich. Dabei gelten die Schutzziele *Vertraulichkeit*, *Integrität* und *Verfügbarkeit*.«[3]
- »**BCM:** Das Business Continuity Management sorgt mit Überbrückungsmaßnahmen für einen reibungslosen Weiterbetrieb der zeitkritischen Geschäftsprozesse. Dies wird in den sogenannten BCPs oder GFP dokumentiert.«
- »**ITSCM:** Das IT Service Continuity Management sorgt mit IT-Notfallvorsorgemaßnahmen dafür, dass die IT-Services und deren IT-Ressourcen, die die zeitkritischen Geschäftsprozesse unterstützen, optimal abgesichert sind und störungsfrei funktionieren.«

Natürlich können Sie diese Sätze in Ihrer Organisation noch wesentlich detaillierter ausschmücken, ganz umformulieren oder auch weglassen. Es wird aber einem Top-Management sehr helfen, zu rekapitulieren, was die anderen Bereiche machen bzw. was diese drei Bereiche eigentlich unterscheidet, wenn die Policy alle zwei Jahre neu unterschrieben werden muss.

4.7 Die fünf Standard-Worst-Case-Szenarien kurz benennen

Im nächsten Schritt werden die fünf *Worst-Case-Szenarien (WCS)* (siehe Kapitel 14) des ITSCM grob beschrieben, mit denen standardmäßig zu rechnen ist. Detaillierter werden sie entweder im ITSC-Lösungskonzept und/oder im ITSCM-Handbuch erläutert.

Als Oberbegriff oder als Begriff aus dem BCM wird nur von einem Worst-Case-Szenario »Ausfall IT« gesprochen. Damit fasst das BCM die fünf WCS des ITSCM zusammen.

Mit einem WCS meint man immer den Totalausfall einer Ressource, der Grund dafür ist egal. Bei den Standard-Worst-Case-Szenarien des ITSCM handelt es sich um:

- **Ausfall eines Rechenzentrums**

  Das komplette RZ ist ausgefallen.
- **Nichtzugänglichkeit eines Rechenzentrums**

  Es kann nicht mehr per Remoteeinwahl auf das RZ zugegriffen werden oder vor Ort kommt man nicht mehr in die RZ-Räumlichkeiten.
- **Ausfall der WAN/RZ-Kopplung**

  Hier kommt es zu einem Ausfall der WAN-Kopplung. Das bedeutet, die Verbindung zwischen zwei RZ oder mehreren RZ ist ausgefallen.
- **Ausfall durch kompromittierte IT-Infrastruktur**

  Damit ist vereinfacht gemeint, dass Ihre gesamte IT-Infrastruktur nicht mehr zu nutzen ist. Sie sind praktisch handlungsunfähig.

3 Dies ist das »klassische« Dreigestirn der IT-Sicherheit, bei dem leider die *Authentizität* als viertes Schutzziel vergessen wird, die aber besonders in modernen IT-Umgebungen eine sehr wichtige Rolle spielt.

- **Ausfall Cloud**

  Hier geht man davon aus, dass Ihre genutzte Cloud-Umgebung nicht mehr zur Verfügung steht.

4.8 Scoping: den Umfang eines ITSCM definieren

In der Policy haben Sie die Möglichkeit, ganz klar und deutlich zu beschreiben, was vom ITSCM betrachtet werden soll und was ausgeschlossen wird. Das nennt man *Scoping*. Sie sollten also praktisch den Umfang eines ITSCM definieren oder einen klaren Fokus setzen. Das dient zur Abgrenzung zu anderen Organisations- und Aufgabenbereichen.

Scoping kann gut genutzt werden, um den Umfang einzugrenzen, wenn Sie erst mit einem sehr kleinen Team oder als »Einzelkämpfer« anfangen, ein ITSCM aufzubauen. Das Scoping kann dann bei der nächsten Policy-Version erweitert werden. Diese Vorgehensweise ist sinnvoll, damit Sie erst mal ans Arbeiten kommen, das Tagesgeschäft organisieren, sich in die Praxis einfinden. Auf Grundlage der Erfahrungen, die Sie in der Praxis sammeln werden, können Sie dann den Scope optimieren. Ein zu großer Scope am Anfang sorgt sonst schnell für Frust und Stagnation.

Das heißt also, dass sich ein Scope dynamisch ändern kann – besser gesagt, dass er sich sogar ändern muss. Es kommen neue Dinge dazu und andere fallen im Laufe der Zeit wieder heraus. Das ist Normalität im ITSCM.

Im Scope

Beispielsweise könnten folgende Aufgaben und Anforderungen im Scope sein:

- sämtliche IT-Notfallvorsorgemaßnahmen, die die IT-Services und deren IT-Ressourcen zur Unterstützung der zeitkritischen Geschäftsprozesse absichern
- Es werden alle IT-Services und IT-Ressourcen, die die zeitkritischen Geschäftsprozesse unterstützen, auf wirksame technische Redundanzen hin überprüft (auf ihr Vorhandensein und ihre Funktion).
- Durch Übungen und Tests werden sämtliche IT-Notfalldokumentationen (z. B. Pläne, Arbeitsanweisungen, Checklisten etc.) auf ihre Wirksamkeit überprüft und gegebenenfalls überarbeitet bzw. wenn nötig dynamisch angepasst.
- Durch geeignete Awareness-Maßnahmen werden das allgemeine Verständnis und die IT-Resilinez in der gesamten Organisation stetig erhöht.

Nicht im Scope (Out-of-Scope)

Ein Beispiel für Aufgaben oder Anforderungen, die Out-of-Scope sind bzw. sein können:

- Jegliche Cyberthematiken (IT-Sicherheit) werden vom ITSCM aktuell *nicht* betrachtet. Diese werden durch das ISM oder das CERT (inklusive SOC) federführend bearbeitet. Diese Bereiche haben dafür eine eigene Organisationsstruktur, eigene Prozesse, Vernetzung und Vorgehensweisen (inklusive Forensik). Darunter fallen z. B.:

- Ransomware-Angriffe
- Denial-of-Service-Angriffe (DoS)
- Distributed-Denial-of-Service-Angriffe (DDoS)
- Man-in-the-Middle-Angriffe (MitM)
- Phishing- und Spear-Phishing-Angriffe
- Advanced Persistent Threats (APT)
- Drive-by-Downloads
- Kennwortangriffe
- SQL-Injection
- Cross-Site-Scripting (XSS)
- Schadsoftware (Malware)
- Social Engineering
- Credential Stuffing
- Zero-Day-Angriff
- Malware (Schadsoftware)
- Botnets
- *[Platz für weitere definierte Szenarien, Angriffsarten etc.]*

4.9 Awareness-Maßnahmen und -Ziele kurz beschreiben

Bei Awareness-Maßnahmen handelt es sich um Aktivitäten, die dafür sorgen, dass in einer Organisation Kenntnisse bzw. ein Bewusstsein für ein bestimmtes Thema oder oder einen bestimmten Themenkomplex aufgebaut wird.

Awareness-Maßnahmen helfen dabei, Menschen für ein bestimmtes Thema zu sensibilisieren, also sie darauf aufmerksam zu machen und ihr Verhalten zu verbessern. Awareness-Maßnahmen sind wichtig, um Mitarbeiter gezielt für Risiken und Best Practices zu sensibilisieren. Sie tragen dazu bei, dass Menschen Fehler und Gefahren erkennen und vermeiden, sei es in der IT, im Datenschutz oder in anderen sicherheitskritischen Bereichen.

Das ITSCM kann dazu folgende Möglichkeiten nutzen:

- Informationsveranstaltungen (online und in Präsenz)
- Workshops (online und in Präsenz)
- Schulungen (online und in Präsenz)
- Hausmessen (in Präsenz)
- Intranet-Meldungen (online)
- Intranet-Seite (online)
- öffentliche Confluence-Seite oder Website (online)

- Gremienarbeit (online und in Präsenz)
- offene Sprechstunden (online und in Präsenz)
- E-Learning-Videos (online)
- White Papers (online/per E-Mail)
- Gamification (online und in Präsenz)
- Aufsteller (vor Ort)
- Flyer (online und in Präsenz)
- etc.

Den Erfolg der Awareness-Maßnahmen wird das ITSCM durch anonyme und freiwillige Umfragen und Feedbacks ermitteln. Echte Lernkontrollen sind durch einen Personalrat (PR) oder einen Betriebsrat (BR) in Deutschland nicht erlaubt.

Hier müssen Sie also etwas kreativ werden, wenn Ihr Top-Management echte Beweise für erfolgreiche Awareness-Maßnahmen haben möchte. Ich werde Ihnen einige Ideen nennen, wenn wir uns in Kapitel 25 um das Thema KPIs (Kennzahlen) kümmern.

4.10 Die Ressourcenfrage klären: Personal, Schulungen, Budget

Die Organisation muss den Rollen und Personen, die dem ITSCM zugeordnet sind, ausreichende finanzielle Mittel sowie zeitliche und personelle Ressourcen zur Verfügung stellen, damit ebendiese Rollen und Personen ihre Aufgaben ordnungsgemäß durchführen können.

Ohne eine verbindliche Zusage dieser Mittel und Ressourcen wird ein ITSCM nur eine Feigenblattlösung werden. Ich würde die Anforderungen sogar (aufgrund meiner bisherigen Erfahrung) noch weiter detaillieren. In Ihrer Policy sollte auf jeden Fall so etwas stehen wie:

- Für den Aufbau eines ITSCM wird ein ITSC-Manager eingestellt bzw. aufgebaut.
- Dafür stehen insgesamt 120.000 € (pro Jahr) zur Verfügung (inklusive Personal-, Schulungs- und Reisekosten, Hardwareanschaffungen etc.).
- Als Zeitrahmen wird dafür ein Jahr festgelegt (vom 01.01.2026 bis 31.12.2026).
- Die Finanzierung wird in der Zeit über die Allgemeinkosten (Umlage) oder einen anderen Etat erfolgen.
- Wird das ITSCM in 2027 weiterbetrieben, werden dem ITSC-Manager ein bis zwei ITSCM-Mitarbeiter zur Seite gestellt. Die Finanzierung wird dann vom Bereich *T* (Technik) oder per Allgemeinkosten (Umlage) übernommen. Das Budget erhöht sich dann auf 300.000€ pro Jahr.
- *[Weitere Regelungen]*

Werden Sie hier also ruhig konkreter. Das gibt Ihnen Sicherheit und einen fest umrissenen Rahmen. Man könnte das noch weiter ausgestalten und mit dem Top-Management vorab abstimmen (siehe das Beispiel in Tabelle 4.1.):

Was?	Zeitraum	Personal
Aufbau des ITSCM	01.01.2026 bis 31.12.2026	1 ITSC-Manager
Betrieb des ITSCM	01.01.2027 bis 31.12.2027	+ 1 ITSCM-Mitarbeiter
Weiterentwicklung und Optimierung des ITSCM	01.01.2028 bis 31.12.2028	+ 1 ITSC-Manager + 1 ITSCM-Mitarbeiter

Tabelle 4.1: Mögliche Ressourcenangaben für ein ITSCM

In diesem Beispiel fangen wir im ersten Jahr mit einer Person an (idealerweise mit dem ITSC-Manager) und würden durch ihn die ersten Strategien, Konzepte, Dokumente und den weiteren Aufbau der ITSCM-Organisation planen und realisieren lassen. Im zweiten Jahr kommt dann ein ITSCM-Mitarbeiter als Unterstützung dazu, und im dritten Jahr könnte man sich personell noch größer aufstellen.

Da die Policy eigentlich nur alle 2 bis 3 Jahre überarbeitet werden sollte, müssen Sie für diesen Zeitraum vorausplanen. Natürlich könnten Sie hier auch schon eine Budgetplanung hinterlegen; das sieht man aber in der eher groben und oberflächlichen Policy selten und höchstens als Ergänzung oder als mitgeltendes Dokument. Aber auch dazu möchte ich Ihnen in Tabelle 4.2 ein Beispiel zeigen.

Jahr	Personalkosten	Sonstige Kosten	Gesamt
2026	90.000 €	10.000 €	100.000 €
2027	90.000 € 70.000 €	10.000 €	170.000 €
2028	90.000 € 90.000 € 70.000 € 70.000 €	20.000 €	340.000 €

Tabelle 4.2: Mögliche Kostenaufstellung pro Jahr

In 2026 wird im Beispiel ein ITSC-Manager beschäftigt, und es fallen etwa 10.000 € an Schulungskosten, Reisekosten und zusätzlicher Büroausstattung an. In 2027 kommt ein ITSCM-Mitarbeiter dazu. Dadurch erhöht sich der Jahresbetrag. In 2028 kommen noch ein

ITSC-Manager und ein ITSCM-Mitarbeiter dazu, was wiederum eine Erhöhung der Kosten mit sich bringt.

Das sind natürlich ganz grobe Mittelwerte. Sie können Personal günstiger oder auch wesentlich teurer einkaufen. Sie können dem ITSC-Manager im ersten Jahr auch einen »Sparringspartner« in Form eines externen Consultants oder Beraters an die Seite stellen. Ich habe z. B. einen Berater im ersten Jahr dazu genutzt, die ersten Versionen aller Notfall-Dokumente und Konzepte/Strategien sehr kritisch zu prüfen. Das hat mir einige interessante »Aha-Effekte« beschert.

Fazit: Sie können mit den zur Verfügung stehenden Ressourcen Ihr ITSCM und dessen Erfolg aktiv steuern.

4.11 Die Sicherheit der Dokumentationen beschreiben

Nun sollten Sie klar darauf hinweisen, dass alle Dokumente des ITSCM besonders schützenswert sind und dementsprechend nur einem begrenzten Kreis von Mitarbeitern (Need-to-know-Prinzip[4]) zur Verfügung gestellt werden.

Die ITSCM-Dokumente sollten in einem internen und geschützten Bereich (passwortverschlüsselt) abgelegt werden. Diese Dokumente werden hochsensible Angriffsziele und/oder Pläne der gesamten (IT-)Infrastruktur einer Organisation enthalten, wie IP-Adressen, Kommunikationswege, Netze, Router- und Switch-Namen, WAN-Leitungsnamen der Telekom etc. – und das mit den realen Bezeichnungen und Namen. Für jeden Hacker wären diese Informationen ein gefundenes Fressen!

Sicherheitsüberprüfungen im ITSCM

Es wäre sinnvoll, als ITSC-Manager eine SÜ2-Überprüfung zu haben (siehe Abschnitt 17.2.7). Diese erweiterte *Sicherheitsüberprüfung (SÜ)* umfasst im Vergleich zur SÜ1 einige zusätzliche Schritte. Insbesondere sollten Sie beachten, dass auch Ermittlungen über Ihren (Lebens- oder Ehe-)Partner erfolgen können.

Es empfiehlt sich natürlich auch, alle anderen ITSCM-Mitarbeiter SÜ2-überprüfen zu lassen. Denn die ITSC-Manager werden die Dokumente und Informationen etc. im Team besprechen und auch zur weiteren Verarbeitung austauschen. Daher ist eine SÜ2 nur dann sinnvoll, wenn auch alle anderen Beteiligten entsprechend überprüft wurden. Somit haben Sie ein Maximum an Sicherheit in diesem Bereich. Das ist auf jeden Fall eine sehr gute Investition, die sich auszahlt. Denn diese Überprüfung ist nicht kostenlos.

4 Das *Need-to-know-Prinzip* (»Kenntnis nur, wenn nötig«), das auch *Erforderlichkeitsprinzip* genannt wird, beschreibt ein Sicherheitsziel für geheime und/oder schützenswerte Informationen. Auch wenn eine Person grundsätzlich Zugriff auf Daten oder Informationen dieser Sicherheitsebene hat, verbietet das Need-to-know-Prinzip ihr den Zugriff, wenn die Informationen nicht unmittelbar für die Erfüllung einer konkreten Aufgabe von dieser Person benötigt werden.

Beachten Sie aber, dass dieser Schritt nur optional und nicht zwingend notwendig ist! Richten Sie sich nach den Sicherheitsstandards in Ihrer Organisation, und denken Sie auch an das Backoffice des ITSCM. Auch diese Kollegen brauchen dann eine SÜ2-Überprüfung, denn dort werden ja die schützenswerten Dokumente und Protokolle ausgetauscht und abgelegt. Ohne die SÜ2 können Sie Ihr ITSCM-Backoffice sonst direkt wieder dichtmachen.

4.12 Unterschrift und Commitment

Die Policy sollten Sie durch die höchstmögliche Position in der Organisation (Präsident, CIO, Vorstand, Geschäftsführer, Top-Management etc.) unterschreiben und dadurch offiziell freigeben lassen. Das ist ein klares *Commitment* an alle Mitarbeiter der Organisation.

Zusätzlich erspart man sich im ITSCM mit so einer offiziellen Policy viele Diskussionen mit den anderen Bereichen innerhalb der Organisation. In so einem Fall brauchen Sie dann nur cool die Policy zücken und den störrischen Kollegen (oder dem Blockierer, Bremsklotz oder Berufsverweigerer) vor die Nase halten. Das schont Ihre Nerven und bringt Sie schneller ans Ziel. Denn sollte der Blockierer Einwände haben, kann er sich gern ans Top-Management wenden. Aus Erfahrung kann ich berichten: Das machen die wenigsten.

4.12.1 Aktualisierung der Policy

Schreiben Sie die Policy nie zu detailliert. Sie werden in der kommenden praktischen Arbeit fast täglich etwas Neues dazulernen. Dabei werden Sie merken, dass Ihre ersten (oft noch sehr) theoretischen Vorüberlegungen und Vorplanungen nicht immer 1:1 in die Praxis umzusetzen sind. Wenn Sie eine Policy anfangs zu genau, also zu feingranular, schreiben, kann es sein, dass Ihre neuen Erkenntnisse Sie praktisch dazu zwingen, häufiger eine Überarbeitung der Policy vorzunehmen. Und das sollte (wenn möglich) vermieden werden.

Im Normalfall sollte man eine Policy alle zwei bis drei Jahre überprüfen und (wenn nötig) anpassen. Es sein denn, es gibt zwingende neue Vorgaben durch Gesetze, Normen, Standards, Organisationsstrategien, Änderungen an Prozessen oder in der Organisation, Änderungen im BCM, ISM etc., die ein kurzfristiges Update erforderlich machen.

Weil die neue Policy wieder an allen wichtigen Stellen einer Organisation zur Freigabe vorgelegt werden muss, sollten Sie den Arbeitsaufwand für alle Beteiligten so gering wie möglich halten. Man möchte sich sein Top-Management nicht mit zu vielen Anfragen nach Unterschriften verärgern, und es wirkt auch nicht gerade professionell, wenn Sie jedes Quartal mit einer überarbeiteten Policy um die Ecke kommen. Wählen Sie alle Änderungen mit Bedacht aus. Man wird es Ihnen danken.

Es ist aber auch ganz normal, dass Aufgaben aus der Policy herausfallen und durch andere ersetzt werden oder dass zusätzliche Aufgaben in die Policy aufgenommen werden. Die IT ist das mit Abstand dynamischste Umfeld der Arbeitswelt. In ihr gibt es fast monatlich Neuigkeiten oder Änderungen (Cloud, KI, Quanten-Computing etc.). Daher wird sich auch Ihre Policy immer wieder ändern. Sie werden nicht die 100-%-Lösung erreichen. Also kommunizieren Sie auch ans Top-Management, dass sich die Policy immer wieder dynamisch den Gegebenheiten anpassen muss und dass das auch gut für die Organisation ist.

4.12.2 Laufweg einer Policy zur Offizialisierung

Ich möchte Ihnen zwei typische Laufwege für eine Offizialisierung einer ITSCM-Policy vorstellen. Eventuell weichen diese etwas von Ihren Laufwegen ab, weil Sie andere Bezeichnungen, Rollen oder Vorgaben innerhalb Ihrer Organisation haben. Das Schema wird aber ähnlich sein. Betrachten Sie es daher bitte wieder als unverbindlichen Vorschlag.

- **Kleiner Laufweg innerhalb der eigenen ITSCM-Organisation**

  ITSC-Manager (Policy-Erstellung) → **ITSCM-Owner** (Gesamtverantwortung) → **ITSCM-Sponsor** (Finanzierung) → genehmigt = zurück an den **ITSC-Manager** (zur Ablage oder Archivierung)

- **Großer Laufweg in der gesamten Organisation**

  ITSC-Manager (Policy-Erstellung) → **BC-Manager** (Abgleich mit BCM-Policy) → Informationssicherheitsbeauftragter (**ISB)** (Abgleich mit ISM-Policy) → **ITSCM-Owner** (Gesamtverantwortung) → **ITSCM-Sponsor** (Finanzierung) → höchstmögliche Position im **Top-Management** (Präsident, CIO, Vorstand, Geschäftsführer etc.) → genehmigt und zurück an den **ITSC-Manager** (zur Ablage oder Archivierung)

Eventuell ist bei Ihnen noch ein Personalrat, Betriebsrat, die Gleichstellungsbeauftragte oder der Compliance-Bereich etc. in diesen Laufweg involviert. Sie können sich bestimmt gut vorstellen, wie lange der Laufweg im großen Verteilerkreis dauert.

Empfehlung

Ich empfehle Ihnen, diese Policy (als Awareness- und Werbungsmaßnahme) im Intranet der Organisation oder am Schwarzen Brett zu veröffentlichen und dadurch allen Mitarbeitern frei zugängig zu machen. Sie werden als ITSCM dadurch sichtbar, und Stakeholder bzw. Interessierte können so auf Sie aufmerksam werden und Sie direkt persönlich ansprechen.

Sie werden sehen: Nach so einer Veröffentlichung wird Ihr Postfach oder Telefon definitiv lebhaft werden. Sie können diese Policy auch in internen (Info-)Veranstaltungen oder Workshops als Nebenthema platzieren. Da sind Ihnen keine Grenzen gesetzt.

Auch hier wieder der Hinweis: Je besser die Mitarbeiter Ihre Policy (und den Mehrwert eines ITSCM) verstehen, desto eher haben Sie diese potenziellen Unterstützer auf Ihrer Seite. Durch so eine Veröffentlichung sind Sie transparent und nahbar. Denn alles, was für die Mitarbeiter eine »Blackbox« darstellt, also mysteriös oder unbekannt ist, stößt fast immer auf eine innere Abwehrhaltung und Distanzierung. Sie möchten aber mit dem ITSCM Verbündete finden und keine Gegner oder gar Blockierer.

Daher wäre für mich das leise und stille Ablegen einer Policy nach der Offizialisierung ein Fehler. Gehen Sie offensiv und stolz mit diesem tollen Arbeitsauftrag in der Organisation hausieren.

4.13 Mitgeltende Dokumente aufführen

Abschließend sollten Sie Ihre wichtigen zusätzlichen Dokumente mit anhängen oder auf sie verweisen. Das gilt aber nur für Dokumente, die auch einen direkten Bezug zu dieser ITSCM-Policy haben. Das kann eine andere Policy sein, eine hausweite Resilienz-Strategie, konzernweite Vorgaben etc.

Typische Kandidaten sind:

- BCM-Policy
- ISM-Policy
- ReM-Policy
- das Sicherheitskonzept und die Freigabe von Dokumenten
- Vorgaben zum Dokumentenmanagement (Benamung, Ablageort, Reviews, Archivierung etc.)
- die Strategie Ihrer Organisation zum Thema »Resilienz«
- Vorgaben zur Dokumentensicherheit, zum Qualitätsmanagement (QM)
- DSGVO-Vorgaben
- BSI Standard 200-4
- ISO 27031-2025-5
- *[weitere Dokumente]*

4.14 Weitere Vorgehensweise und Übungsaufgaben

Jetzt, nach der Policy, geht es zur ersten Ist-Aufnahme: Welche Informationen sind schon da, und was kann davon genutzt werden? Dies spart Ihnen viel Zeit und Arbeit. Synergien werden erkannt, und es ergibt sich ein (hoffentlich) schlüssiges Gesamtbild für Sie und das ITSCM. Nun gilt es, genau diese Informationen zu sammeln, zu sichten und optimal zu nutzen.

F-04-1: Was ist eine Policy?

a) Ein Kooperationsvertrag zwischen BCM und ITSCM
b) Eine detaillierte Rollenbeschreibung für das ITSCM
c) Der Arbeitsauftrag für das ITSCM
d) Der Schulungsplan für alle ITSCM-Rollen und -Mitarbeiter

F-04-2: Sollte ein Geltungsbereich in der Policy definiert werden?

a) Nein, es ist immer alles organisationsweit ausgelegt.
b) Ja, damit fokussiert man sein ITSCM und gibt den Rahmen vor.
c) Nein, er wird in der übergeordneten BCM-Policy mit angegeben.
d) Ist überflüssig, da man die Policy immer kurz und knapp halten will.

F-04-3: Was sind typische ITSCM-Rollen?

a) ITSC-Manager, ITSC-Koordinator, ITSCM-Owner, ITSCM-Mitarbeiter
b) BC-Manager, BC-Koordinator, BC-Mitarbeiter
c) Servicebüro, Assistenz, Backoffice
d) Vorstand, CIO, Präsident, Geschäftsführer