

Onboarding von Quereinsteigern in die InfoSec

von der medizinischen Pflege hin zur Absicherung von IT-Systemen

Philipp Reisinger – SBA & Christoph Stock - GRAWE

Vorstellung



Philipp Reisinger

Informationssicherheitsberater SBA Research

preisinger@sba-research.org



Christoph Stock

CISO Grazer Wechselseitige Versicherung AG

Christoph.stock@grawe.at

01-2022: Mitarbeitergespräch Informationssicherheits- Risikomanagerin kündigt mit 01.07.2022

Ausschreibungen



1.Versuch-01-2023

1 Bewerber

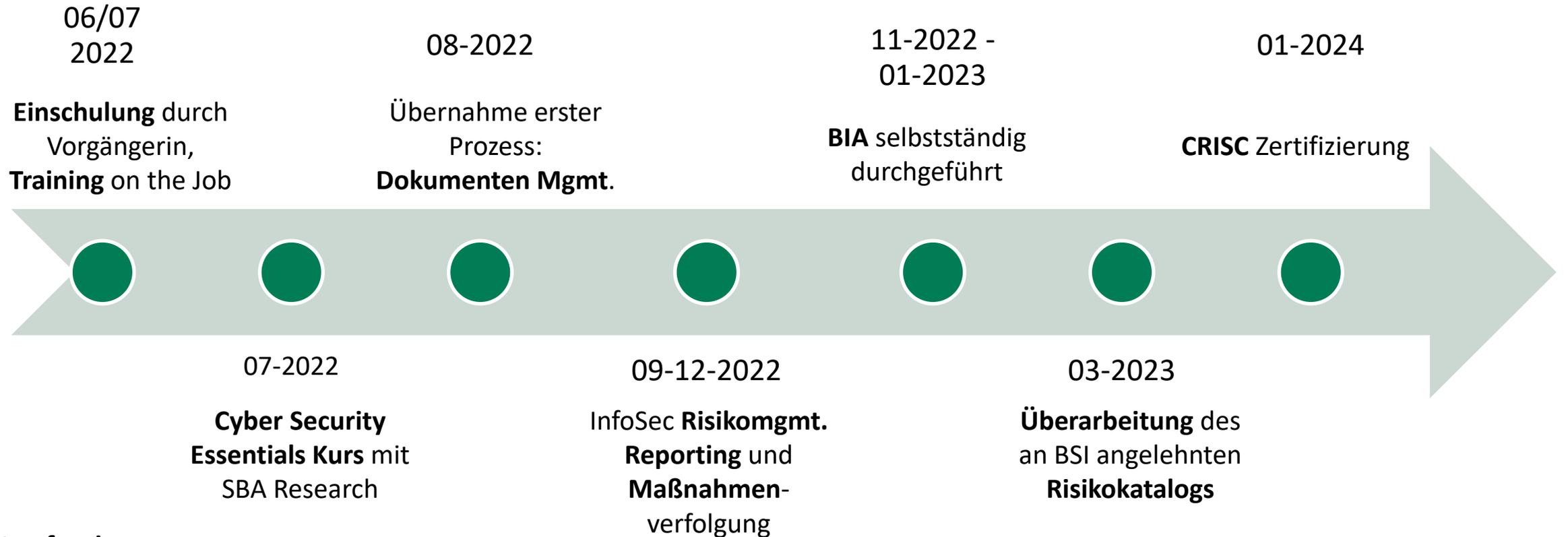
2.Versuch-04-2023

7 Bewerber

Mitarbeiter - Profil

- Ausgebildet als Diplomkrankenschwester
- Als Führungskraft tätig
- Prozessmanagement
 - Selbst Prozesse definieren und verbessern
 - Hohes Reifegradbewusstsein
- Dokumentenmanagement
 - Selbst Richtlinien verfassen
 - Auf Einhaltung kontrollieren
 - Strikte Handhabung
- Risikomanagement
 - Mehrmals täglich
 - Ableitung von Maßnahmen
 - Reporting
 - Maßnahmenverfolgung
- Nachvollziehbare und lückenlose Dokumentation

Ausbildung bzw. Doing in the Job



Laufend:

- **Training on the Job**
- **Mentoring Sessions**
- **Informelles Lernen/Austausch** (Mittagessen etc.)
- **Partner** ebenso in IT -> dadurch bekommt man auch andere Brille/Sicht mit

Lessons Learned

- Persönlichkeit entscheidend
 - Sehr engagiert
 - Akribisches abarbeiten
 - Motivation & persönliches Interesse
- Job sehr umfangreich – daher - nicht nur inhaltliche sondern auch die Prozessuale Ebene betrachten
- Mentoring braucht Zeit!
 - Konzept für mehrere Wochen/Monate
 - Teilzeit passt perfekt in den Mentoring Rahmen
 - Schauen, dass die sich Person bald produktiv einbringen kann – nicht zu lange „rumdümpeln“ -> Selbstvertrauen stärken & erste „Erfolgsergebnisse“ ermöglichen

Grenzen: Was geht & was geht nicht?

- + **Governance**, Compliance, **Prozesse** (& Prozess Mgmt.)
- + **Support Center** (Enduser Anfragen und Support)
- + Aufbereitung von **Awareness** Schulungen
- + **Projekt Mgmt.**
- + Infosec/IT **Koordinator** (zu Fachbereich)
- + **Schnittstelle** Datenschutz/Infosec/IT/User

- ~ **Leitungsfunktionen**/Führungsrollen (Softskills wichtiger als Hardskills)
- ~ **Service Ownership**

- Grenze sind **technische Hardskills** (z.B. Sys Admin, Threat Hunter)
- Infosec / IT **Auditor** (Sicherheit und Detailwissen)
- Tiefes technisches Verständnis um Risikobewertungen / technischen **Evaluierungen hinterfragen zu können** (QS)
- Vorgaben für Informationssicherheitsstandards (Richtlinien Inhalte)

Empfehlungen

1. Versuchen Sie es selbst → Horizont Erweiterung
2. Normalen Einstellungsprozess um „erweitertes Screening“ ausbauen
3. Wenn Skills It. Papier passen → Einladung, Arbeitsweise ansehen
 - a) Kleine Todos aus dem Tagesgeschäft
 - b) Fragen stellen – nur schlechte Antwortoptionen – Diskussion
 - c) Wie ist der Umgang mit neuen Situationen ?
 - d) Wie eignet sich die Person wissen an ?
 - e) Wie ist die Arbeitsweise der Person ?
4. Passt die Person auch persönlich ins Team?