Wirkungsvolle Umsetzung von IT-Compliance & -Awareness

Dr. Kristin Masuch

Co-Gründerin und Geschäftsführerin

- Studierte Wirtschaftsinformatikerin
- Promoviert im Bereich Informationssicherheit, Fokus Security Crisis Recovery
- Mehrjährige Erfahrung im (Informationssicherheits-) Projektmanagement
- Zertifizierte Projektmanagerin & ISO 27001 Beraterin

Prof. Dr. Simon Thanh-Nam Trang

Co-Gründer

- Studierter und promovierter Wirtschaftsinformatiker
- Professor für nachhaltige Informationssicherheit an der Universität Paderborn
- Mehrjährige Erfahrung im Informationssicherheits-management im KRITIS-Sektor
- Zertifizierter Projektmanager & ISO 27001, CISSP, ITIL, TOGAF

Projekte in 2023/24

RPD Rezeptprüfstelle Duderstadt

Stadtwerke Bielefeld

innovativ. flexibel. zuverlässig.

Kreis Paderborn

...nah bei den Menschen!

ITS.Kompetent

LAN IT Landesarbeitskreis Niedersachsen für Informationstechnik/ Hochschulrechenzentren

KISK

Kompetenzorientierte und stellenspezifische IT-Sicherheit für Mitarbeiter:innen in Krankenhäusern

PROBLEMSTELLUNG

Der Arbeitsalltag in Unternehmen führt zu Herausforderungen bei der Umsetzung von ITS-Maßnahmen

Maßnahmen
...zur Steigerung der mitarbeiterbezogenen IT-Sicherheit

Anwendung
... von Prozeduren und Werkzeugen zur Gewährleistung der IT-Sicherheit

Problem ITS-Interventionen weisen eine geringe Effektivität auf und führen zu geringer Anwendung von ITS-Prozeduren im Krankenhausalltag

Ursache **Fehlende Kompetenzorientierung**
a) Unklarheit bzgl. der tatsächlichen Kompetenzbedarfe
b) Trainings orientieren sich nicht am tatsächlichen Qualifizierungsbedarf
c) Keine anforderungsorientierte Evaluation der Interventionseffektivität
d) Geringe Motivation für das Thema bei Schulungen und der Anwendung

Lösung
a) Kompetenzmodellierung zeigt Kompetenzbedarf
b) Kompetenzaufbau durch zielgerichtete Interventionen
c) Kompetenzmessung ermöglicht nachhaltige Verhaltensänderung und wissenschaftlich evaluierte ITS-Awareness-Toolkits
d) Nachhaltiger Trainingserfolg und Verhaltensänderung durch ITS-Nudges

Teil 1 + 2

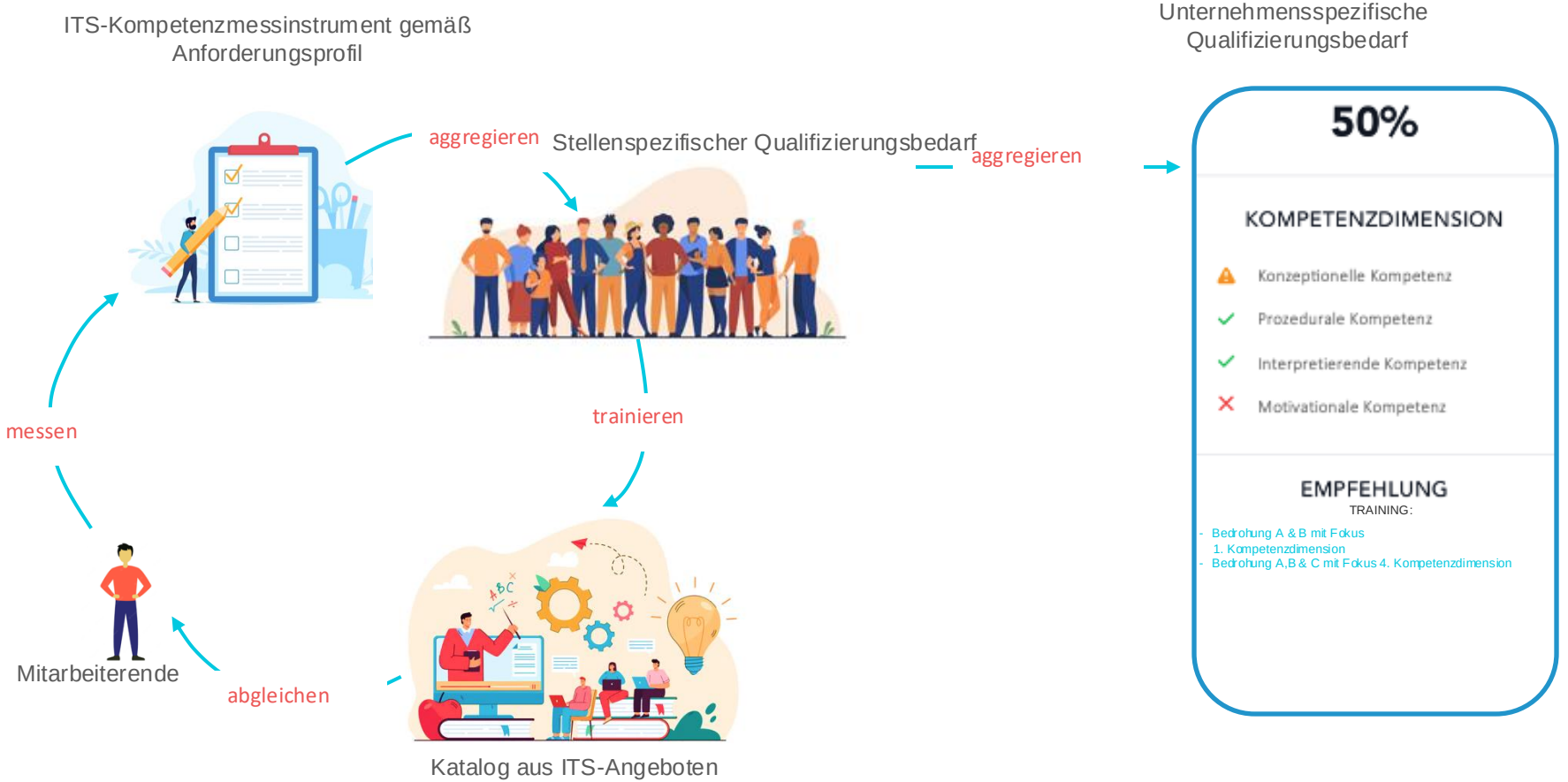
ITS.kompetent

ITS.KOMPETENT: KMU-Mitarbeiter und -Entscheider können sich zielgerichtet und effizient in IT-Sicherheit durch die Vermittlung passgenauer Trainingsinhalte professioneller Anbieter weiterbilden.

METHODEN: Kompetenzmessung, Matching-Verfahren, Data Collection, Field Studies, Web Platform Architecture Development

ZEITRAUM TEIL 1: 2021 – 2024

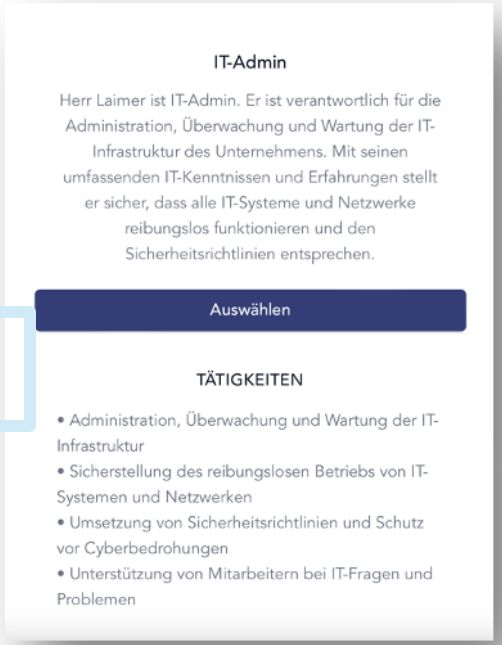
ZEITRAUM TEIL 2: 2024 – 2027

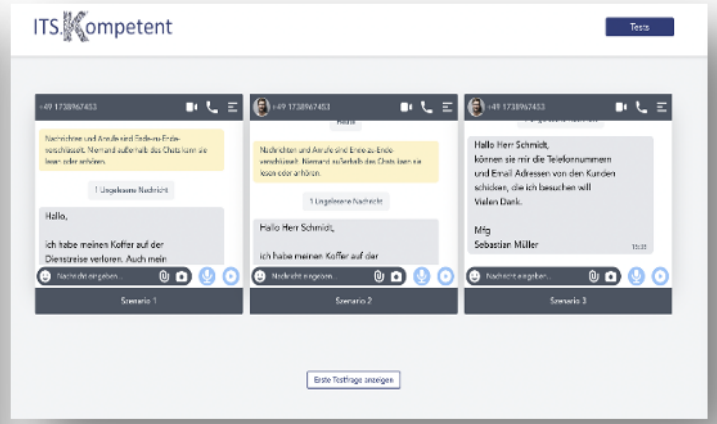


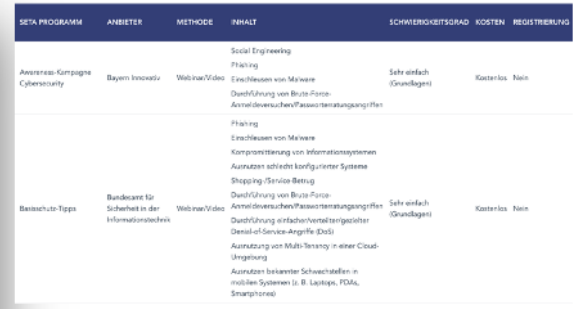
Teil 1 (abgeschlossen und kostenlos für KMUs)

ITS.kompetent

1. ITS-Anforderungsprofil bestimmen
2. ITS-Kompetenzen messen
3. ITS-Statistiken erhalten
4. ITS-Trainingsempfehlungen erhalten







Security Baukasten

Kompetenz-Benchmarking

- Kompetenzmessinstrumente*

ITS-Trainings-Materialien

- Mehrgliedrige Schulungsunterlagen*
- Micro-Learning-Einheiten*

ITS-Awareness-Materialien

- Gebrandete Basic Nudging-Vorlagen (Poster/Flyer, Screen Saver, Serious Games)*
- Innovative Nudges (Awareness-Zonen, Awareness-Podcast*

ITS-Kompetenzprofil

- Bewertete ITS- Bedrohungsfelder auf Grundlage von IT- und Daten- Nutzung
- Notwendige ITS- Kompetenzen

* Beruhen auf Kompetenzmodell

BEISPIEL

Security Baukasten – Ganzheitliche IT-Sicherheitsstrategie je Domaine

Anforderungsprofile

Verwaltungs-personal

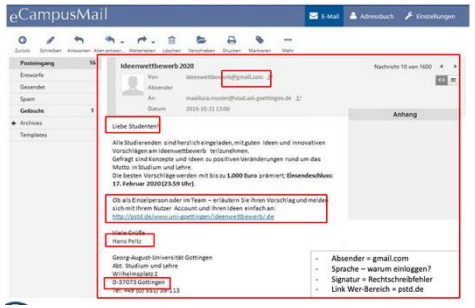
Bspw. über IT-Verwendung

IT-Admins

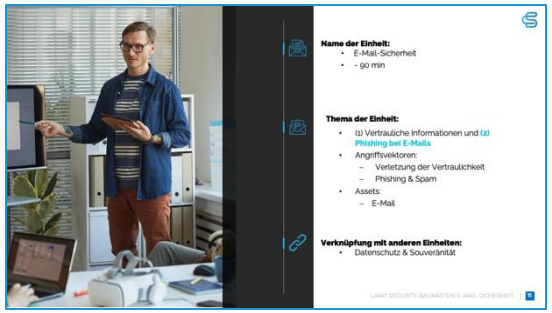
Messinstrumente

Sie sind derzeit für einen Patienten zuständig, auf dessen Blutpobe Sie schon den ganzen Tag warten, um die medikamentöse Einstellung vorzunehmen und dem Stationsarzt, Herrn Köhler, mitzuteilen.

Welche der folgenden möglichen Situationen ist die größte Bedrohung für die Informationssicherheit der Universitätsklinik Grüning?
Sortieren Sie nach folgendem Schema:
[1] Die Situation ist am bedrohlichsten.
[2] Die Situation ist weniger bedrohlich.
[3] Die Situation ist am wenigsten bedrohlich.

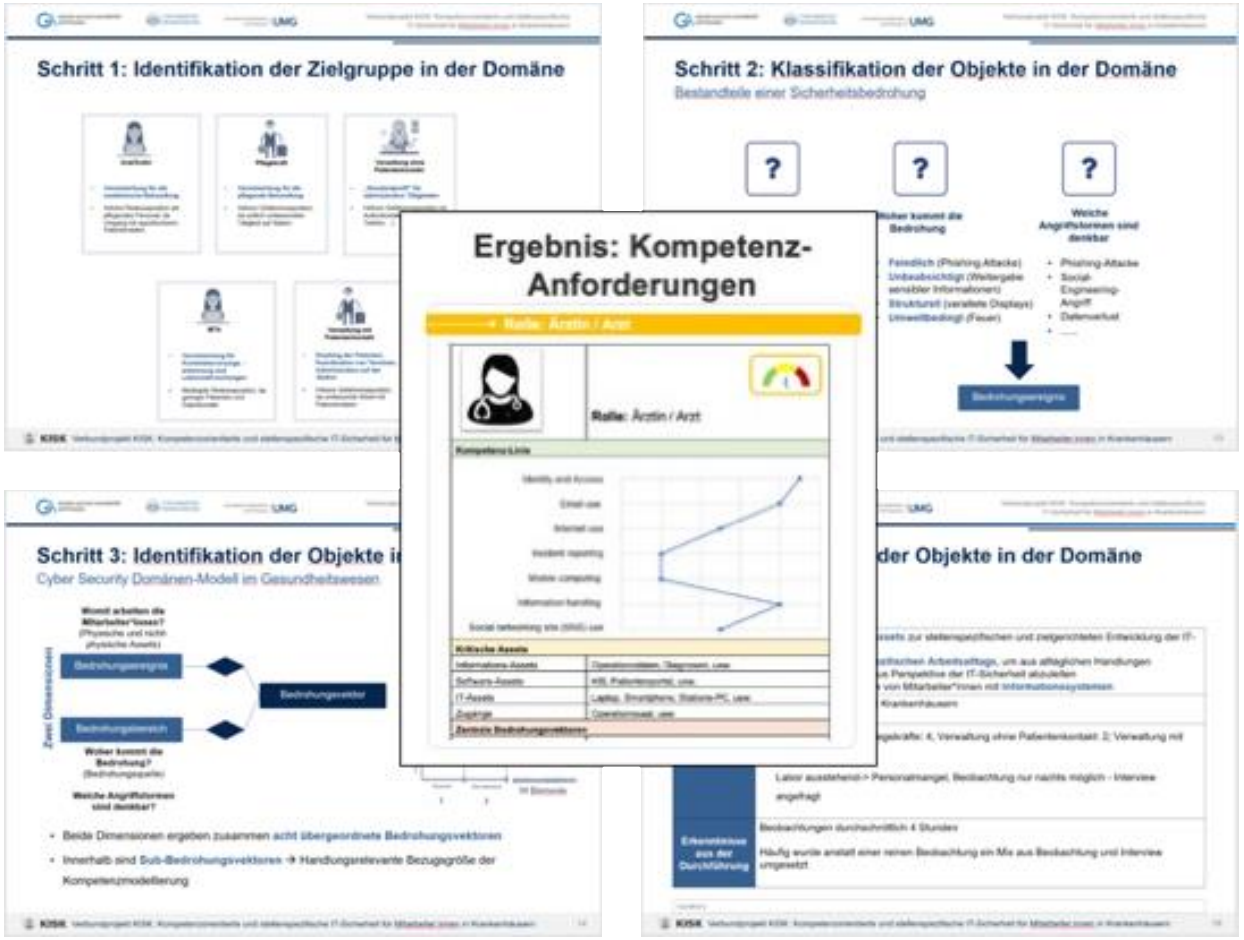


Trainings-Material



Awareness-Material

Erhöhung der Trainings-Effektivität und Reduktion der Trainingszeit durch Kompetenz-Anforderungsprofile



Leitfrage: Welche Kompetenzen benötigen verschiedene MitarbeiterInnen?

Ergebnis

- Kompetenz-Anforderungsprofile: bspw. Geschäftsführung, Außendienst, IT-Admin Ärzt*in, Medizinische Fachkraft, Verwaltungsfachkaft alles je mit und ohne Patient*innenkontakt
- Assets: u.a. Informationen, Software, Physische Assets
- Gewichtete Bedrohungen
- Kompetenz-Linien
- Kompetenzmessinstrumente

Ranking der Bedrohungsvektoren Profil: ärtzliches Fachpersonal

Nr.	Relevante Bedrohungsvektoren (d.h. Bedrohungsereignis & Kritisches Asset)	
1.1	Falscher Umgang mit kritischen und/oder sensiblen Informationen durch autorisierte Benutzer / KIS oder Mitarbeitende	Ein autorisierter, privilegierter Benutzer gibt versehentlich kritische/sensible Informationen bei Nutzung des KIS preis.
1.2	Angreifer erstellt Duplikate legitimer Internetseiten und leitet die Mitarbeitende auf gefälschte Internetseiten, um Informationen zu sammeln (z.B. Duplizierung einer Internetseite eines Lieferanten) / Internet-Browser	Typische Angriffe erfolgen per E-Mail, Instant Messaging oder auf vergleichbare Weise; dabei werden die Benutzer in der Regel auf scheinbar legitime Websites geleitet, während die eingegebenen Informationen in Wirklichkeit gestohlen werden.
1.3	Einschleusen falscher, aber glaubwürdiger Daten/Informationen in organisatorische Informationssysteme (z.B. von Insidern) / KIS	Ein autorisierter Benutzer verunreinigt irrtümlich ein Gerät, ein Informationssystem oder ein Netzwerk, indem er Informationen mit einer Klassifizierung/Sensibilität darauf ablegt oder an sie sendet, zu deren Handhabung er nicht autorisiert wurde.
1.4	Einschleusen bekannter Malware an interne Informationssysteme (z.B. Viren über unsichere Internetseiten) / Internetbrowser	Der Angreifer nutzt gängige Übermittlungsmechanismen (z. B. über unsichere Webseiten), um bekannte Malware (z. B. Malware, deren Existenz bekannt ist) in Informationssysteme von Unternehmen zu installieren/einzuschleusen.
1.5	Falscher Umgang mit kritischen und/oder sensiblen Informationen durch autorisierte Benutzer / Smartphone	Ein autorisierter, privilegierter Benutzer gibt versehentlich kritische/sensible Informationen über sein Smartphone preis.
1.6	Spear-Phishing (z.B. durch personalisierte Mails) / Mailsystem	Der Angreifer fälscht Mitteilungen von einer legitimen/vertrauenswürdigen Quelle, um sensible Informationen wie Benutzernamen, Kennwörter oder SSN zu erlangen. Typische Angriffe erfolgen über E-Mail, Instant Messaging oder vergleichbare Mittel.
1.7	Verwendung von nicht autorisierter Hard- und Software von Drittanbietern / Mitarbeitende	Dieses Risiko entsteht, wenn Mitarbeitende Geräte, Anwendungen oder Dienste in das Unternehmensnetzwerk einbringen, die nicht durch die IT-Abteilung geprüft und genehmigt wurden.
1.8	Social Engineering Angriffe, um Mitarbeitende davon zu überzeugen, schädliche Maßnahmen zu ergreifen (z.B. durch Shoulder Surfing) / Mitarbeitende	Der Angreifer unternimmt Aktionen (z. B. per E-Mail oder Telefon) mit der Absicht, Mitarbeitende überreden oder auf andere Weise dazu zu bringen, kritische/sensible Informationen (z. B. personenbezogene Daten) preiszugeben.
1.9	Verbreiten sensibler Informationen (z.B. durch Kommunikation über WhatsApp) / Instant-Messenger	Ein autorisierter Benutzer kontaminiert irrtümlich ein Gerät, Informationssystem oder Netzwerk, indem er darauf Informationen mit einer Klassifizierung/Sensibilität, zu deren Handhabung er nicht berechtigt ist. Die Informationen sind dem Zugriff Unbefugter ausgesetzt, und das Gerät, System oder Netzwerk ist nicht verfügbar, während der Schaden untersucht und entschärft wird.
1.10	Autorisiertem Personal folgen, um Zutritt zu organisatorischen Einrichtungen zu erhalten / Mitarbeitende / Physische Parameter	Der Angreifer folgt ("tailgates") autorisierten Personen in sichere/kontrollierte Bereiche mit dem Ziel, sich unter Umgehung der physischen Sicherheitskontrollen Zugang zu Einrichtungen zu verschaffen.

Kompetenzforschung und dessen Potential:– Ganzheitliche IT-Sicherheitsstrategie je Domaine

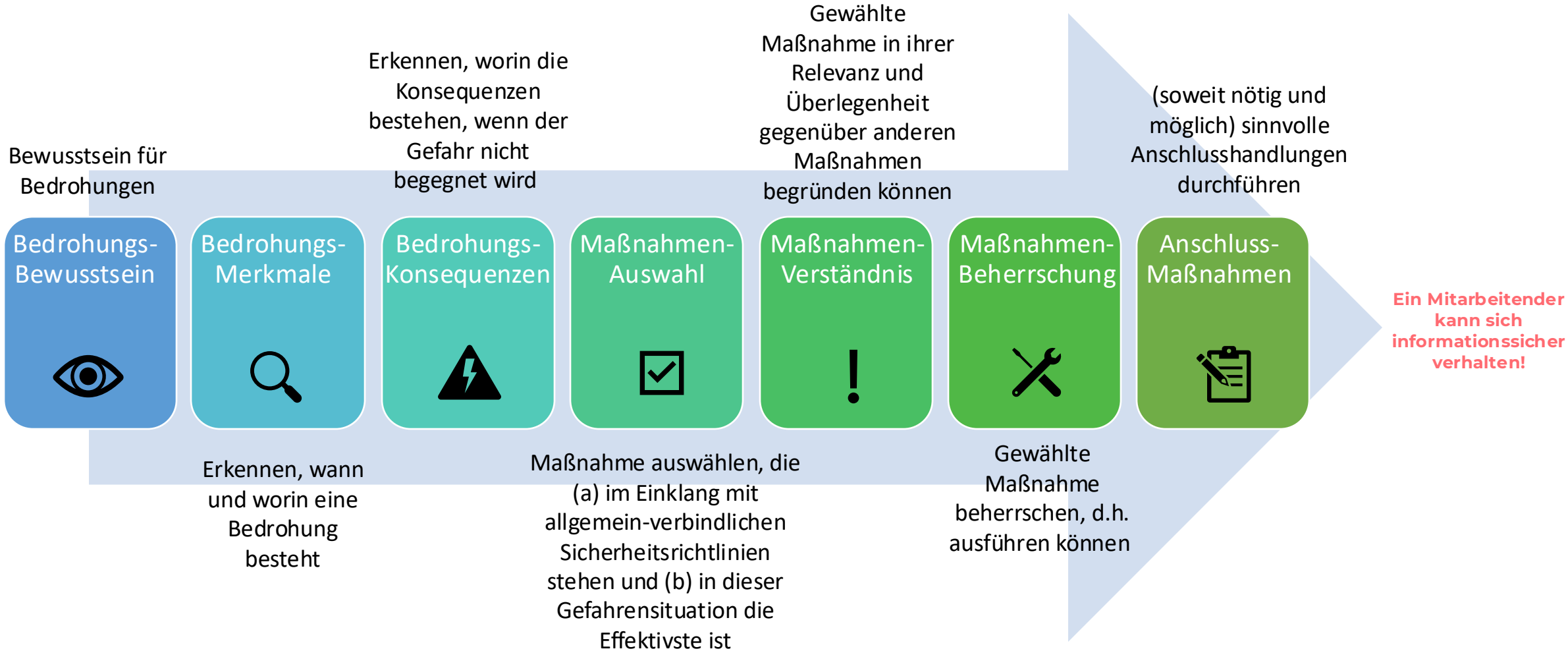
Jemand ist in einem Bereich gut qualifiziert durch:

Was?	Konzeptionelle Kompetenz	Regelbasiertes, abstraktes Wissen in einem Bereich.
Wie?	Prozessuale Kompetenz	Wissen über Verfahren und Fähigkeiten, die erforderlich sind, um konzeptionelles Wissen in bestimmten Handlungssituationen anzuwenden.
Wann?	Interpretierende Kompetenz	Kognitives Erkennen der Anforderungssituation und Wissen über angemessene Interpretation und Validierung der Situation.
Warum?	MotivationaleKompetenz	Grundlegende motivationale und affektive Merkmale in bestimmten Handlungssituationen.

Jemand ist gut qualifiziert sich informationssicher zu verhalten:

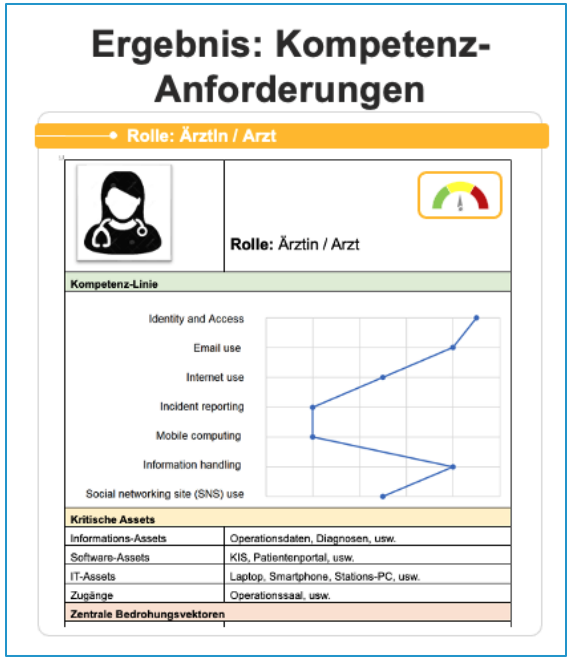
- Wissen über ITS-Bedrohungen & ITS- Maßnahmen
- Anwendung von ITS-Maßnahmen
- Erkennen von ITS-Bedrohungen
- Auswahl der besten Gegenmaßnahmen
- Bewertung der Gegenmaßnahmen
- Motivierende Faktoren

Entwicklung Kompetenzmessinstrumente Profil : medizinisches Fachpersonal



Messung des IST-Zustands und Vergleich mit dem Soll-Zustand der Security Awareness

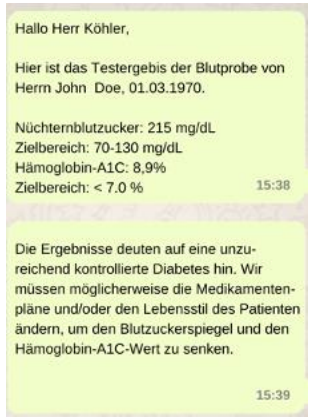
1.

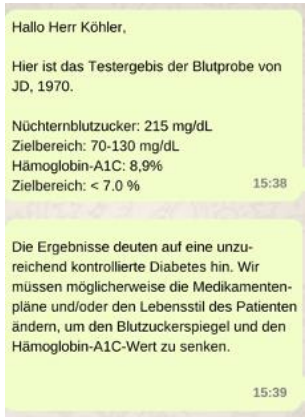


2.

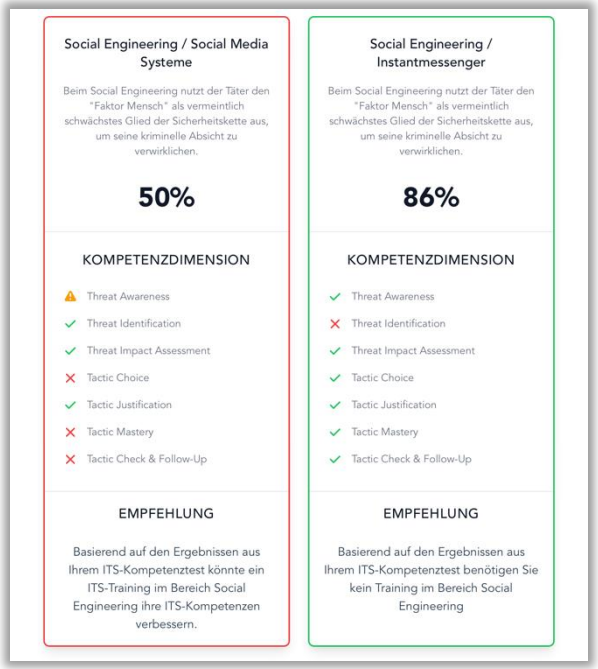
Sie sind derzeit für einen Patienten zuständig, auf dessen Blutpobe Sie schon den ganzen Tag warten, um die medikamentöse Einstellung vorzunehmen und dem Stationsarzt, Herrn Köhler, mitzuteilen.

Welche der folgenden **möglichen Situationen** ist die **größte Bedrohung** für die **Informationssicherheit** der Universitätsklinik Grüning?
Sortieren Sie nach folgendem Schema:
[1] Die Situation ist **am** bedrohlichsten.
[2] Die Situation ist **weniger** bedrohlich.
[3] Die Situation ist **am wenigsten** bedrohlich.





3.



A	Personenbezogene Daten des Patienten werden nicht anonymisiert. (1)
B	Personenbezogene Daten des Patienten werden über WhatsApp ausgetauscht. (2)
C	Personenbezogene Daten des Patienten werden nicht pseudonymisiert. (1)
D	Der Nüchternblutzuckerspiegel liegt deutlich über dem Zielbereich. (0)

Messung des IST-Zustands der Security Awareness

Bitte betrachten Sie nochmals **diese Nachricht** genauer:

Was macht diese Nachricht konkret zu einer **Bedrohung der Informationssicherheit**?

Wählen Sie **eine** Antwort aus.

O Personenbezogene Daten des Patienten werden nicht anonymisiert.

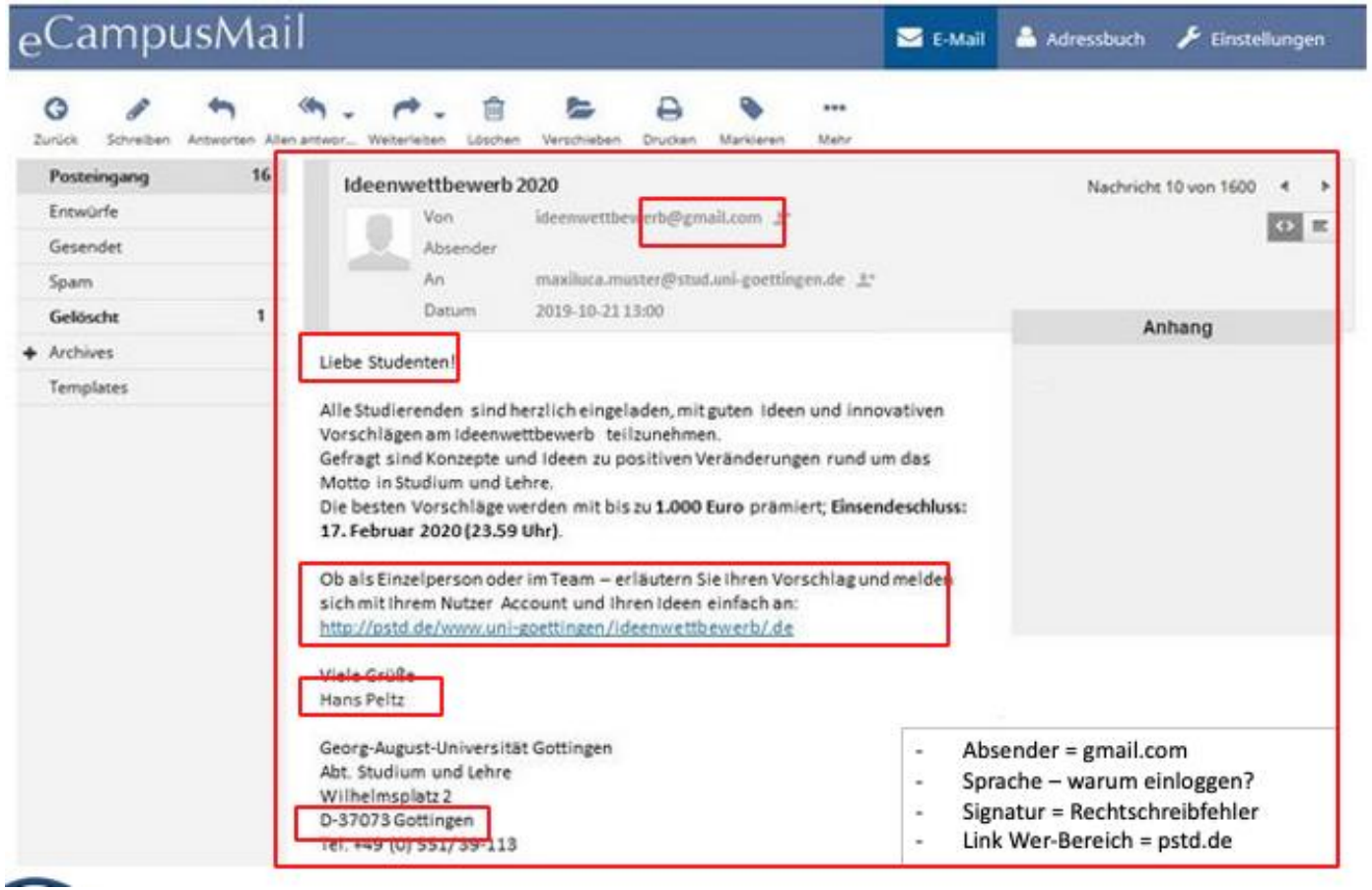
O Personenbezogene Daten des Patienten werden über private Messengerdienste ausgetauscht.

O Personenbezogene Daten des Patienten werden nicht pseudonymisiert.

O Personenbezogene Daten des Patienten werden nicht mit einer Ende-zu-Ende-Verschlüsselung ausgetauscht.

O Der Patient hat starke Brustschmerzen und braucht für heute Nachmittag ein EKG.

Messung des IST-Zustands der Security Awareness



BEISPIEL: MESSINSTRUMENT

Input Phishing

Stress

1. **Workload:** Erhöhter Arbeitsaufwand durch zusätzliche Mails
2. **Misstrauen:** Häufige und ohne Transparenz durchgeführte Simulationen werde als Manipulation wahrgenommen
3. **Technostress:** Stress durch bspw. Gamification

Bestrafung

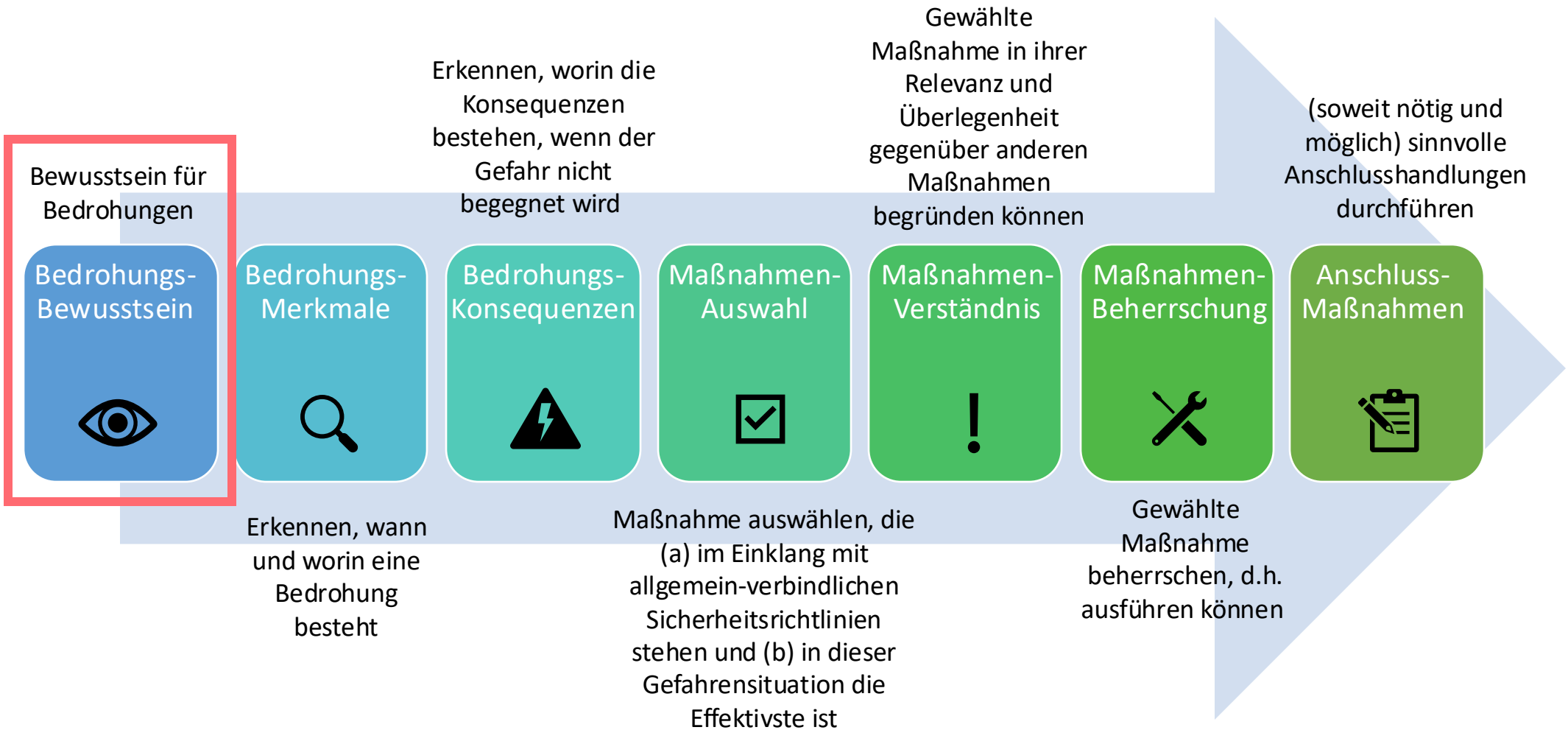
1. **Motivation:** Sinkende Motivation bspw. Phishingmails zu melden
2. **Lernbereitschaft:** Interesse aus Situationen zu lernen sinkt stark
3. **Fehleranfälligkeit:** Mitarbeitende machen häufiger Fehler, die sie vorher nicht gemacht hätten

Messbarkeit

1. **Schwierigkeitsgrad:** Ohne Profilzuordnung keine Aussagekraft
2. **Klickrate bei bestimmten Themen:** Keine Aussagekraft ohne vorherige Justierung
3. **Branchenvergleich:** Keine Aussagekraft, wenn Mails angepasst wurden

BEISPIEL

Entwicklung Kompetenzmessinstrumente Profil : medizinisches Fachpersonal



BEISPIEL

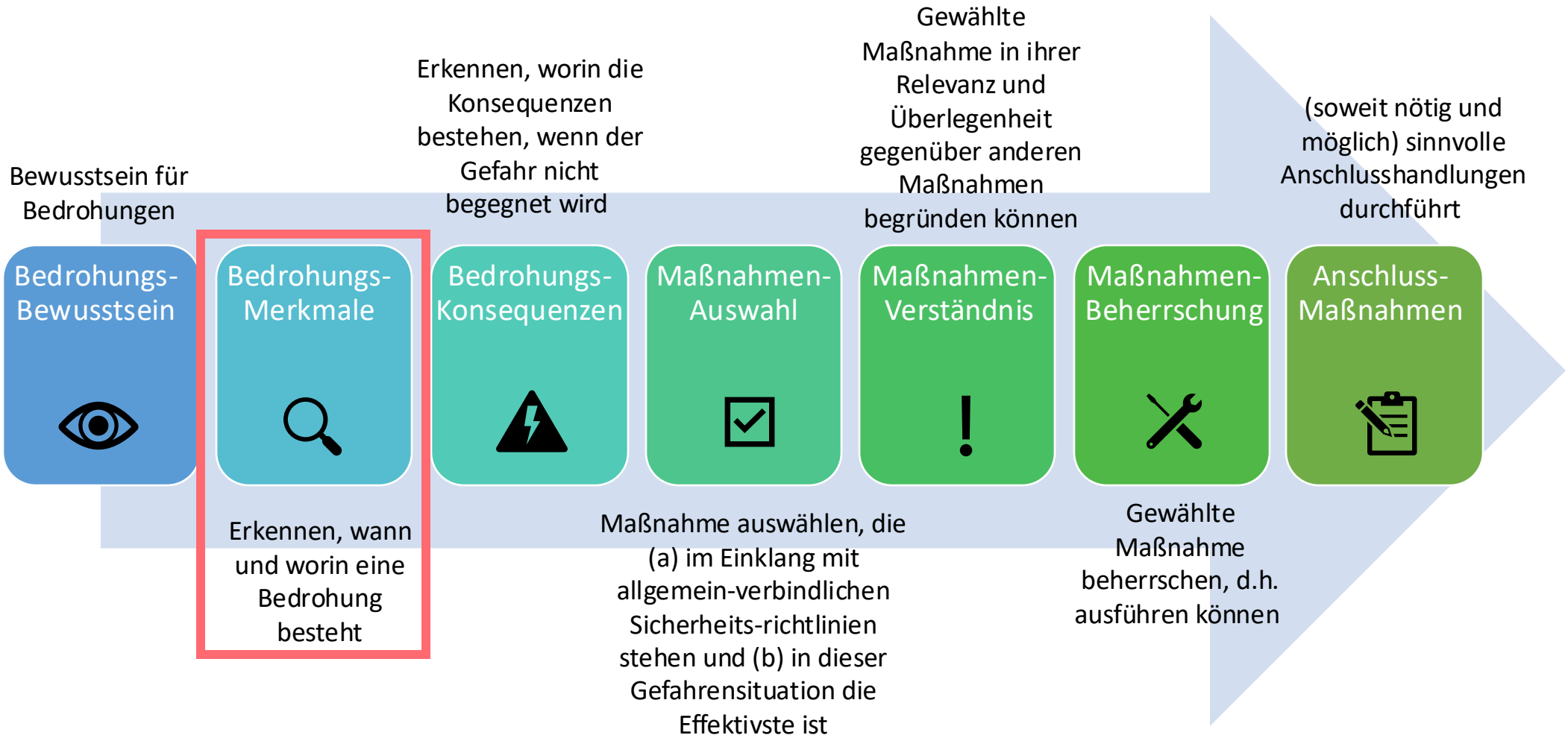
Bedrohungs-Bewusstsein– Entwicklung Kompetenzmessinstrumente Profil: medizinisches Fachpersonal

Nachdem Sie heute Morgen Ihren Frühdienst beendet haben und nun zu Hause angekommen sind, erinnern Sie sich plötzlich daran, dass Sie während der Übergabe eine wichtige Information vergessen haben an Ihre Kollegin weitergegeben. Schnell zücken Sie Ihr privates Smartphone und senden eine kurze Nachricht über einen Ihrer privaten Messenger-Dienste an sie. Welche der folgenden möglichen Nachrichten ist die größte Bedrohung für die Informationssicherheit der Universitätsklinik Grüning?

Sortieren Sie nach folgendem Schema:
[1] Die Nachricht ist **am bedrohlichsten**.
[2] Die Nachricht ist **weniger** bedrohlich.
[3] Die Nachricht ist **am wenigsten** bedrohlich.

BEISPIEL

Entwicklung Kompetenzmessinstrumente Profil : medizinisches Fachpersonal



BEISPIEL

Bedrohungs-Merkmale– Entwicklung Kompetenzmessinstrumente Profil: medizinisches Fachpersonal

Bitte betrachten Sie nochmals **diese Nachricht** genauer:

Was macht diese Nachricht konkret zu einer **Bedrohung der Informationssicherheit**?

Wählen Sie **eine** Antwort aus.

O Personenbezogene Daten des Patienten werden nicht anonymisiert.

O Personenbezogene Daten des Patienten werden über private Messengerdienste ausgetauscht.

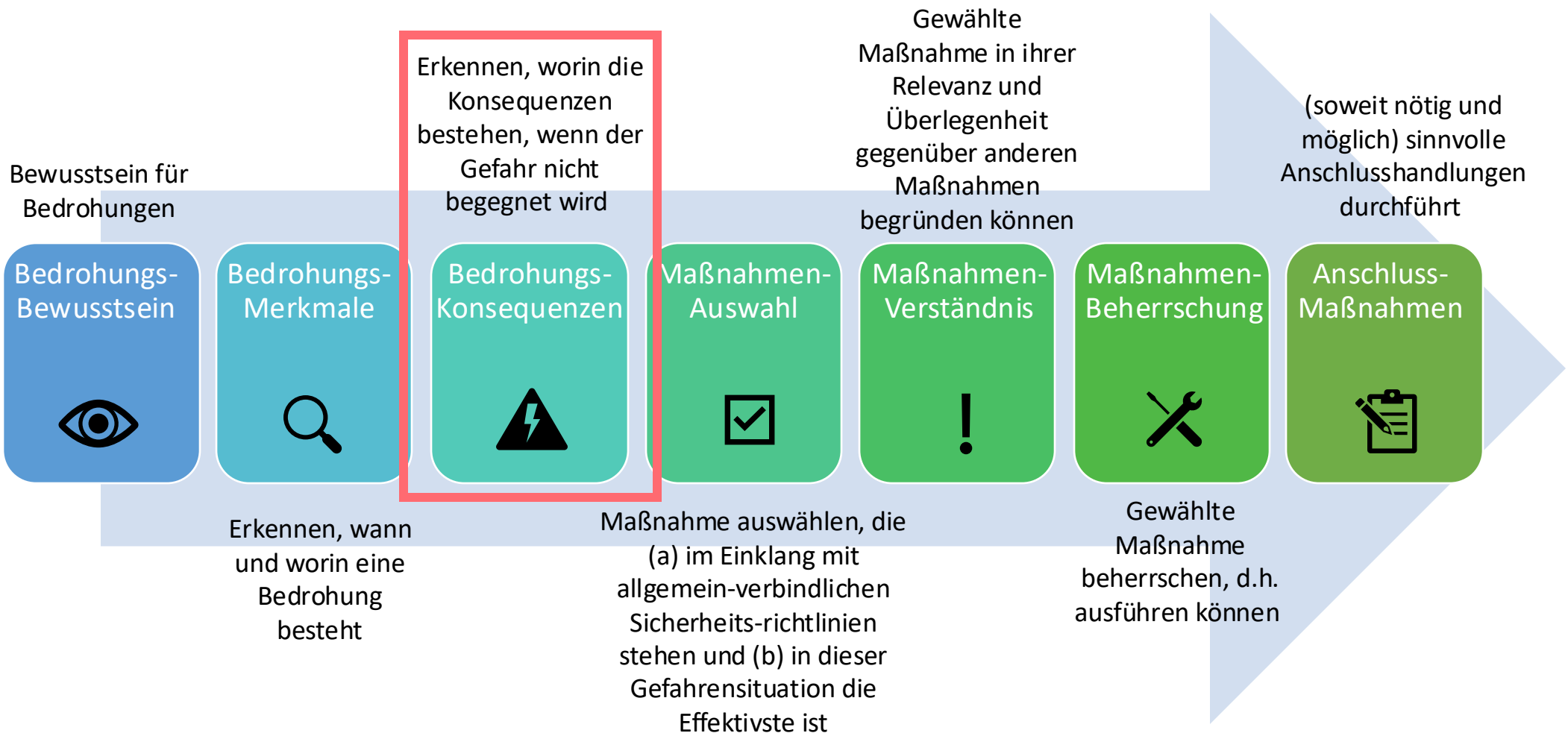
O Personenbezogene Daten des Patienten werden nicht pseudonymisiert.

O Personenbezogene Daten des Patienten werden nicht mit einer Ende-zu-Ende-Verschlüsselung ausgetauscht.

O Der Patient hat starke Brustschmerzen und braucht für heute Nachmittag ein EKG.

BEISPIEL

Entwicklung Kompetenzmessinstrumente Profil : medizinisches Fachpersonal



BEISPIEL

Bedrohungs-Konsequenzen– Entwicklung Kompetenzmessinstrumente Profil: medizinisches Fachpersonal

Welche Konsequenzen könnte diese Nachricht schlimmstenfalls für die Informationssicherheit der Universitätsklinik Grüning nach sich ziehen?

Wählen Sie **eine** Antwort aus.

Durch diese Nachricht könnte …

O die Universitätsklinik Grüning eine Geldstrafe auferlegt bekommen.

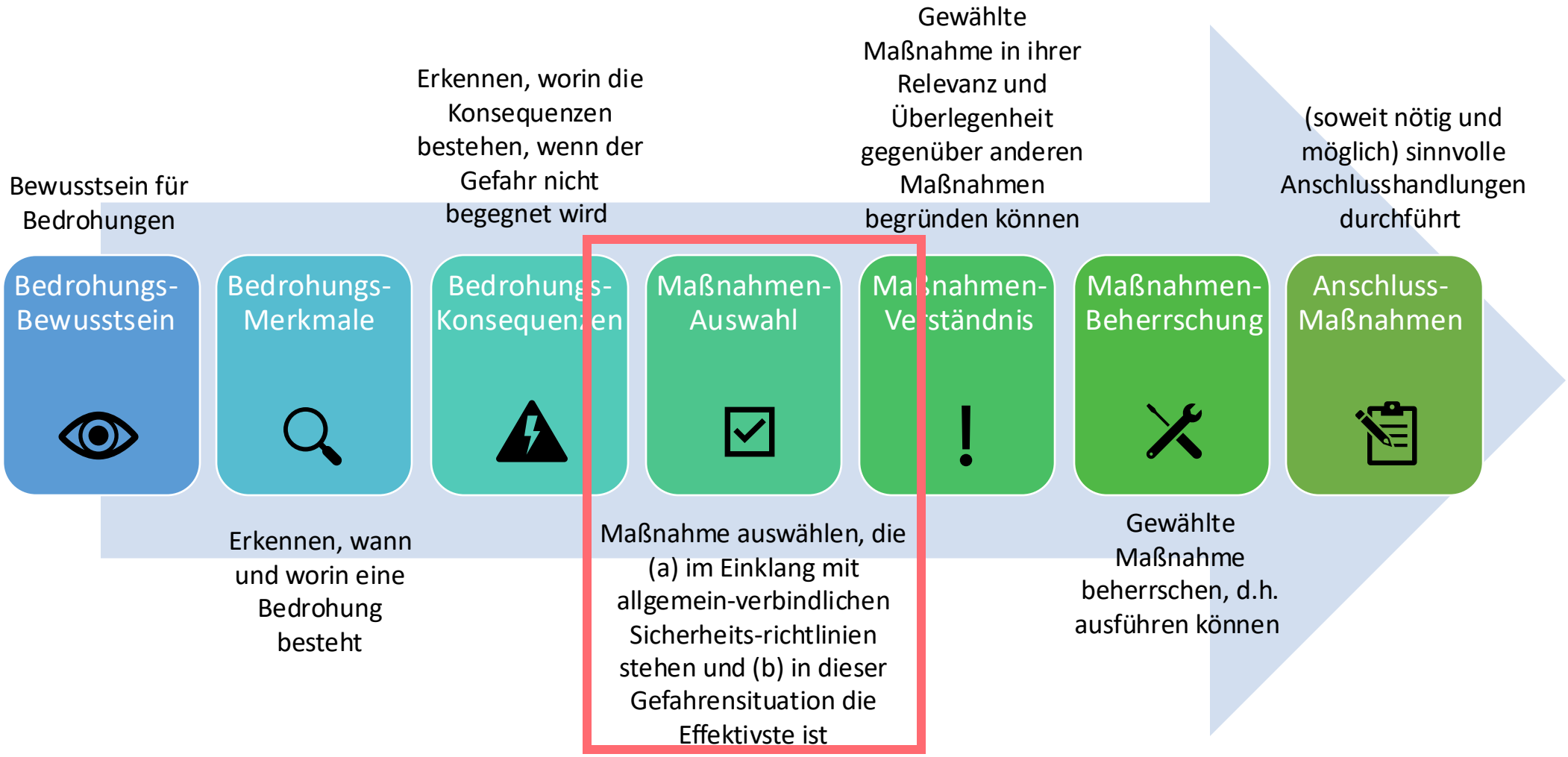
O es zu einer Verletzung des Datenschutzes führen, wenn der Patient die Weitergabe der personenbezogenen Daten ausdrücklich verbietet.

O es die Privatsphäre des Patienten verletzen, was zu Rufschädigung des Patienten und Verlust des Vertrauens in das Personal der Klinik führen kann.

O den beteiligten Mitarbeitenden der Universitätsklinik aufgrund von Datenschutzverletzungen ein Verlust ihres Arbeitsplatzes drohen.

BEISPIEL

Entwicklung Kompetenzmessinstrumente Profil : medizinisches Fachpersonal



BEISPIEL

Maßnahmen-Auswahl – Entwicklung Kompetenzmessinstrumente Profil: medizinisches Fachpersonal

Welche der aufgeführten **Maßnahmen** hätten Sie angesichts dieser Be drohung ergreifen müssen?

Wählen Sie **eine** Antwort aus.

Ich übermittle personenbezogene Daten …

O nur pseudonymisiert via private Messengerdienste.

O nur anonymisiert via private Messengerdienste.

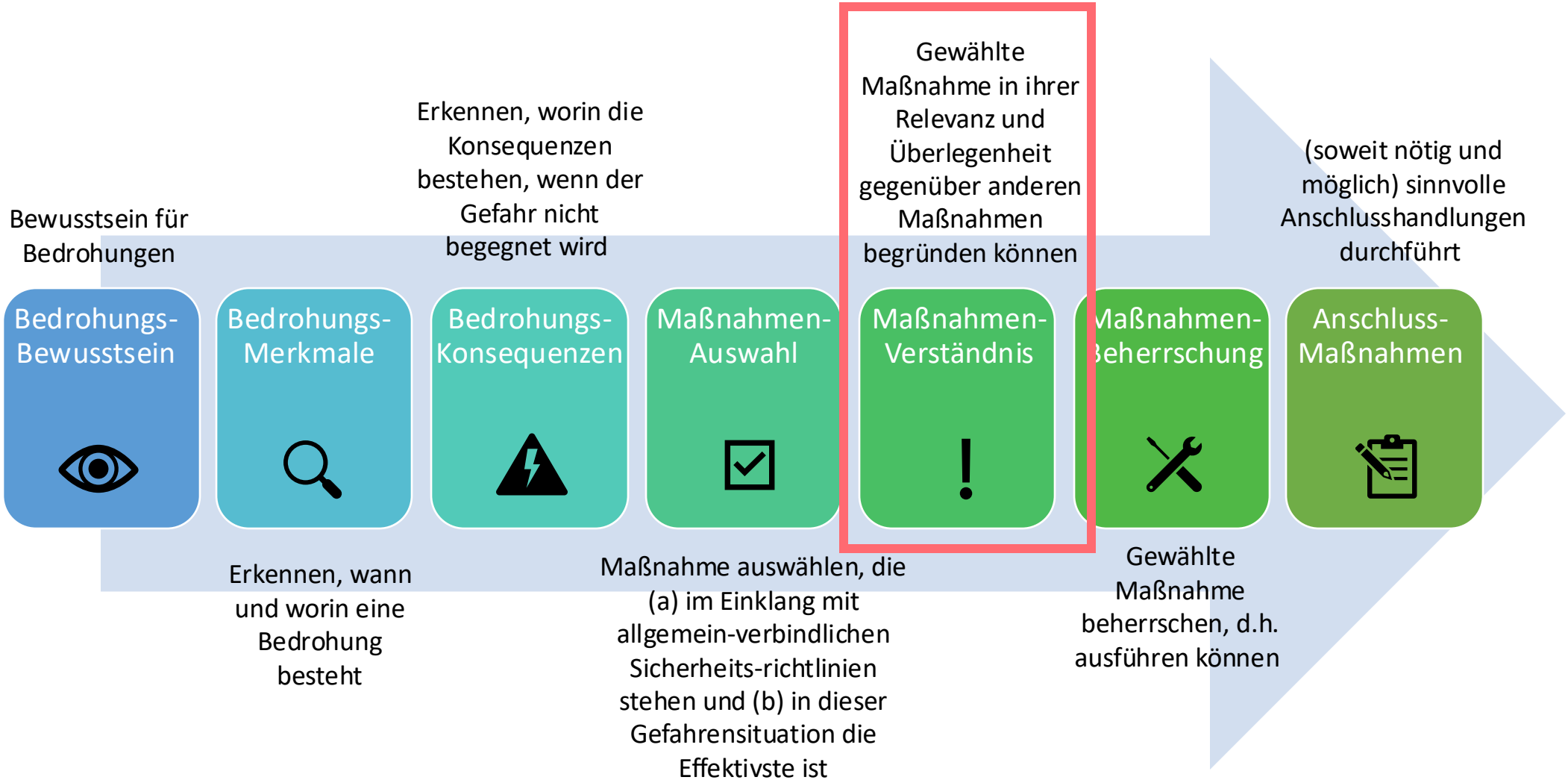
O verschlüsselt über private Messengerdienste.

O via private Messengerdienste und lösche die Nachricht sofort nachdem sie gelesen wurde.

O über keinen meiner privaten Messengerdienste.

BEISPIEL

Entwicklung Kompetenzmessinstrumente Profil : medizinisches Fachpersonal



BEISPIEL

Maßnahmen-Verständnis – Entwicklung Kompetenzmessinstrumente Profil: medizinisches Fachpersonal

Warum ist es wichtig, personenbezogene Daten über organisationsinterne Kommunikationswege zu übermitteln?

Wählen Sie **eine** Antwort aus.

Diese Wege gewährleisten …

O …
eine höhere Geschwindigkeit beim Übermitteln von Informationen und verbessern die Effizienz der medizinischen Versorgung.

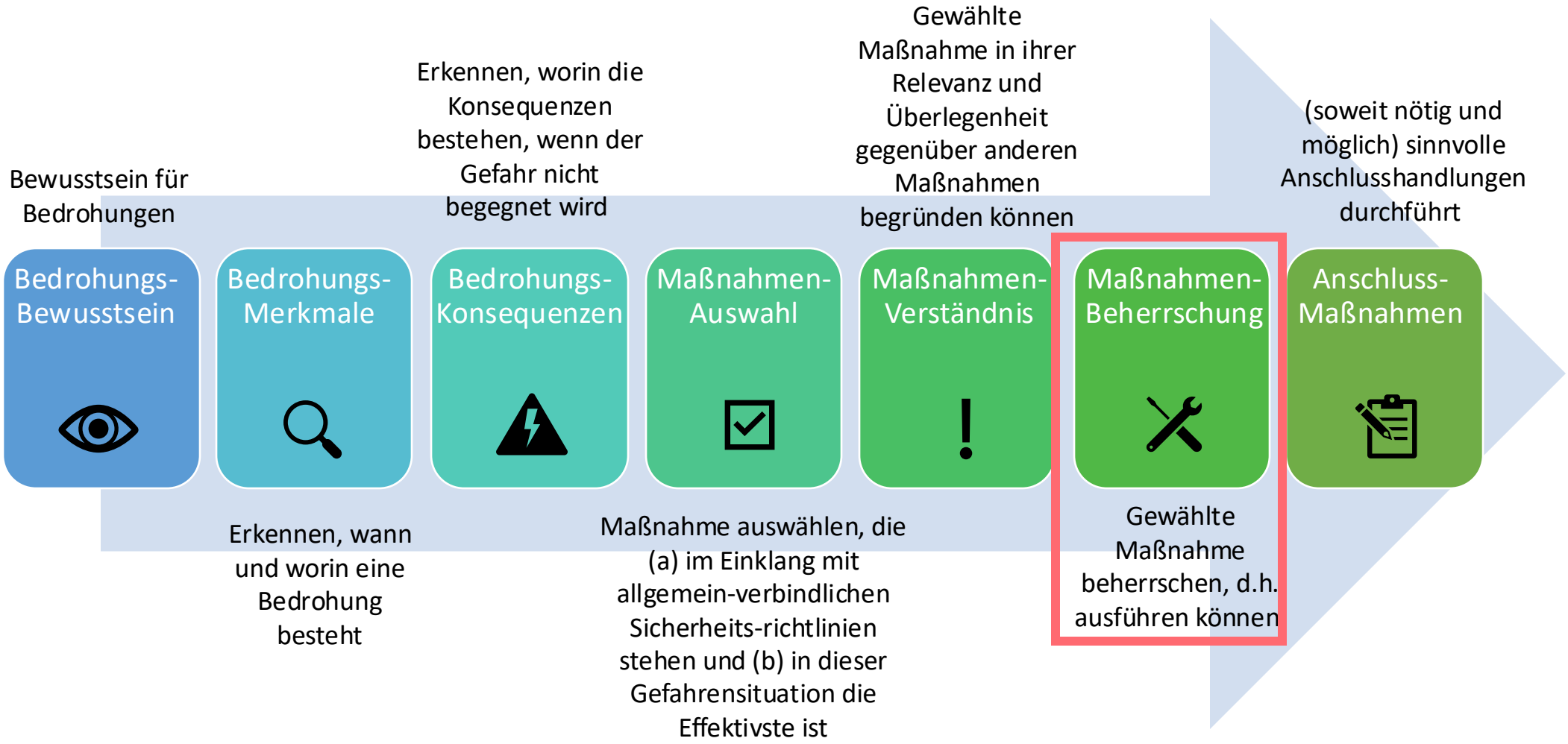
O … gewährleisten den Schutz personenbezogener Daten der Patient:innen, indem sie über notwendige Sicherheitsmaßnahmen verfügen.

O … eine unverschlüsselte Übermittlung personenbezogener Daten,
um unbefugten Zugriff und Datenlecks zu verhindern.

O … eine bessere Koordination zwischen den verschiedenen Abteilungen und Fachkräften im Gesundheitswesen, was zu einer verbesserten Patientenversorgung führen kann.

BEISPIEL

Entwicklung Kompetenzmessinstrumente Profil : medizinisches Fachpersonal



BEISPIEL

Maßnahmen-Beherrschung – Entwicklung Kompetenzmessinstrumente Profil: medizinisches Fachpersonal

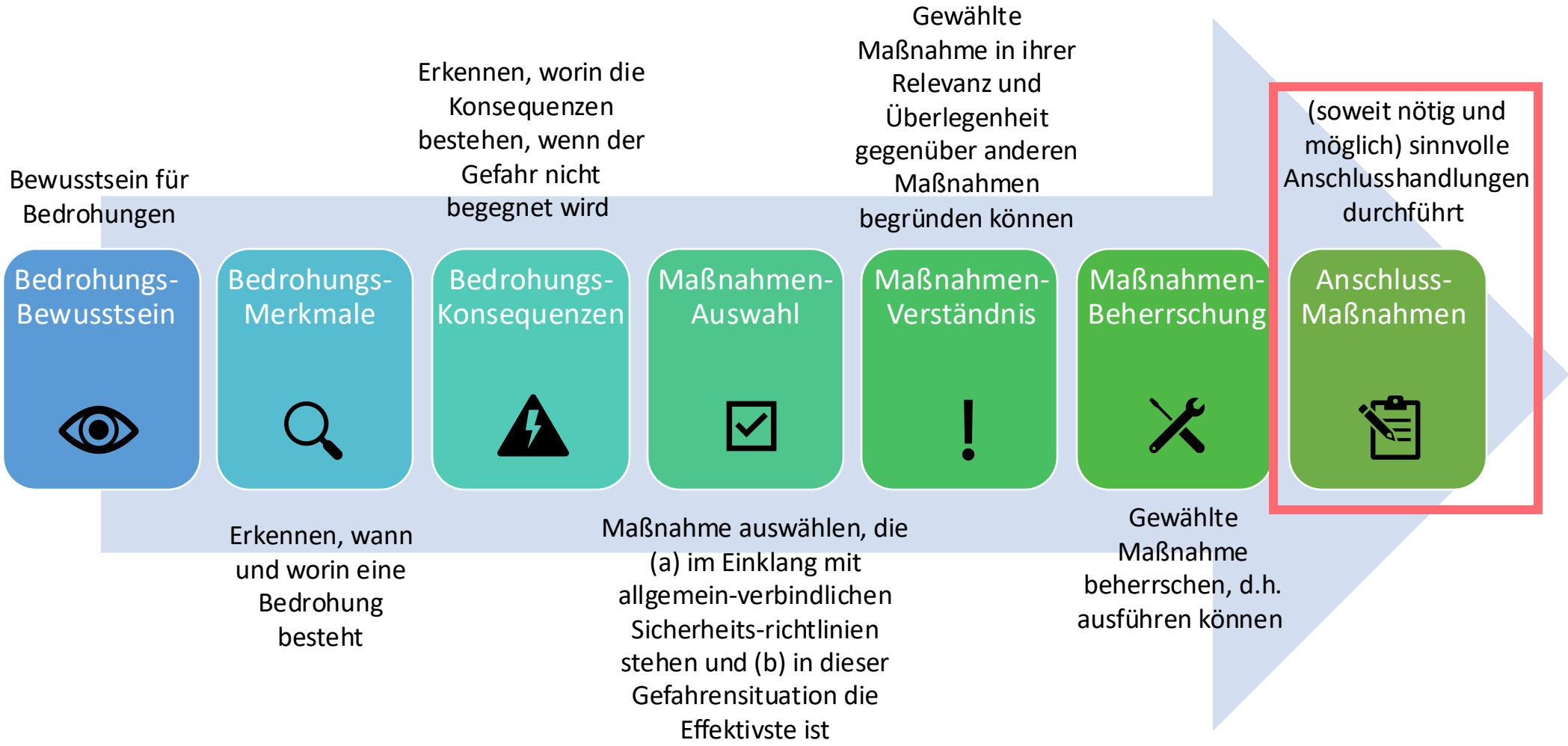
Wenn Sie personenbezogene Daten über organisationsinterene Kommunikations-wege übermitteln möchten, **wie** gehen Sie dabei konkret vor?

Wählen Sie **zwei** Antworten aus.

- [ ] Ich übermittle die Information unverschlüsselt über meine private E-Mail.
- [ ] Ich übermittle die Information vollständig über die klinischen IT-Systeme.
- [ ] Ich rufe meine Kollegin bei Dringlichkeit persönlich per Diensttelefon an und mache sie auf die Information aufmerksam.
- [ ] Ich übermittle die Information verschlüsselt über meine private E-Mail.
- [ ] Ich übermittle die Information über eine kurze SMS mit meinem privaten Smartphone.

BEISPIEL

Entwicklung Kompetenzmessinstrumente Profil : medizinisches Fachpersonal



BEISPIEL

Anschluss-Maßnahmen – Entwicklung Kompetenzmessinstrumente Profil: medizinisches Fachpersonal

Welche **ergänzenden Maßnahmen** zur Gefahrenabwehr sind in dieser Situation sinnvoll oder gar notwendig?

Wählen Sie **zwei** Antworten aus.

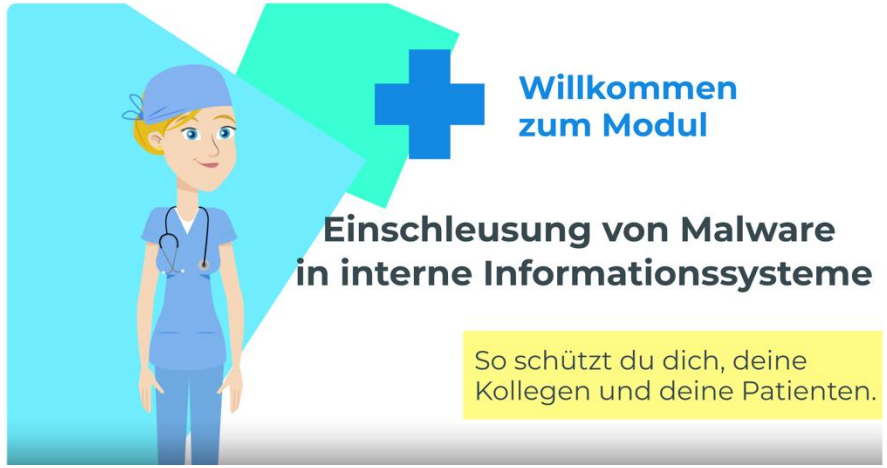
☐ Ich informiere mich über die aktuellen Datenschutzrichtlinien und -vorschriften meiner Organisation und halte mich daran.

☐ Ich beantrage die Nutzung von Ende-zu Ende-Verschlüsselung für meine privaten Messenger-Dienste bei der Informationssicherheitsabteilung.

☐ Ich nehme regelmäßig an Schulungen und Fortbildungen zum Datenschutz und zur Datensicherheit teil.

☐ Ich anonymisiere alle personenbezogenen Daten während der Kommunikation mit meiner Kollegin.

Steigerung der Trainingsmotivation durch situierte, tätigkeits-adäquate und interaktive Trainings-Module



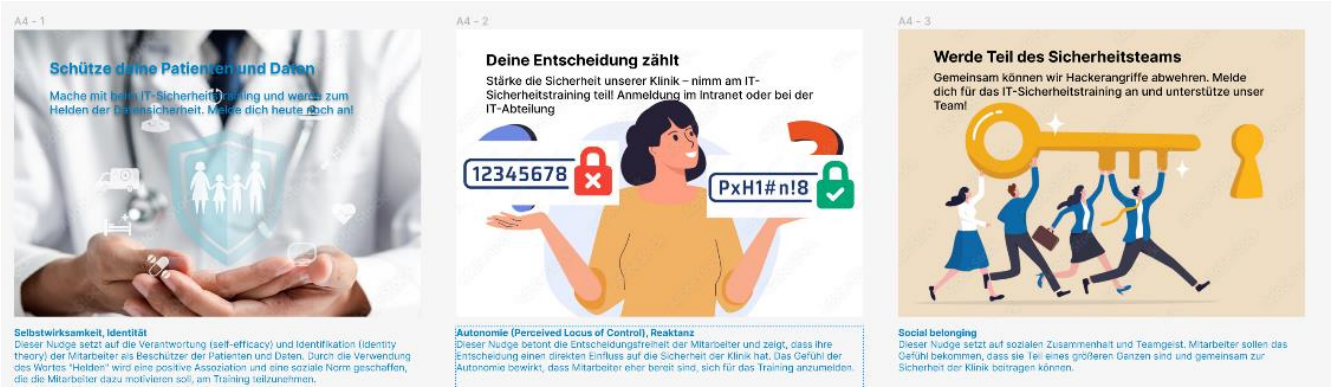
Leitfrage: Wie lassen sich effektiv und tätigkeits-adäquat die benötigten Kompetenzen vermitteln?

Ergebnis

- Interaktive-Online-Trainings (‚Micro-Interventionen‘)
- Situiert, ausgelegt an beobachteten Handlungsszenarien
- Kurzweilig, leicht in den Arbeitsalltag integrierbar

Nachhaltige Steigerung des tatsächlichen sicheren Verhaltens der MitarbeiterInnen im Arbeitsalltag

Poster



Innovative Konzepte

Aufsteller

Leitfrage: Wie lässt sich die ‚Knowledge-Doing-Gap' umschiffen?

Ergebnis

- Micro-Nudges: Aufsteller, Bildschirmschoner, Innovative Konzepte „Micro-Games"
- Kampagnen-Pläne

FEEDBACK

Testung Kompetenzmessinstrumente Profil: medizinisches Fachpersonal

Die Messauswertungen zeigen, dass die spezifischen Trainings einen signifikant höheren Lerneffekt haben, als allgemeine Trainings.

Ich empfand das Thema als spannend und wichtig. Wenn ich was verbessern müsste: eine Fortschrittsanzeige ;)

Das waren realistische Situationen, die passieren können, besonders die erste. Die Studie hat auch Spaß gemacht zu bearbeiten und zu überlegen, wie ich in der Situation reagieren würde.

Sehr immersiv und extremst realistische Situationen. Zudem auch tolle Bilder!

ich musste teilweise raten, weil ich nicht sicher war

Ein abschließendes Feedback, dass die gewählten Antworten noch einmal mit den korrekten Maßnahmen vergleicht, wäre wünschenswert gewesen.

Die Teilnahme per Mobiltelefon war teilweiße schwierig. Die drei Situationen, welche ein Rechnungssystem zeigten und Detailansichten der Rechnungen war auch in Vergrößerung so gut wie nicht zu lesen. Evtl zukünftig auf PC beschränken?

Vielen Dank für Ihre Aufmerksamkeit!

Vielen Dank für Ihre Aufmerksamkeit!

LinkedIn

Dr. Kristin Masuch

KISK-Materialien

Kontakt

kristin.masuch@cysec-institut.de

ITS.kompetent-Materialien