5. Kommunaler IT-Sicherheitskongress 2018

Aus der Praxis für die Praxis

Landkreis Esslingen

IT-Notfallmanagement in Kommunen –

Herausforderungen und mögliche Lösungsansätze

Regina Holzheuer

AGL IT-Sicherheit und IT-Verwaltung

Freitag, 27.04.2018, 18:30 Uhr

Landkreis Esslingen

Päuschen?

Nein!

Lebt er noch?

(Der letzte Erste-Hilfe-Kurs ist echt lang her…)

Griff zum Telefon: Nichts – das Telefon ist tot!

Was tun?

Landkreis Esslingen

Panisch im Kreis rennen?

Sich neben den Kollegen legen?

Kollegen / sich verstecken?

Auf die Tastatur hämmern?

Wohl eher nicht…

Was tun?

- Vorgesetzten (Wochenende) oder 112 ?
- Wie kommt RD rein? Haus wird um 14 Uhr abgeschlossen…
- Hausmeister? Handynummer?
- Kollegen allein lassen?
- ….und wer bringt jetzt die Telefonie wieder in Gang?

Beachten Sie:

Die IT ist eine zentrale Einheit mit zahlreichen Abhängigkeiten. Entsprechend vielfältig sind Auslöser für „IT“-Notfälle.

Beispiele: Hardwaredefekte, Leitungsschäden, Einbruch, Sabotage, Erkrankung von IT-Personal, Ransomware, Datenabfluss, Extremwetterlagen

Wir brauchen ein IT-Notfallmanagement

Landkreis Esslingen

Ziele:

- Schaden begrenzen
- Kontinuierlichen Betrieb kritischer Bereiche sicherstellen
- Schnelle Wiederherstellung
- Rechtskonformität
- Lernen aus Zwischenfällen & Fehlern ermöglichen
- Weiteren Notfällen vorbeugen

Wir brauchen ein IT-Notfallmanagement

Landkreis Esslingen

Aber….

„Das kann ich nicht entscheiden“

„Wer soll das machen?“

„„Wie soll das gehen?“

„Das machen wir, wenn wir mal Zeit haben!“

„Bei uns passiert doch nichts!“

„Keine Zeit für sowas!“

„Wo steht, dass wir das machen müssen?“

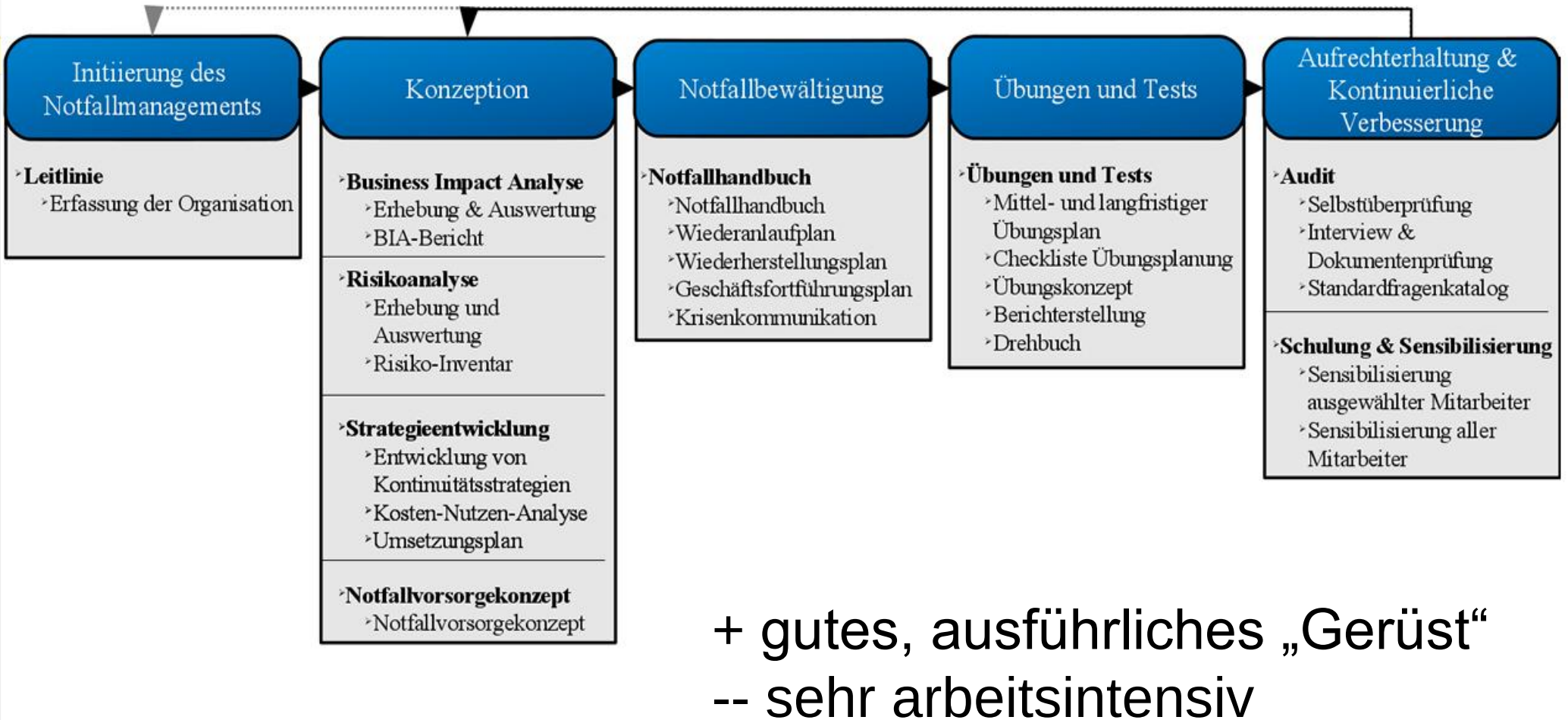
Wir passen doch auf!“

„An Vorgesetzten melden reicht aus!“

„Welche Strafen sind zu erwarten?“

„Dafür ist doch der KatSchutz zuständig!“

Standard 100-4



+ gutes, ausführliches „Gerüst“
-- sehr arbeitsintensiv

Notfallmanagement hat ein Problem

Landkreis Esslingen

- bringt kein Geld
- keine schönen Pressebilder
- ist nicht „sexy“
- verlangt die gedankliche, flexible Beschäftigung mit unangenehmen Ereignissen
- und macht eine Menge Arbeit….

Zitat BSI-Standard 100-4, S. 31:

Landkreis Esslingen

„Da breite Mitarbeit sowohl in den Geschäftsbereichen, den Organisationseinheiten wie auch auf der Ressourcen-Ebene (z. B. Administration für die IT) benötigt wird, muss sichergestellt sein, dass der Arbeitsauftrag durch die oberste Ebene getragen und dessen Bedeutung institutionsweit kommuniziert wird.“

Herausforderungen

Landkreis Esslingen

Mangel an

- Ressourcen
- Unterstützung
- Umsetzungswillen
- Einsicht zur Notwendigkeit

Herausforderungen

Landkreis Esslingen

- Länge der Entscheidungsprozesse
- Trennung von Aufgaben, Verantwortlichkeiten und Kompetenzen
- Vielfalt / Komplexität
- Gewohnheit („immer schon so gemacht“)
- Herrschaftswissen /-denken; Bereichsegoismen

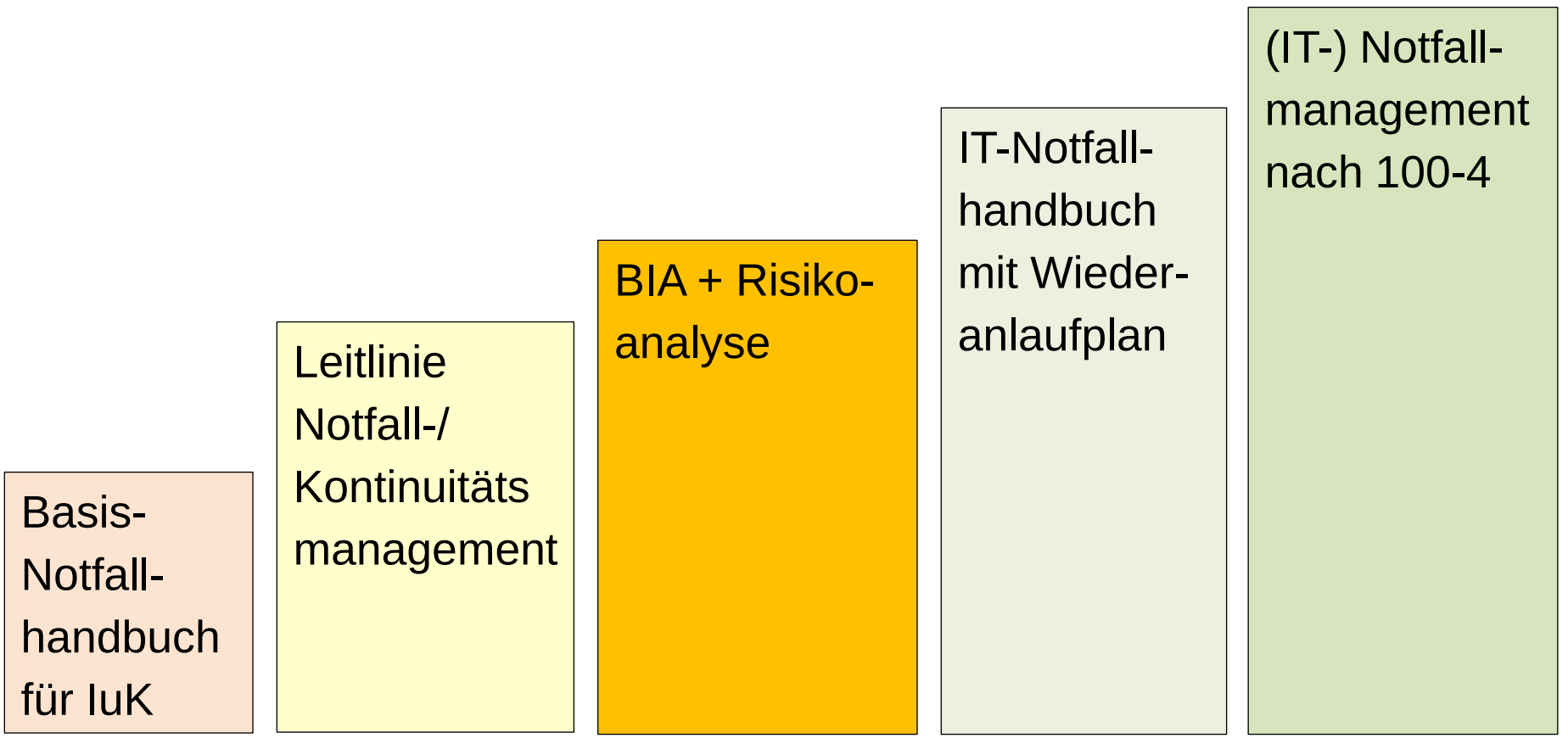
Mögliche Lösung im kommunalen Bereich

Landkreis Esslingen

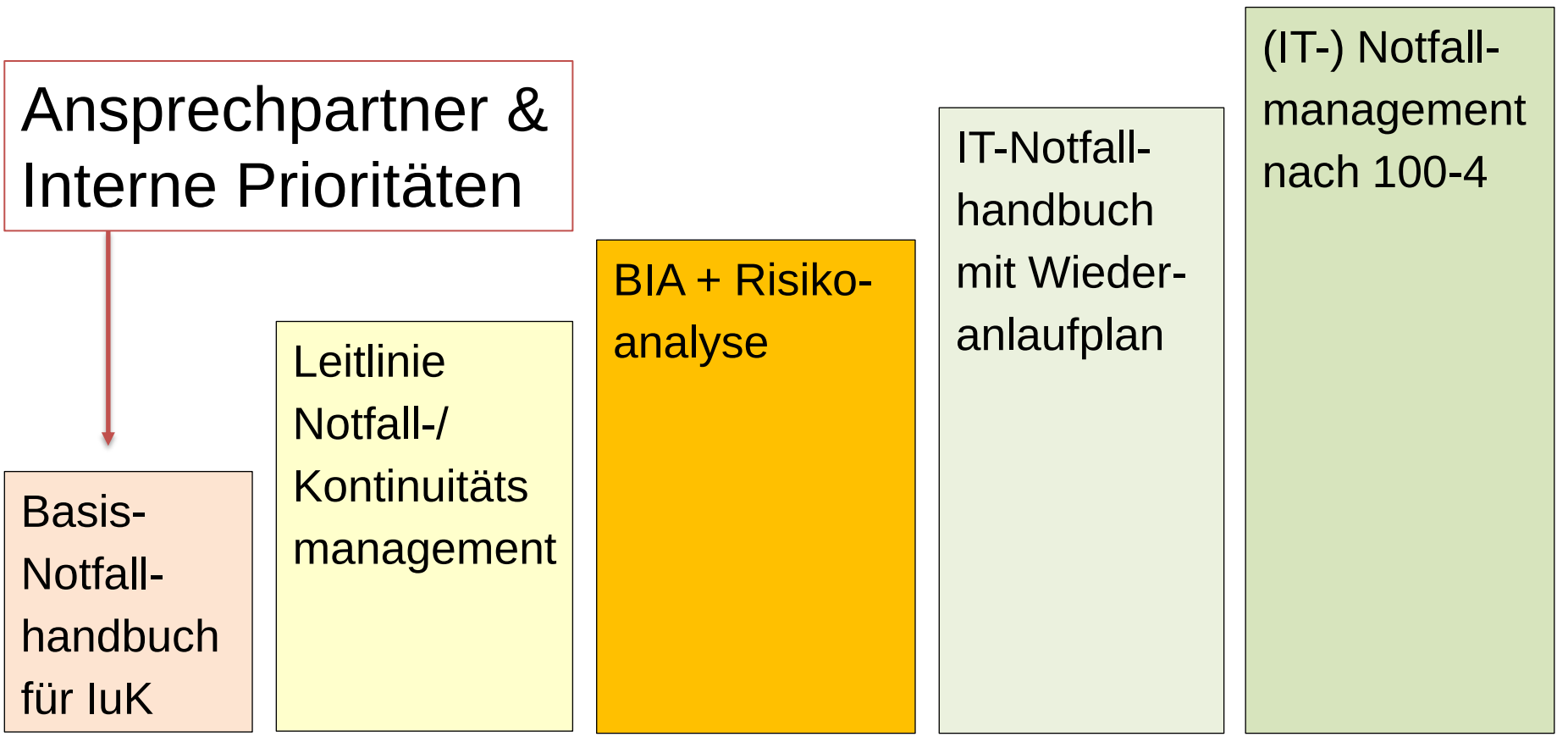
- Hartnäckigkeit
- Kurz- und Langstrecken-Ziele setzen
  - Übergangs-Notfallmanagement (Wallace/Webber)
  - Crisis- / Crew-Resource-Prinzipien

- BSI-Standard 100-4
  - (IT-)Notfallkonzept als studentische Abschlussarbeit?
- Menschl. Bedürfnisse im Notfall einplanen

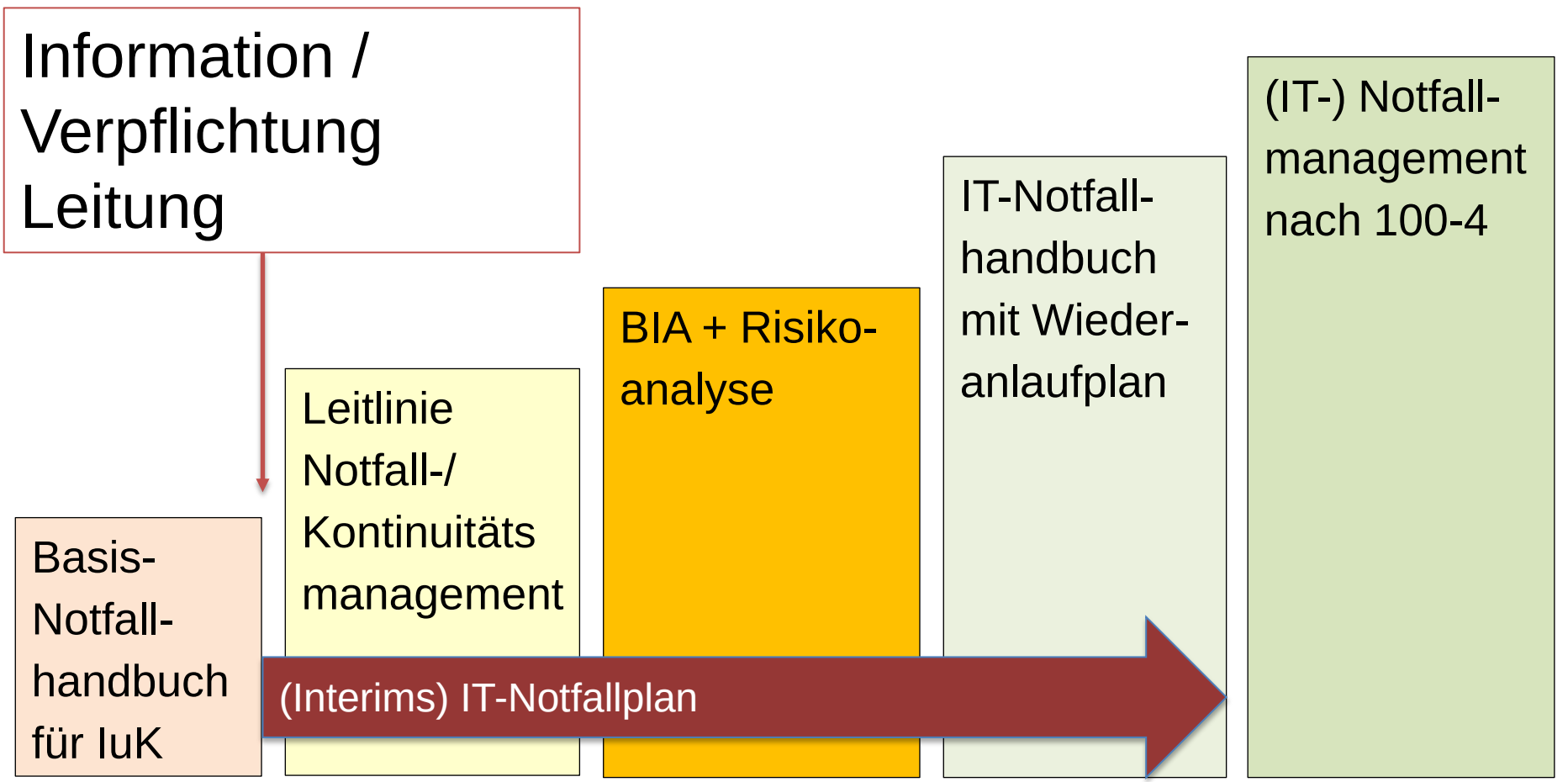
Strategie


Basis-Notfall-handbuch für IuK
Leitlinie Notfall-/ Kontinuitäts management
BIA + Risiko-analyse
IT-Notfall-handbuch mit Wieder-anlaufplan
(IT-) Notfall-management nach 100-4

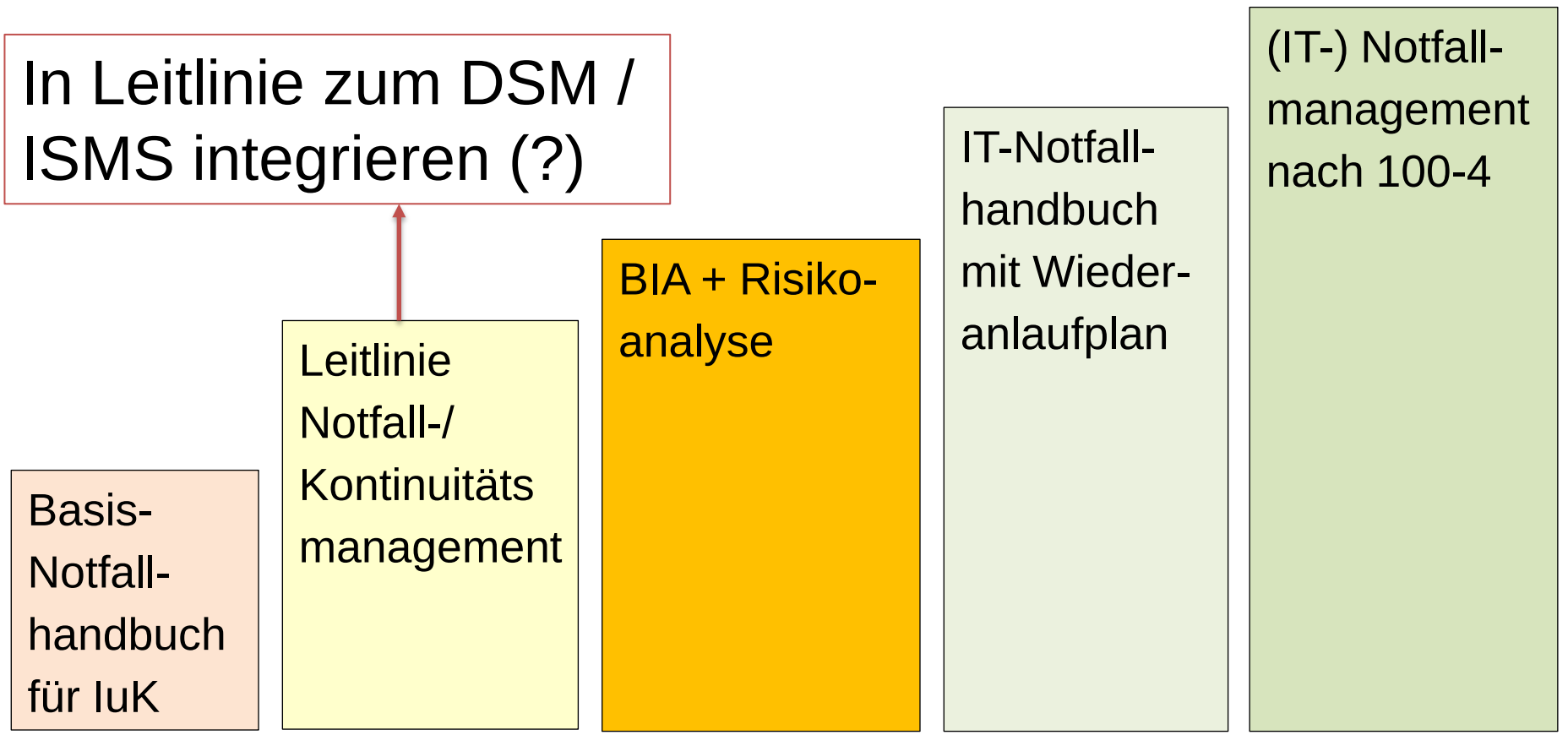
Strategie


Ansprechpartner & Interne Prioritäten
Basis-Notfall-handbuch für IuK
Leitlinie Notfall-/ Kontinuitäts management
BIA + Risiko-analyse
IT-Notfall-handbuch mit Wieder-anlaufplan
(IT-) Notfall-management nach 100-4

Strategie


Information / Verpflichtung Leitung
Basis-Notfall-handbuch für IuK
Leitlinie Notfall-/ Kontinuitäts management
BIA + Risiko-analyse
IT-Notfall-handbuch mit Wieder-anlaufplan
(IT-) Notfall-management nach 100-4
(Interims) IT-Notfallplan

Strategie


In Leitlinie zum DSM / ISMS integrieren (?)
Basis-Notfall-handbuch für IuK
Leitlinie Notfall-/ Kontinuitäts management
BIA + Risiko-analyse
IT-Notfall-handbuch mit Wieder-anlaufplan
(IT-) Notfall-management nach 100-4

Strategie

Landkreis Esslingen

Information / Mitwirkung Fachbereiche

Basis-Notfall-handbuch für IuK

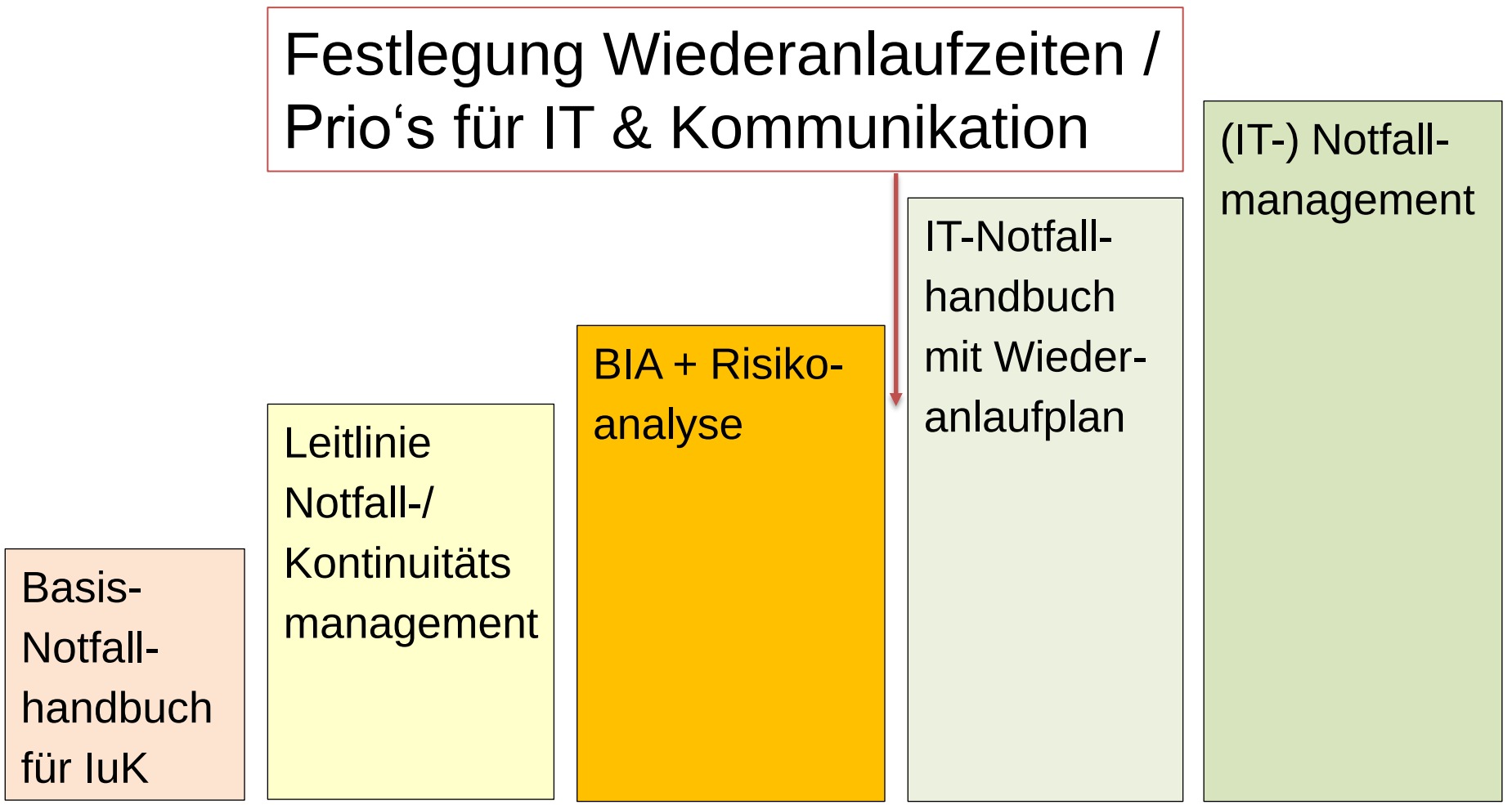
Leitlinie Notfall-/ Kontinuitäts management

BIA + Risiko-analyse

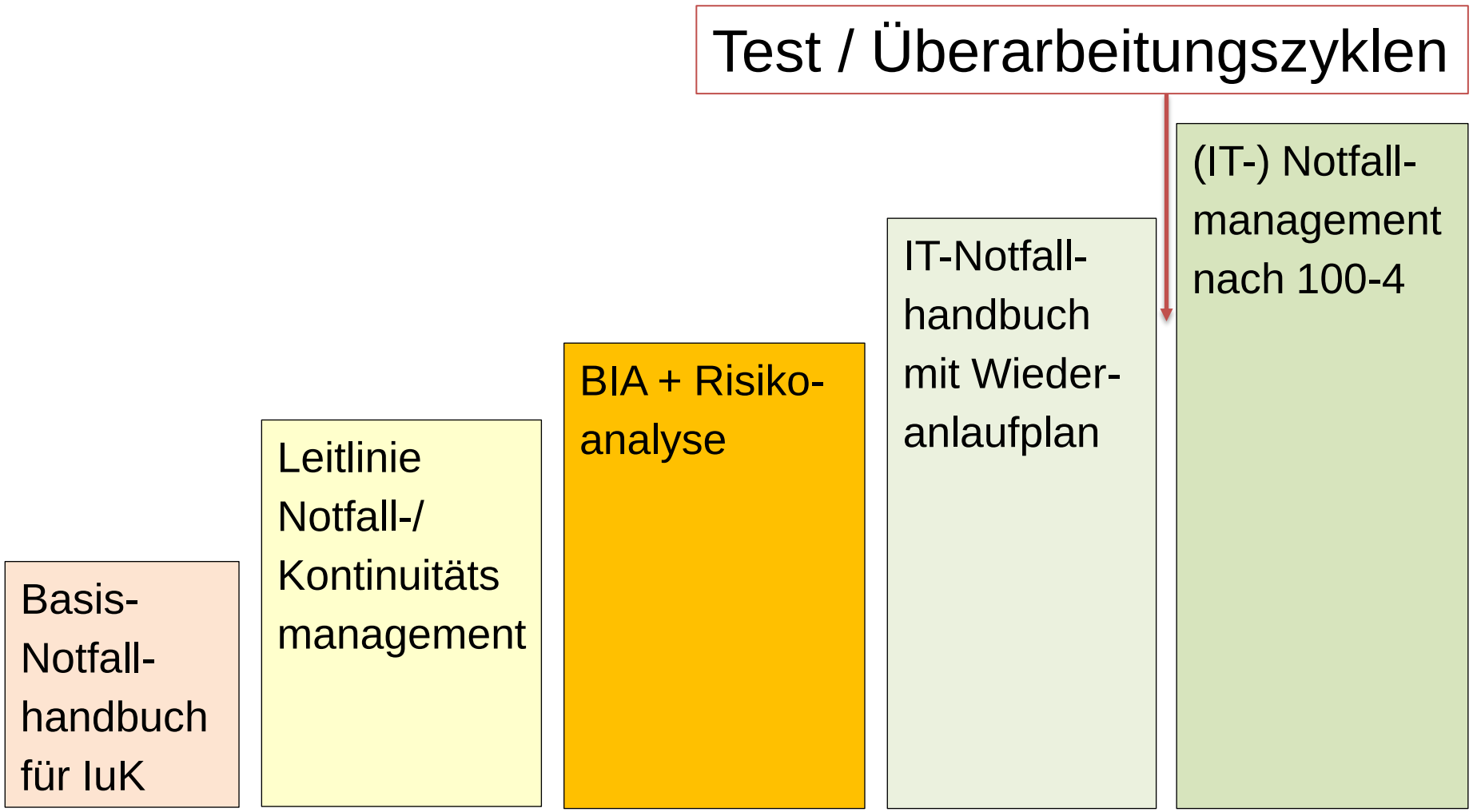
IT-Notfall-handbuch mit Wieder-anlaufplan

(IT-) Notfall-management nach 100-4

Strategie


Festlegung Wiederanlaufzeiten / Prio‘s für IT & Kommunikation
Basis-Notfall-handbuch für IuK
Leitlinie Notfall-/ Kontinuitäts management
BIA + Risiko-analyse
IT-Notfall-handbuch mit Wieder-anlaufplan
(IT-) Notfall-management

Strategie


Test / Überarbeitungszyklen
(IT-) Notfall-management nach 100-4
IT-Notfall-handbuch mit Wieder-anlaufplan
BIA + Risiko-analyse
Leitlinie Notfall-/ Kontinuitäts management
Basis-Notfall-handbuch für IuK

Interims-Notfallplan erstellen

Landkreis Esslingen

- Nur für Notfallteam! Nicht weiter im Haus kommunizieren!

  Ziel: Notfallbewältigung sicherstellen

- IT-Perspektive

Interims-Notfallplan erstellen

Landkreis Esslingen

1. Wer gehört ins Team? Wer führt es?

Notieren (Datei & Papier):

- Verantwortung (Admin, Hausmeister, Leitung)
- Erreichbarkeit
- ggf. Meldewege

Interims-Notfallplan erstellen

Landkreis Esslingen

2. Wer kann helfen?

- Dienstleister (Wofür?)
- Wartungsverträge durchsehen:
  - Zeitfenster?
  - 24/7, 8-17h, Wartung / Austausch
- (aktuelle) Kontaktdaten

Dokumentation

Interims-Notfallplan erstellen

Landkreis Esslingen

2. Wer kann helfen?

- Kollegen im Fachbereich / außerhalb
  - Fachanwendungsbetreuer
  - Sozialarbeiter
  - Ersthelfer / Feuerwehrleute

Dokumentation

Interims-Notfallplan erstellen

Landkreis Esslingen

3. Zugang / Zugriff

Notieren:

- Wo sind Ersatzschlüssel?
- Wo sind Passwörter?
- Wer hat Berechtigungen?
  - ggf. 1.o. 2. überarbeiten

Interims-Notfallplan erstellen

Landkreis Esslingen

4. Reaktionsort („Krisenzentrum“) vorbereiten

- Wo treffen wir uns?
- Was brauchen wir?
  - Strom,
  - Kommunikation (Netzwerk/Flipchart/Stifte…),
  - Verpflegung (Kaffee!),
  - Toiletten,
  - Rückzugsort

Interims-Notfallplan erstellen

Landkreis Esslingen

5. Software / Hardware

Notieren und ggf. bereitstellen:

- Was brauchen wir?
- Was wird zur Aufrechterhaltung / Wiederherstellung unbedingt benötigt?

Interims-Notfallplan erstellen

Landkreis Esslingen

6. Was sind unsere eigenen Prioritäten?

- IT-Intern
- Wovon sind wir abhängig?
  - Strom
  - Wasser
- Welche Dienste / Systeme müssen funktionieren, damit es andere können?

Beispiel für IT-Prioritäten

Landkreis Esslingen

Prio / Schritt 1	Prio / Schritt 2	Prio / Schritt 3	Prio / Schritt 4
1. Netzwerkmanagement (inkl. RZRS-Anbindung) **2. Virtuelle Umgebung** **3. Domaindienste / Benutzer-management:** • ADS Benutzer- und Rechteverwaltung **4. Exchange / Contentfilter & Telefoniemanagement**	**1. Datenbankverwaltung** **2. Clientmanagement** • SCCM-Installa-tion/Fehleranalyse • OS-Deployment / Betriebssystemin-stallation • Clientmanagement im SCCM und AD	**1. Firewall/ Proxy (Internet)** • Installation/Fehler-analyse • Verwaltung VPN, HOB, RD Gateway **2. Server** **3. Anwendungsbetreuer / UHD** **3. Betreuung Clients/ Peri-pherie**	Alles andere, wie z.B. • **Programmierungen** • **Beschaffung** • **Ausbildung**

Interims-Notfallplan erstellen

Landkreis Esslingen

6. Was sind unsere (geschätzten) Prioritäten?

„kleine, informelle“ BIA

- Welche Bereiche müssen funktionieren, damit es andere können?
- Welche Bereiche können (lebens)wichtig werden? (Feuerwehr, Jugendamt, Krankenhäuser)
- Wo drohen hohe Schäden (Finanzen/Image)?

Interims-Notfallplan erstellen

Landkreis Esslingen

7. Selbstschutz beachten:

Gibt es Gefahren für das Team?

- Giftige / leicht entflammbare Stoffe?? (Dieseltank!)
- Gefahren durch Unglücke auf Verkehrswegen?

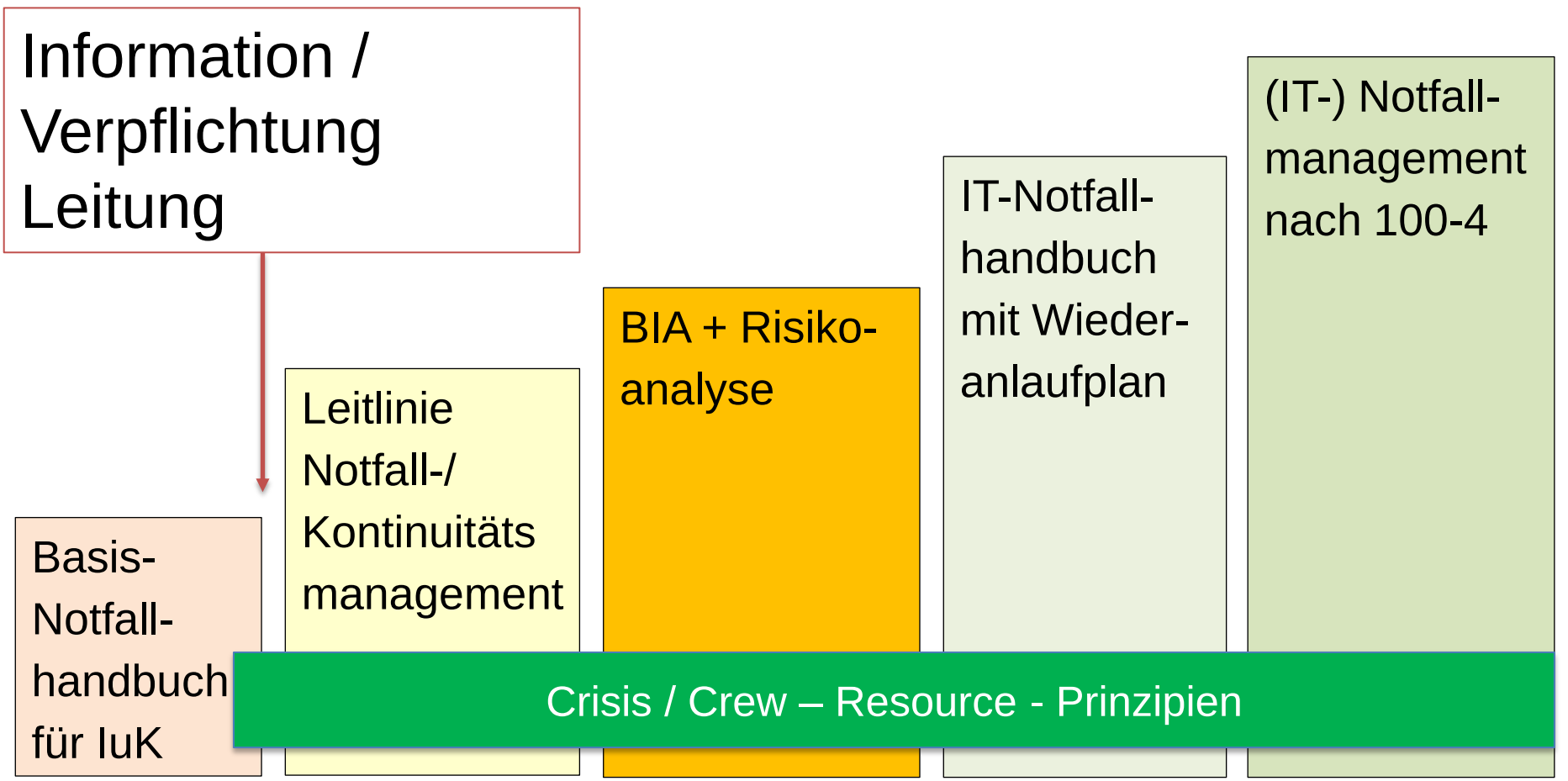
- Notieren und im Team kommunizieren

Beachten Sie:

Landkreis Esslingen

Menschen, die traumatische Situationen (mit-) erlebt haben, sind selten kurz danach wieder (voll) fähig, sich ihrer Arbeit bzw. der Notfallbewältigung am Arbeitsplatz zu widmen!

Strategie


Information / Verpflichtung Leitung
Basis-Notfall-handbuch für IuK
Leitlinie Notfall-/ Kontinuitäts management
BIA + Risiko-analyse
IT-Notfall-handbuch mit Wieder-anlaufplan
(IT-) Notfall-management nach 100-4
Crisis / Crew – Resource - Prinzipien

CRM
(Crisis- / Crew-Resource-Management)

Landkreis Esslingen

CRM

- stammt aus der Luftfahrt (Crew-Ressource-M.)
- wurde in der Notfall-/Intensivmedizin adaptiert (Crisis-Ressource-Management)

Anregungen aus dem CRM

Landkreis Esslingen

Was bringt mir CRM für kommunales (IT-) Notfallmanagement?

1. **Prinzipien des Handelns in Routine- und Krisensituationen für den Einzelnen und die Gruppe**
2. Existenzbedrohende Situationen schnell „entschärfen“

Anregungen aus dem CRM

Landkreis Esslingen

1. **Kenne deine Arbeitsumgebung**

- IT-Infrastruktur
- Bauliche Infrastruktur
- Geschäftsverteilungsplan / Kollegen!

(Schwachstellen? Risiken?)

Anregungen aus dem CRM

Landkreis Esslingen

2. Kenne mögliche Hilfen

- Interne Ansprechpartner
- Externe Kollegen („Amtshilfe“)
- Wartungs- und Dienstleistungsverträge
- Landes-CERT?
- LKA / Polizei?

Anregungen aus dem CRM

Landkreis Esslingen

3. Plane vorausschauend

- Wo lauern Gefahren?
- Merkhilfen / Checklisten anlegen und bereithalten
- „Unsicherheitskultur“ sanktionieren

Anregungen aus dem CRM

Landkreis Esslingen

4. Arbeite <u>sicher</u> in Gruppen

- Klare Aufgabenverteilung
- Klare, verantwortungsvolle Führung:

  Wer führt, entscheidet - Wer entscheidet, führt!

➢ Entscheidungen fällen

- Jeder muss und darf Beitrag leisten

Anregungen aus dem CRM

Landkreis Esslingen

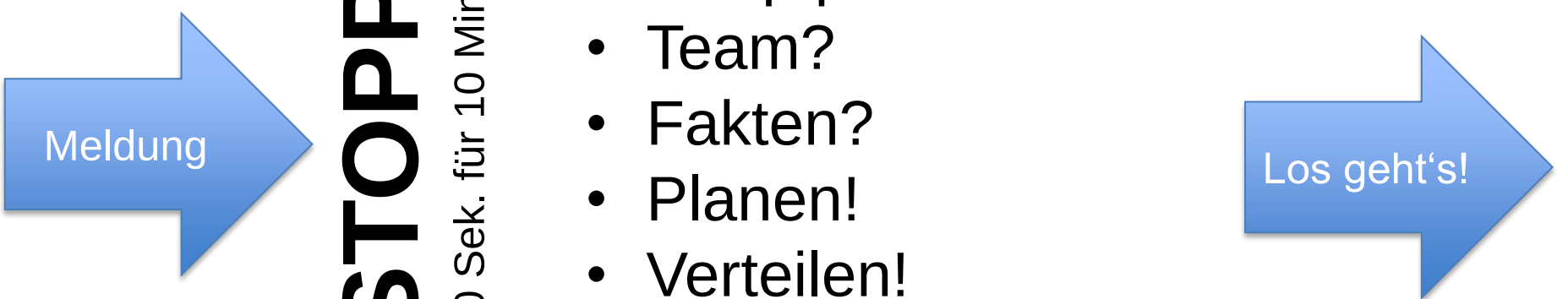
5. Kommuniziere sicher

- Deutlich sprechen
- Zweifel laut äußern - Bedenken berücksichtigen
- Effektiv (lange Diskussionen vermeiden)
- Direkt (ohne Geschwafel, Höflichkeitsfloskeln, Hierarchiedünkel)
- Unklarheiten durch Rückfragen ausräumen, erhaltene Aufträge stets bestätigen.

Anregungen aus dem CRM

Landkreis Esslingen

6. Nehme die (Notfall-)Situation wahr



Anregungen aus dem CRM

Landkreis Esslingen

6. Nehme die (Notfall-)Situation wahr

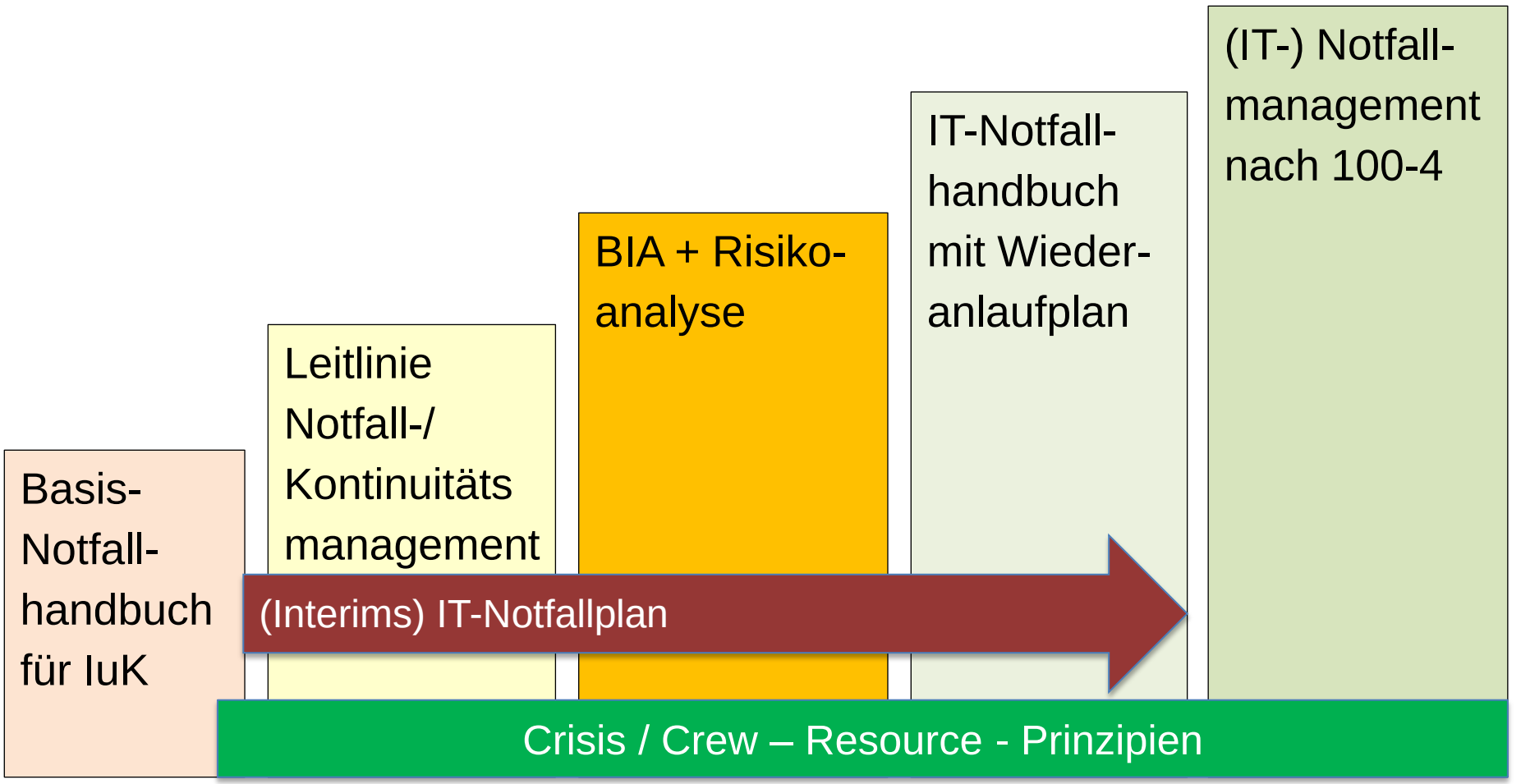
- Wo lauern Gefahren in der Situation?

➢ Fixierungsfehler erkennen & verhindern

- Situation ständig überdenken, Prio‘s neu setzen

➢ Führung teilt ggf. weitere Aufgaben zu

Strategie „Aufbau kommunales IT-Notfallmanagement“

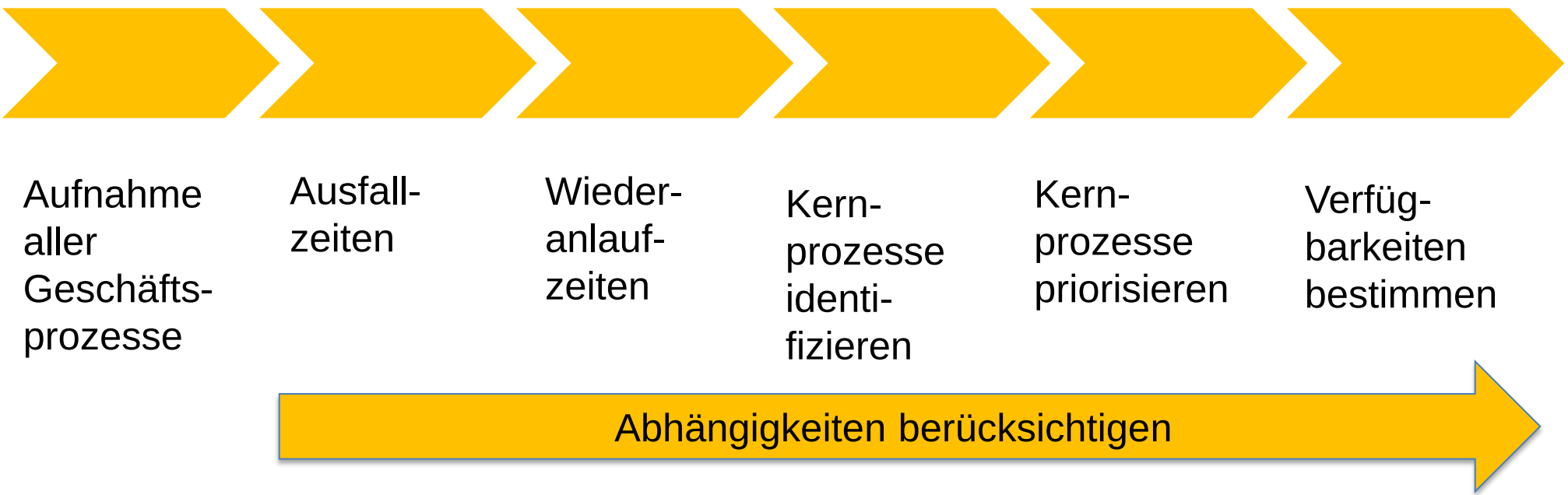


BIA und Risikoanalyse

Landkreis Esslingen

= „Rückgrat des Notfallmanagements“

Schrittfolge:



BIA und Risikoanalyse

Landkreis Esslingen

= „Rückgrat des Notfallmanagements“

Schrittfolge:

Alle Fachbereiche müssen mitwirken
Empfehlung: Bildung Projektgruppe

Notfallhandbuch

Landkreis Esslingen

- Sofortmaßnahmepläne
  - Meldewege
- Notfallteam / Krisenstab
  - Rollen und Aufgaben
  - Krisenkommunikation
- Wiederanlaufpläne / Prioritäten
- (Fachbereichsbezogene) Kontinuitätspläne

Beachten Sie:

Landkreis Esslingen

Menschen, die traumatische Situationen (mit-) erlebt haben, haben ein verändertes Kommunikationsbedürfnis!

Krisenkommunikation einplanen

Landkreis Esslingen

In der Leitlinie verankern:

- einheitlicher Kommunikationskanal (one voice policy / single point of contact) nach außen

Im Notfallhandbuch zusätzlich:

- Mögliche Ansprechpartner (Sozialarbeiter?)
- Vorgesetzte informieren / schulen (Umgang mit schwerer Erkrankung / Todesfall)

Beachten Sie:

Landkreis Esslingen

Der Notfall ist erst beendet, wenn er bewältigt wurde !

Menschen, die traumatische Situationen (mit-) erlebt haben, müssen die Möglichkeit der Verarbeitung bekommen!

Der Notfall

Landkreis Esslingen

…wird nicht geduldig warten, bis Sie ein Notfallmanagement haben.

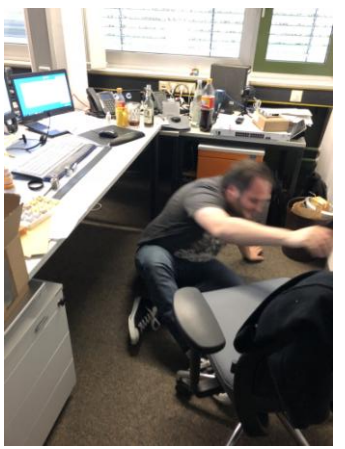
Also warten Sie besser nicht auf den Notfall…

Vielen Dank

Landkreis Esslingen

…für Ihre Aufmerksamkeit !

…den Kollegen vom LRA ES-SG 115 IuK für die Unterstützung.



Literatur

- Spörer: Business Continuity Management, Kölner Wissenschaftsverlag 2014
- Osterhage: Notfallmanagement in Kommunikationsnetzen, Springer-Xpert.press 2016
- Wallace / Webber: The disaster recovery handbook, 2017
- Rall, Lacker: Crisis resource Management, Springer, 2010
- St.Pierre, Hofinger: Human Factors und Patientensicherheit in der Akutmedizin, Springer 2014