HOSPITALVEREINIGUNG ST. MARIEN GMBH: DER WICHTIGE SCHRITT AUF DEM WEG ZUR ZERTIFIZIERUNG NACH ISO/IEC 27001 UND B3S

AUF EINEN BLICK

Aufgabe
Die Hospitalvereinigung St. Marien GmbH strebt die ISO 27001-Zertifizierung sowie eine Umsetzung der Vorgaben aus B3S Gesundheitswesen an. SVA unterstützt bei der Bestandsaufnahme und der Definition von notwendigen Maßnahmen.

Leistungsumfang
Audit und Reifegrad-Analyse

Vorteile
- Aufnahme des Ist-Zustandes
- Definition von Maßnahmen
- Aufdecken von Risiken und Defiziten
- Konformitäts-Reifegrad zur ISO 27001 und B3S Gesundheitswesen

Die Hospitalvereinigung St. Marien GmbH gehört zur Stiftung der Cellitinnen zur hl. Maria und bündelt unter ihrem Dach vor allem die vielfältigen Krankenhausaktivitäten. Neben den Akutkrankenhäusern gehören zwei Reha-Kliniken und Schulen sowie weitere Einrichtungen (NTC, RTZ, MVZ St. Marien, MVZ Medi-Wtal, Hospiz St. Marien) zum Verbund. Damit deckt die Hospitalvereinigung mit ihren Einrichtungen ein breites medizinisches, pflegerisches und therapeutisches Spektrum ab, das durch seine differenzierten Schwerpunktbildungen die Grund- und Regelversorgung der Menschen in den Regionen Köln und Wuppertal auf hohem Niveau gewährleistet.

ANALYSE ZUM STAND DER INFORMATIONSSICHERHEIT UND REIFEGRAD ZUR ISO 27001 SOWIE B3S

Das erklärte Ziel der Hospitalvereinigung ist es, eine Zertifizierung nach ISO 27001 und B3S für das Gesundheitswesen zu erreichen, um zukünftig den Anforderungen des BSI an kritische Infrastrukturen (KRITIS) zu genügen. Die Absicherung der IT-Infrastruktur, der Schutz von sensiblen Informationen, wie z. B. den Gesundheitsdaten der Patienten, sowie die Sicherstellung der medizinischen Versorgung gehören bei der Hospitalvereinigung zu den wichtigsten Grundanforderungen an den IT-Betrieb.
Der erste Schritt auf dem Weg zur Zertifizierung sollte stets eine kritische Bestandsaufnahme sein. Um den Ist-Zustand der Informationssicherheit zu ermitteln, wurde SVA beauftragt, eine Informationssicherheits-Status-Analyse (ISSA) durchzuführen. Anschließend sollte der Reifegrad zur ISO 27001 ermittelt werden, um festzustellen, in welchen Bereichen bereits eine Konformität besteht und welche Bereiche priorisiert behandelt werden müssen, um die Konformität zu erreichen.

Cellitinnen
Der Mensch in guten Händen

Durch die ISSA und die Reifegrad-Analyse konnte festgestellt werden, dass die Hospitalvereinigung ein gutes Niveau der Informationssicherheit vorweisen kann.

EINE ISSA LIEFERT AUFSCHLUSS ÜBER MÖGLICHE RISIKEN

Die ISO 27001 Norm definiert Anforderungen an ein Informations-Sicherheits-Management-System (ISMS). Die Anforderungen sind vergleichsweise allgemein definiert, damit die Norm in möglichst vielen Bereichen angewendet werden kann.

Der speziell für Krankenhäuser geltende Branchenstandard B3S für das Gesundheitswesen orientiert sich an der ISO 27001. Er enthält aber auch konkrete, von der Deutschen Krankenhausgesellschaft (DKG) entworfene Vorgaben für IT-Infrastrukturen und ist als Umsetzungshilfe für die ISO 27001 gedacht. Um das Niveau der Informationssicherheit bei der Hospitalvereinigung St. Marien GmbH umfassend bewerten zu können, hat das für Governance, Risk & Compliance verantwortliche Team von SVA die Informationssicherheits-Status-Analyse (ISSA) durchgeführt. Bei der ISSA handelt es sich um ein sogenanntes „Friendly Audit“, in dessen Rahmen die SVA-Experten in mehreren Workshops Fragestellungen zu einer Vielzahl von Themengebieten untersuchen. Die Themengebiete sind dabei sowohl technischer als auch organisatorischer Natur. Die Fragen werden im Verlauf der Gespräche dynamisch an den Kunden angepasst. Um einen praxisorientierten Ansatz zu gewährleisten, ist die ISSA nicht nur an der ISO 27001 ausgerichtet, sondern auch am BSI-Grundschutz sowie vielen Best-Practice-Empfehlungen. Dies spielte insbesondere im Hinblick auf B3S eine große Rolle. Zu jedem erkannten Risiko wurde eine Maßnahme für die Hospitalvereinigung definiert, die das Risiko reduzieren kann.

MASSNAHMEN AUS DER ISSA WERDEN FORTLAUFEND GEPRÜFT

Alle bei der ISSA entdeckten Risiken wurden in einen Maßnahmenkatalog überführt, um entsprechende Folgeschritte planen und realisieren zu können. Nachdem erste Maßnahmen erfolgreich umgesetzt worden sind, hat SVA eine Reifegrad-Analyse (Compliance Check) durchgeführt, um den Reifegrad zu den Anforderungen der ISO 27001 zu ermitteln.

DIE HOSPITALVEREINIGUNG WEIST EIN GUTES SICHERHEITSNIVEAU VOR

Durch die ISSA und die Reifegrad-Analyse konnte festgestellt werden, dass die Hospitalvereinigung ein gutes Niveau der Informationssicherheit vorweisen kann. In wenigen Bereichen wurden Defizite ermittelt, welche umgehend in den Maßnahmenkatalog zur weiteren Bearbeitung aufgenommen wurden. Durch die dynamische Anpassung des Maßnahmenkatalogs und die Reifegrad-Analyse kann die Hospitalvereinigung den Fortschritt bei der Entwicklung jederzeit nachvollziehen und in Zukunft einen Prozess etablieren, der eine kontinuierliche Weiterentwicklung der Informationssicherheit sicherstellt.

KONTAKT
SVA System Vertrieb
Alexander GmbH
Borsigstraße 26
65205 Wiesbaden
Tel: +49 6122 536-0
Fax:+49 6122 536-399
mail@sva.de
www.sva.de

Cellitinnen
Der Mensch in guten Händen