Aleksandra Sowa *Hrsg.*

IT-Prüfung, Sicherheitsaudit und Datenschutzmodell

Neue Ansätze für die IT-Revision

Springer Vieweg

die regelmäßig erscheinenden repräsentativen KPMG-Studien zur Wirtschaftskriminalität und zu e-Crime.

Prof. Dr. Andreas Hartmann lehrt und forscht mit den Schwerpunkten Software-Engineering und IT-Architektur an der Hochschule für Telekommunikation Leipzig. Mit Berufserfahrung als IT-Führungskraft und CIO liegt sein Interesse zudem bei IT-Strategie, IT-Governance und IT-Management. Er engagiert sich seit vielen Jahren für die Modernisierung der IT im öffentlichen Sektor.

Guido Havers ist Senior Manager bei KPMG Deutschland im Bereich Governance & Assurance Services und betreut in dieser Position schwerpunktmäßig Unternehmen im Rahmen der Prüfung und Implementierung von internen Kontroll- und Compliance Management Systemen. Er kann auf eine elfjährige Erfahrung als Wirtschaftsprüfer bei der Prüfung von Jahres- und Konzernabschlüssen nach IFRS und HGB zurückblicken. Neben der Veröffentlichung von Fachbeiträgen zu ausgewählten Governance bezogenen Themen engagiert er sich neben- und außerberuflich in diversen Praxis- und Beraternetzwerken sowie in Arbeitskreisen.

Reiner Kraft ist wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Sichere Informationstechnologie und befasst sich seit fast zwanzig Jahren mit Fragestellungen rund um das Management der Informationssicherheit. Zu seinen Arbeitsschwerpunkten gehören IT-Risikomanagement, die Anwendbarkeit von IT-Sicherheitsstandards in unterschiedlichen Einsatzszenarien und in diesem Zusammenhang insbesondere auch Fragestellungen rund um die Überprüfung und Bewertung des IT-Sicherheitsniveaus einer Institution.

André Kres IBM Executive IT Architect, Chief Architect Cognitive Business Analytics – ist im CIO Bereich für weltweite Analytics Lösungen unter Einbindung Cognitive Computing verantwortlich.

Jens Carsten Laue leitet bei KPMG Deutschland den Bereich Governance & Assurance Services, der Unternehmen dabei unterstützt, Risiken zu identifizieren und die Sicherheit zu geben, richtige Entscheidung für die Zukunft zu treffen. Als Experte für Corporate Governance berät er Unternehmen in allen Fragestellungen rund um Compliance, Risikomanagement, internes Kontrollsystem und interne Revision. Als Wirtschaftsprüfer verfügt Jens C. Laue darüber hinaus über mehr als 15 Jahre Erfahrung in der Prüfung von Einzel- und Konzernabschlüssen nach IFRS, US-GAAP und HGB. Er ist gefragter Redner auf renommierten Fachveranstaltungen und Laudator auf Preisverleihungen wie dem „Corporate Compliance Award“.

Jorge Machado IT Architect – entwickelt Security Konzepte für Unternehmen in den Branchen Bank, Versicherung und Automobil.

Raoul Mayr IBM Executive IT Architect, CTO IBM for Oracle Europe – als Thought Leader stehen neben seiner Arbeit an digitalen Transformationsprojekten im Oracle-Umfeld das Vorantreiben von innovativen Technologien im CAMSS-Umfeld inkl. Cognitive Computing im Mittelpunkt.

Martin W. Murhammer Senior Managing Consultant, Senior Architect – als Thought Leader im Bereich Security Architecture berät, unterstützt und entwickelt Security Konzepte für Unternehmen weltweit.

Martin Rost Unabhängiges Landeszentrum für Datenschutz, Studium der Soziologie. Früh hatte er technische und sozialwissenschaftliche Publikationen zum Internet und deren gesellschaftlichen Auswirkungen. Aktuell ist er Leiter der „Unterarbeitsgruppe Standard-Datenschutzmodell“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

Andreas Schmengler IBM Executive IT Architect und Mitglied der IBM Academy of Technology. Er berät große Unternehmen im technisch-strategischen Bereich mit dem Schwerpunkt neuer Technologien.

Dipl.-Inf. Sebastian Schreiber ist Geschäftsführer der SySS GmbH in Tübingen, die sich hauptsächlich mit der Durchführung von Penetrationstests beschäftigt. Geboren 1972, studierte er Informatik, Physik, Mathematik und BWL an der Universität Tübingen. Von 1996 bis 1998 war er Mitarbeiter bei Hewlett-Packard. Noch während seines Studiums gründete er 1998 die SySS. Seit 2000 tritt Schreiber regelmäßig bei Messen und Kongressen im In- und Ausland als Live-Hacker auf und zeigt anschaulich, wie IT-Netze übernommen, Passwörter geknackt und Daten abgezogen werden können. Er ist gern gesehener IT-Sicherheitsexperte in Printmedien, Rundfunk und Fernsehen. Als langjähriges Mitglied engagiert er sich darüber hinaus im Verband für Sicherheit in der Wirtschaft Baden-Württemberg e.V. oder auch im Beirat der Zeitschrift „Datenschutz und Datensicherheit“.

Dr. Aleksandra Sowa gründete und leitete zusammen mit dem deutschen Kryptologen Hans Dobbertin das Horst Görtz Institut für Sicherheit in der Informationstechnik, ist Autorin diverser Bücher und Fachpublikationen, Dozentin, zertifizierte Datenschutzbeauftragte, Datenschutzauditor und IT-Compliance-Manager. Dr. Sowa ist aktuell für einen Telekommunikationskonzern tätig.

Rolf Stadler IBM Executive IT Architect. Er ist Berater für die Anwendung neuer Cloud- und cognitiver Technologien in strategischen Projekten bei Banken und Versicherungen.

Mechthild Stöwer leitet die Abteilung Security Management am Fraunhofer-Institut für Sichere Informationstechnologie. Sie studierte Volkswirtschaftslehre und Informatik an der Technischen Universität Berlin. In Beratungs- und Entwicklungsprojekten unterstützt

sie Unternehmen, IT-Risiken besser zu verstehen und Sicherheitslösungen im Hinblick auf die Anforderungen der Geschäftsprozesse zu optimieren. Ihr besonderer Fokus liegt auf der Erarbeitung gut nutzbarer Methoden zur quantitativen Analyse von Sicherheitssystemen etwa mit Hilfe von Metriken. Sie ist Dozentin an der Hochschule Bonn-Rhein-Sieg für die Informatikspezialisierung Informationssicherheit.

Prof. Dr.-Ing. Sabine Wieland arbeitet als Professorin seit 2000 an der Hochschule für Telekommunikation Leipzig. Ihre Forschungsinteressen liegen im Bereich Software Engineering, hier besonders die Themen Software Requirement und Software Qualität, im Bereich Cloud Computing, hier besonders die IT Sicherheit für KMU, im Bereich IT-Infrastrukturen für Energieverteilnetze, hier besonders die Realisierung einer sicheren dezentralen IT-Infrastruktur. Für die Lehre setzt sie innovative Lehr- & Lernformen ein, um einen nachhaltigen Wissenstransfer zu ermöglichen. Sie wurde mit dem Titel „Professor des Jahres 2015“ in der Kategorie Ingenieurswissenschaften/Informatik ausgezeichnet.

Dr. Johannes Wiele Managing Security Consultant, berät Organisationen in den Bereichen strategische Informationssicherheit, Security Intelligence, Cognitive Security und Datenschutz und ist Lehrbeauftragter am Institut für Internetsicherheit (if(is)), Westfälische Hochschule, Gelsenkirchen.

Holger Wieprecht IBM Executive IT Architect, berät als CTO einer IBM Enterprise Business Unit Kunden unterschiedlicher Industrien im Umfeld der digitalen Transformation.

Verzeichnis der Beitragsautoren

Torsten Andrecht IBM, Hannover, Deutschland

Daniela Duda rehm Datenschutz GmbH, München, Deutschland

Erlijn van Genuchten SySS GmbH, Tübingen, Deutschland

Alexander Geschonneck KPMG AG, Berlin, Deutschland

Andreas Hartmann HfTL, Leipzig, Deutschland

Guido Havers KPMG AG, Köln, Deutschland

Reiner Kraft Fraunhofer-Institut für Sichere Informationstechnologie, Sankt Augustin, Deutschland

André Kres IBM, Hannover, Deutschland

Jens Carsten Laue KPMG AG, Düsseldorf, Deutschland

Jorge Machado IBM, Hannover, Deutschland

Raoul Mayr IBM, Hannover, Deutschland

Martin W. Murhammer IBM, Wien, Österreich

Martin Rost Unabhängiges Landeszentrum für Datenschutz, Kiel, Deutschland

Andreas Schmengler IBM, Bonn, Deutschland

Sebastian Schreiber SySS GmbH, Tübingen, Deutschland

Aleksandra Sowa Deutsche Telekom AG, Bonn, Deutschland

Rolf Stadler IBM, Zürich, Schweiz

Mechthild Stöwer Fraunhofer-Institut für Sichere Informationstechnologie, Sankt Augustin, Deutschland

Sabine Wieland HfTL, Leipzig, Deutschland

Johannes Wiele IBM, München, Deutschland

Holger Wieprecht IBM, Hannover, Deutschland

Abkürzungsverzeichnis

Abs.	Absatz
AktG	Aktiengesetz
AP-VO	Anlage zur Prüfungsverordnung
AV	Antiviren-Software, Antiviren-Programm (kurz: AV-Software)
B.A.T.M.A.N.	Better Approach To Mobile Adhoc Networking
BDSG	Bundesdatenschutzgesetz
BMBF	Bundesministerium für Bildung und Forschung
BMI	Bundesministerium des Innern
BPMN	Business Process Model and Notation (e.g. BPMN-Diagramm)
BS WP/vBP	Berufssatzung für Wirtschaftsprüfer/vereidigte Buchprüfer
BSI	Bundesamt für Sicherheit in der Informationstechnik
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CR	Change Request
CSMS	Cyber Security Management System
d. h.	das heißt
DDoS	Distributed-Denial-of-Service (e.g. Distributed-Denial-of-Service-Attacke)
DIN	Deutsches Institut für Normung
DNS	Domain Name Server
DoS	Denial-of-Service (e.g. Denial-of-Service-Attacke)
DSBK	Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder
DS-GVO	Europäische Datenschutz-Grundverordnung
DSMS	Datenschutzmanagementsystem
ED NOCLAR	Exposure Draft Responding to Non-Compliance with Laws and Regulations
EU-VO	EU-Verordnung
ff.	fortfolgende
FTP	File Transfer Protocol (Dateiübertragungsprotokoll)
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung