Die Arbeit hat zum Ziel, ein Modell für die Sicherheit von Informationssystemen unter spezifischer Berücksichtigung der IT-Risiken, deren Management und der Möglichkeiten ihrer Beherrschung zu entwickeln. Im Mittelpunkt steht der strategische Umgang mit Risiken der Informationsverarbeitung resultierend aus der Ungewissheit der zukünftigen Entwicklung im Umfeld des Unternehmens. Diese Ungewissheit wird auf Basis des entwickelten Modells auf den Planungsebenen für eine geschäftsübergreifende Unternehmensstrategie untersucht. Diese Untersuchungsebenen sind gleichzeitig die Bewertungsdimensionen für die ex-ante Bewertung der IT-Security.

Risiken der IT-Sicherheit können den Regelbetrieb massiv gefährden. Der Lösungsansatz der IT-Abteilung basiert darauf, bei der Entwicklung und Optimierung ihrer Systeme den störungsfreien Betrieb sicherzustellen. Neben den technisch-organisatorischen Maßnahmen zur Gewährleistung des störungsfreien Betriebs sind auch die Konzepte zum Umgang mit IT-Risiken zwecks Gewährleistung des Regelbetriebs mit größtmöglicher Wertschöpfung bei akzeptablem Risiko von Bedeutung. Entsprechend gehört die Beherrschung von Risiken zu den strategischen Feldern eines Unternehmens und sichert den mittel- und langfristigen Geschäftserfolg. Die Forderung an das IT-Management (zunächst den störungsfreien Betrieb sicherzustellen) st zu erweitern um Potenziale für eine positive Auswirkung auf den Ertrag/Erfolg des Unternehmens.

Ein zentraler interner Erfolgsfaktor ist die organisatorische Abwicklung der Geschäftsprozesse, sie bezieht sich auf die mittels geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens. Die Absicherung der strategischen Nutzenpotenziale soll durch ein adäquates IT-Security-Management erfolgen. Diese wird daran ausgerichtet, worauf geeignete Eskalations- und Risikobewältigungsstrategien sowie ein geeignetes Business Continuity Planning (Notfallplanung/Incident Management) abzielt: auf die Unterstützung/Herstellung der Handlungsbefähigung. Diese Überlegungen führen zu der IT-Security-Sicht auf die Sicherheit eines Systems: Unterstützung der Strategie konformen und IT-Nutzenpotenzial absichernden Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategisch-operativer Handlungsspielräume. Um die strategische Sicht zusammen mit der technisch-organisatorischen Sicht in einem Modell zu verknüpfen, werden Konzepte vor allem des Controllings im Zusammenhang mit der IT-Security als Projekt begleitende Aufgabe bei der Risiko-orientierten Analyse, Bewertung und Ausgestaltung der Sicherheit von Informationssystemen untersucht. Die im Kontext der Gestaltung der organisatorischen Abwicklung der Geschäftsprozesse mit dem Ziel der Unterstützung strategischer Handlungsspielräume relevanten Risiken werden gemanagt, indem das strategische Performance Management auf die strategische Planungs- und

Lenkungsaufgabe bezüglich des IT-Securityprozesses übertragen wird. Die im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen relevanten Risiken werden gemanagt, indem das operative Performance Management auf die operative Planungs- und Lenkungsaufgabe bezüglich des IT-Securityprozesses (abgeleitet aus der Abstimmung der Unternehmensziele und des IT-Securityprozesses aufeinander) übertragen wird. Das entwickelte Risiko-Controlling wird in dieser Arbeit als "strategisch-operatives" Risiko-Controlling bezeichnet; dadurch soll zum Ausdruck gebracht werden, dass die strategische und die operative Sicht eng miteinander verknüpft werden. Bei dem im Weiteren dargestellten strategisch-operativen IT-Security-Management, welches auf dem strategisch-operativen Risiko-Controlling aufsetzt, knüpft der operative Teil an die Phase "Do" des vom strategischen Teil des IT-Security-Managements gesteuerten strategischen IT-Security-Prozesses an, repräsentiert quasi das Operative im Strategischen.