Lucerne University of
Applied Sciences and Arts
HOCHSCHULE
LUZERN
Wirtschaft

MAS-IS 19

Modul MM 4.4
Fallstudie Risikomanagement (Anwendung: ISMS)

IWI Institut für Wirtschaftsinformatik

Hans-Peter Königs **Marcus Griesser**

Luzern, Mai 2014

FH Zentralschweiz

Agenda

- Lernziele der Fallstudie
- Ausgangslage zur Fallstudie
- Kurzbeschrieb des Fallstudien-Inhalts
- Erwartete Ergebnisse der Fallstudie
- Aktivitäten und Ablauf der Fallstudie
- Bewertung der Fallstudienresultate
- Rahmenbedingungen und Arbeitsprinzipien

Viel Erfolg !

Lernziele der Fallstudie

- Vertiefung und Anwendung des theoretischen Grundlagenwissens in den Bereichen ISMS und Risikomanagement.

- Umgangs mit prozessorientierten Standards und deren praktischen Anwendung - hier im Besonderen die aktuellen Versionen der Standards ISO/IEC 27001 (ISMS), ISO/IEC 27002, ISO/IEC 27003 und ISO/IEC 27005

- Wie können sich die beiden Themen ISMS und Risikomanagement gegenseitig ergänzen bzw. beeinflussen.

- Aneignen der analytischen und praktischen Fähigkeit ein ISMS auf prozessspezifischer, risikooptimierter Basis des Standards ISO/IEC 27001 in der Praxis einzuführen.

- Vor- und Nachteile bzw. Problemstellungen erkennen, die entsprechende praktische ISMS-Lösungen beinhalten könnten.

Ausgangslage zur Fallstudie

- Ihnen ist die Unternehmung SANAMED bereits bestens bekannt.

- Im Rahmen eines internen Audits wurde u.a. bemängelt, dass …
  - keine Konzeption bez. der Definition und Implementation eines ISMS gefunden werden konnte.
  - für die vorhandenen Sicherheits-Controls keine Dokumentation besteht, welche die im Gesamtkontext massgeblichen Risiko-Überlegungen darlegen würde
  - die Verantwortlichkeiten unklar sind.

- Es ist eine konkreter Vorschlag zur Definition und Implementierung eines ISMS bei der SANAMED ist auszuarbeiten.

Kurzbeschrieb der Fallstudie

- Im Auftrag einer fiktiven Geschäftsleitung auf der Basis der bereits geleisteten SANAMED-Arbeiten und Ihrem Know-how soll ein Vorgehensplan, ein Konzept und ein praktisches Proposal für die Definition und Implementation eines risikoorientierten ISMS erstellt werden.
- Die grundsätzliche Einführung des ISMS ist bereits entschieden. Die Geschäftsleitung entscheidet basierend auf Ihrem Gesamtvorschlag noch über das „Wie“ der Einführung.
- Das Proposal an die Geschäftsleitung mit den wichtigsten relevanten Schritten soll auf den Standard ISO/IEC 27001 abgestützt sein.
- Dabei ist den Anforderungen von ISO/IEC 27001 bezüglich Definition des Scope, sowie den Standard-Klauseln über Risikoanalyse, risikobasierter Massnahmenbestimmung, Management-Involvement, Dokumentation und Überwachung sowie von rechtlichen und wirtschaftlichen Aspekten Rechnung zu tragen.

Erwartete Ergebnisse der Fallstudie - 1

- Erstellung eines Vorgehensplans und eines Einführungskonzepts zur Einführung eines ISMS.
- Berücksichtigung des Risikoansatzes sowie des anschliessenden Betriebs des zu implementierenden ISMS.
- Ausblickes auf einen KVP, um die Qualität des ISMS Prozesses sowie dessen Ergebnisse regelmässig zu verbessern.
- Sukzessive, prozessorientierte Bearbeitung der Fallstudie gemäss der gestellten Aufgaben anhand von nachvollziehbaren, bewertbaren Grundlagendokumenten.
- Berücksichtigung möglicher Einflussfaktoren z.B. Anforderungen aus sozialen, rechtlichen, organisatorischen und technologischen Aspekten.
- Aufzeigen kritischer Trade-offs zwischen Standard und umsetzbarer Realität.

Erwartete Ergebnisse der Fallstudie - 2

- Austausch der Gruppen untereinander zur Erzielung einer möglichst breiten Abdeckung der wichtigsten Geschäfts-prozesse des Spitals innerhalb einer begrenzten Fallstudien-bearbeitungszeit
- Erstellung und Durchführung einer managementgerechten Präsentation, aus der verständlich, überzeugend und nach-vollziehbar das Einführungskonzept mit seinen nachhaltigen Leistungen und betrieblichen Konsequenzen (einschl. der Aufwände und Kosten für die nächsten 3 Jahre) hervorgeht.

→ Details entnehmen Sie der Aufgabenstellung.

Aktivitäten und Ablauf der Fallstudie

Tag 1: 08:05-16:30 Uhr	**Tag 2**	**Tag 3: 08:05-16:30 Uhr**
Einleitung und Hinweise zur Bearbeitung der Fallstudie • **ca. 8:30 Uhr Kick-off der Gruppenarbeiten** Mittagspause nach individueller Einteilung ▪ **Offizieller Meeting Point: 14:30 Uhr** (ab 16:30 Uhr open end für die Gruppen-Teilnehmenden)	**Gruppenarbeiten** • Selbständige Bearbeitung in den Gruppen • Open end Bearbeitung → ab 17:00 Uhr steht die Mensa zur Verfügung	**Gruppenarbeiten** bis 10:45 Uhr Abgabe der Unterlagen an die Dozenten 11-12 Uhr Präs. Gruppe 1* 12-13 Uhr Mittagspause 13-14 Uhr Präs. Gruppe 2* 14-15 Uhr Präs. Gruppe 3* 15-16 Uhr Präs. Gruppe 4* • ab 16:00 Uhr Schlussrunde

* ca. 20 min. Präsentation, max. 30 min. Diskussion, ca. 5-10 min Pause

Räumlichkeiten

Folgende Gruppenräume sind reserviert:

Mittwoch:	**1.10** / 1.07 / 1.27 / 2.05
Donnerstag:	**1.10** / 1.07 / 1.14 /
Freitag:	**1.10** / 1.07 / 1.27 / 2.37

bis 12:00 Uhr

Abendarbeit nach 17:00 Uhr in der Mensa.

Bewertung der Fallstudienresultate

- Die endgültige Bewertung der Ergebnisse erfolgt mit einem kurzen Bewertungsbericht gemäss der bereits bekannten Bewertungsskalen, die bereits bei der früheren Fallstudien-bearbeitung SANAMED angewandt wurde.
- Mitglieder der Gruppe, die während der gesamten Zeit mitge-arbeitet haben, erhalten individuelle und die durch die Gruppe erreichte Punktzahlen gutgeschrieben.
- Maximal erreichbare Punktzahl pro Teilnehmer:

  40 Punkte entsprechend Note 6.0
- Die Bewertung wird in der Regel innerhalb einer Woche nach der Durchführung der Fallstudie vorgenommen. Eine ent-sprechende Nachbesprechung der Lösungen kann separat mit den Dozenten vereinbart werden.

Rahmenbedingungen und Arbeitsprinzipien

- Sie sind gebeten, sich an die hier referenzierten minimalen Bedingungen in der Aufgabenstellung zu halten, und von Ihrer Vernetzung und Ihren Unterlagen Gebrauch zu machen.
- Vor der Fallstudie, müssen Sie sich unbedingt in der Klasse darauf einigen, welche der bereits erarbeiteten Fallstudien-Resultate (wie z.B. die Sicherheitspolitik) verwendet werden.
- Da Sie vom Zeitbudget her unter hohem Druck arbeiten müssen, ist es wichtig, dass Sie Ihr Vorgehen und Ihre Ressourcen anhand der Aufgabenstellung 1 sorgfältig planen. Eine sinnvolle Aufgabenteilung und gute Gruppendynamik sind unverzichtbare Voraussetzungen für guten Erfolg.
- In diesem Zusammenhang ist es auch wichtig, dass Sie die Qualität höher gewichten wie die Quantität.
- Nachvollziehbares wissenschaftliches Arbeiten wird vorausgesetzt.

Wir wünschen Euch nun viel Erfolg und Spass bei der Arbeit – es lohnt sich !