MBA Master Thesis 2011

Messung, Überwachung und Steuerung von Informationssicherheitsmanagement im Kontext von ISO 27001

Ausgangssituation und Fragestellung

Das heutige Geschäftsleben ist höchst volatil und von schnell wechselnden Situationen geprägt. Dies wirkt sich auch auf die Risikolage der Organisationen aus. Im Gegensatz dazu werden Sicherheitsprozesse in Organisationen heutzutage zu häufig noch statisch und ohne präzise Messung und Überwachung ausgeführt. Der Aufbau eines Sicherheitsmanagementprozesses steckt in vielen Unternehmen noch in den Kinderschuhen und ist auch mit Blick auf Compliance Anforderungen dringend voranzutreiben.

Um Sicherheitsvorfälle zu verhindern und ein angemessenes Management operationeller Risiken zu betreiben, setzen viele Organisationen inzwischen auf die Einführung und Nutzung der internationalen Norm ISO/IEC 27001:2005. Diese fordert die Wirksamkeits- und Zielerreichungsprüfung der Sicherheitsziele, der ISMS Prozesse und der ausgewählten Schutzmaßnahmen.

Jedoch wurden in der ISO 27001 keine näheren Angaben zum Vorgehen zur Wirksamkeitsmessung gemacht, und der begleitend erschienene, informative Standard ISO/IEC 27004:2009 ist umstritten. Daher wird im Rahmen dieser Arbeit eine normkonforme Methodik zur Messung, Überwachung und Steuerung von Informationssicherheitsmanagement im Kontext von ISO 27001 entwickelt und evaluiert.

Master Thesis

Die vorliegende Arbeit wird evaluieren, wie der von der ISO propagierte Methodenstandard im Kontext von ISO 27001 die notwendigen Kriterien erfüllt, um den zuvor skizzierten Problemen im Management der Informationssicherheit und den darüber hinaus abgedeckten Security-Themen zu begegnen. Weiterhin wird ein eigenes Modell vorgestellt und untersucht, welches auf Basis eines Strukturkonzeptes etablierte Methoden aus dem Strategischen Management in den Bereich des Sicherheitsmanagements transportiert und dort als Synthese zusammenführt.

Auswirkungen in der Praxis

Die Ergebnisse der Untersuchungen sind, dass die ISO 27004 nicht den gestellten Anforderungen gerecht wird im Gegensatz zum alternativ vorgestellten 4P-Modell. Dieses bürdet jedoch einer implementierenden Organisation noch Aufwände zur Definition der konkreten Metriken auf. Dennoch wird die normkonforme Methodik des 4P-Modell zukünftig das Standardvorgehen der TÜV Rheinland Group für ISO 27001-konformes IS Measurement darstellen.

MBA Master Thesis 2011

Measurement, Monitoring and Steering of Information Security Management in the context of ISO 27001

Background and problem description

Today's business is highly volatile and characterized by rapidly changing situations. This also has an effect on the risk situation of the organizations. In contrast, security processes carried out in organizations today are too often static and without precise measuring and monitoring. The creation of a security management process is in many companies still in its infancy and needs to be greatly improved lastly due to compliance requirements.

In order to prevent security incidents and to conduct an adequate operational risk management, many organizations are now relying on the introduction and use of the international standard ISO/IEC 27001:2005. This standard requires the measurement of effectiveness and achievement of security objectives, ISMS processes and the selected security controls.

But the ISO 27001 does not specify a procedure how to measure effectiveness and the accompanying, informative standard ISO/IEC 27004:2009 is controversial. Therefore, as part of this thesis, a standard-compliant methodology for measuring, monitoring and control of information security management in the context of ISO 27001 is developed and evaluated.

Master Thesis

This study will evaluate how the measurement standard proposed by ISO meets the criteria in order to tackle the previously outlined problems in the management of information security and further covered security topics. Furthermore, a separate model is presented and analyzed, which will transport methods from strategic management according to a structural concept into the field of security management and brings together a synthesis.

Impact on the industry

The results of the tests show that the ISO 27004 will not meet the necessary requirements as opposed to the alternative presented 4P model. However, the latter imposes additional efforts on an implementing organization to define the specific metrics. Nevertheless, in the future the standard-compliant methodology of the 4P model will be the standard approach for ISO 27001-compliant IS Measurement in the TÜV Rheinland Group.