Xpert.press

Die Reihe **Xpert.press** vermittelt Professionals in den Bereichen Softwareentwicklung, Internettechnologie und IT-Management aktuell und kompetent relevantes Fachwissen über Technologien und Produkte zur Entwicklung und Anwendung moderner Informationstechnologien.

Christoph Wegener · Thomas Milde · Wilhelm Dolle

Informationssicherheits-Management

Leitfaden für Praktiker und Begleitbuch zur CISM-Zertifizierung

Springer Vieweg

Christoph Wegener
Gevelsberg, Deutschland

Wilhelm Dolle
Berlin, Deutschland

Thomas Milde
Hamburg, Deutschland

ISSN 1439-5428
Xpert.press
ISBN 978-3-662-49166-9
ISBN 978-3-662-49167-6 (eBook)
DOI 10.1007/978-3-662-49167-6

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg ist Teil von Springer Nature
Die eingetragene Gesellschaft ist Springer-Verlag GmbH Germany
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Für Caroline und Greta
Die besten Dinge im Leben sind nicht die,
die man für Geld bekommt.
(Albert Einstein)

Für Petra, Lesley und Nathalie
Es ist ein lobenswerter Brauch: Wer was Gutes
bekommt, der bedankt sich auch.
(Wilhelm Busch)

Für Claudia, Johanna und Maximilian
Keine Schuld ist dringender als die,
Dank zu sagen.
(Marcus Tullius Cicero)

Geleitwort

Seit dem Jahre 2002 bietet die ISACA, die Information Systems Audit and Control Association, die Zertifizierung zum *Certified Information Security Manager* (*CISM*) an. Daher freue ich mich sehr, dass die Dozenten der CISM-Vorbereitungskurse, die zudem erfahrene Praktiker in diesem Bereich sind, nun ein Werk geschaffen haben, das den Titel „Begleitbuch zur CISM-Zertifizierung" zu Recht trägt. Damit steht erstmals ein Handbuch in deutscher Sprache zur Verfügung, das nicht nur die CISM-Kandidaten, sondern auch die erfolgreichen Absolventen der CISM-Zertifizierung unterstützt: Für die Kandidaten stellt es kurz und prägnant die Inhalte des CISM vor und bietet damit eine exzellente Lernhilfe für das Examen, für die Absolventen des CISM werden anhand von mehreren Praxisbeispielen die Vorgehensweisen im Bereich des Security Management vertieft.

Berlin, im Mai 2016

Karin Thelemann
Vorsitzende des Vorstands, ISACA Germany Chapter

Geleitwort

Die Bedeutung der Informationssicherheit nimmt ständig zu, die Gründe hierfür liegen primär in der stetig fortschreitenden Digitalisierung. Anbieter, aber auch Kunden und Lieferanten müssen den daraus entstehenden Herausforderungen begegnen und bedarfsgerechte Lösungen entwickeln. Dabei ist vor allem das Wissen der Beteiligten ein entscheidender Faktor. Für die Deutsche Telekom AG als einem Anbieter im Bereich der Informationssicherheit ist die Qualifizierung der eigenen Mitarbeiter, wie sicherlich auch für die meisten anderen Unternehmen in diesem Umfeld, seit Jahren selbstverständlich. Der vorliegende Leitfaden ist ein praxisnahes Kompendium, das die Theorie, aber auch die Umsetzung der Informationssicherheit verständlich vermittelt. Es dient sowohl dem Know-how-Erhalt im Selbststudium als auch als Nachschlagewerk für die Vertiefung einzelner Themen.

Bonn, im Mai 2016

Thomas Tschersich
Deutsche Telekom AG, Leiter Group Security Services

Vorwort

Bereits seit dem Jahre 2008 haben wir, die drei Autoren dieses Buches, unter anderem in den CISM-Vorbereitungskursen des ISACA Germany Chapter Erfahrungen im Bereich der Vorbereitung von Teilnehmern für die CISM-Examensprüfung sammeln können. Dabei stellte sich allerdings immer wieder heraus, dass das bereits vorhandene Material für die meist deutschsprachigen Teilnehmer dieser Kurse nicht optimal bzw. nicht ausreichend ist.

Vor diesem Hintergrund wurde der vorliegende Leitfaden aus der Praxis heraus entwickelt. Insbesondere die Notwendigkeit, ein angemessenes Trainingsbuch für die Teilnehmer im deutschen Sprachraum zu haben, das gleichzeitig entsprechend kurz und prägnant die wesentlichen Inhalte für die CISM-Zertifizierung vermittelt, waren die Leitgedanken bei der Erstellung.

Ergänzt wird das Material zur CISM-Vorbereitung durch einen Abschnitt zum Thema BSI IT-Grundschutz und einige Praxisbeispiele, die ausgewählte Facetten des Security Management – vor allem die im deutschsprachigen Raum – im Detail vorstellen. Wir hoffen, dass wir dadurch nicht nur den CISM-Kandidaten vor und nach der Prüfung, sondern auch allen am Thema Security Management Interessierten eine wertvolle Gedankensammlung geben können, die auch aufzeigt, wie vielfältig dieser Bereich in der Praxis tatsächlich ist.

Kein Werk ist wirklich fehlerfrei – daher freuen wir uns über jegliche Rückmeldung zu Fehlern und auch über Anregungen zu zukünftigen Erweiterungen des Buches. Dafür und für die Diskussion zum Inhalt stehen wir Ihnen, verehrte Leser, gerne unter der E-Mail-Adresse autoren@ism-buch.de zur Verfügung.

Gevelsberg, Hamburg und Berlin,
im Oktober 2016

Christoph Wegener
Thomas Milde
Wilhelm Dolle

Danksagung

Die Autoren sind einer Vielzahl von Personen und Institutionen zu Dank verpflichtet, die hier leider nicht alle namentlich erwähnt werden können.

Explizit erwähnen möchten wir aber das Team des Springer-Verlags, insbesondere Dorothea Glaunsinger, die uns in allen Phasen dieses Projekts unterstützt hat, das ISACA Germany Chapter, das uns durch die Trainertätigkeit bei den CISM-Vorbereitungskursen den Ansporn zu diesem Buch gegeben hat, sowie Hanna Lurz für ihre Unterstützung bei der Erstellung und dem Lektorat der Texte.

Dieses Buch basiert auf den Ergebnissen eines Projekts der Bildungsinitiative *Open Competence Center for Cyber Security* (kurz: *Open C³S*), das vom Bundesministerium für Bildung und Forschung unter dem Förderkennzeichen 16OH12026 im Rahmen des Wettbewerbs *Aufstieg durch Bildung: offene Hochschulen* gefördert wurde, der aus BMBF-Mitteln und dem Europäischen Sozialfonds finanziert wird.

Nicht zuletzt bedanken wir uns bei unseren Familien für die großartige Unterstützung, ohne die die Entstehung dieses Buches definitiv nicht möglich gewesen wäre. Besonderer Dank geht hier an Caroline Fichtner und Claudia Schrank für ihre Geduld und ihre Unterstützung bei der Erstellung und dem Lektorat der Texte.

GEFÖRDERT VOM

ISACA Trust in, and value from, information systems Germany Chapter

Bundesministerium für Bildung und Forschung

Open C³S Open Competence Center for Cyber Security

AUFSTIEG DURCH BILDUNG OFFENE HOCHSCHULEN

EUROPÄISCHE UNION

ESF Europäischer Sozialfonds für Deutschland

Abkürzungen

BAAIN	Bundesamt für Ausrüstung, Informationstechnik und Nutzung
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BC	Business Continuity
BCM	Business-Continuity-Management
BDA	Business Dependency Analysis
BIA	Business Impact Analysis
BKA	Bundeskriminalamt
BMI	Bundesministerium des Inneren
BMVg	Bundesministeriums der Verteidigung
BMWi	Bundesministerium für Wirtschaft und Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik
CERT	Computer Emergency Response Team
CISM	Certified Information Security Manager (ISACA)
CISO	Chief Information Security Officer
CIO	Chief Information Officer
CMM	Capability Maturity Model
COBIT	Control Objectives for Information and Related Technology
DDoS	Distributed Denial of Service
DoS	Denial of Service
DMZ	Demilitarized Zone
DR	Disaster Recovery
GHB	Geheimschutzhandbuch, auch: Handbuch für den Geheimschutz in der Wirtschaft
GS	Grundschutz
HIDS	Host Intrusion Detection System
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IRM	Incident-Response-Management
IRT	Incident-Response-Team
IS	Informationssicherheit, auch engl.: *Information Security*

ISACA	Information Systems Audit and Control Association
ISM	Informationssicherheits-Management
ISM	Informationssicherheits-Manager
ISIRM	Information Security Incident Response Management
ISMS	Informationssicherheits-Managementsystem
ISO	International Standardization Organization
IT	Informationstechnologie
IT-GS	IT-Grundschutz
ITGA	Informationstechnische Geheimschutzanweisung
ITIL	IT Infrastructure Library (itSMF)
ITS	IT-Sicherheit
ITSiBe	IT-Sicherheitsbeauftragter
ITSiG	IT-Sicherheitsgesetz
IV	Informationsverbund
KGI	Key Goal Indicator
KPI	Key Performance Indicator
KRI	Key Risk Indicator
MAD	Amt für den Militärischen Abschirmdienst
MTO	Maximum Tolerable Outage
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology (US)
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PDCA	Plan-Do-Check-Act (Deming-Cycle)
PESTELO	Political, Economic, Social, Technological, Environmental, Legal and Organisational
RfP	Request for Proposal
RM	Risikomanagement, auch engl.: *Risk Management*
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RoI	Return on Investment
RoSI	Return on Security Investment
SDLC	Software Development Lifecycle
SLA	Service Level Agreement
SMART	Specific Measurable Accepted Realistic Time Bound
SSE-CMM	Systems Security Engineering Capability Maturity Model
SSLA	Security Service Level Agreement
SWOT	Strengths, Weaknesses, Opportunities and Threats
TCO	Total Cost of Ownership
VPN	Virtual Private Network
VS	Verschlusssache
VSA	Verschlusssachenanweisung

Inhaltsverzeichnis

Die Autoren

Dr. Christoph Wegener (CISA, CISM, CRISC) ist seit 1999 freiberuflich in den Themen IT-Sicherheit, Datenschutz und Open Source aktiv. Zudem ist er – nach mehr als achtjähriger Tätigkeit am Horst Görtz Institut für IT-Sicherheit (HGI) an der Ruhr-Universität Bochum – seit Ende 2012 IT-Leiter der dortigen Fakultät für Elektrotechnik und Informationstechnik. Herr Dr. Wegener ist Mitglied des Beirats der Fachzeitschrift „Datenschutz und Datensicherheit (DuD)“ sowie Gründungs- und Vorstandsmitglied der Arbeitsgruppe Identitätsschutz im Internet (a-i3) und des German Chapters der Cloud Security Alliance (CSA). Neben den Zertifizierungen der ISACA hält Herr Dr. Wegener das „Certificate of Cloud Security Knowledge“ (CCSK) der Cloud Security Alliance und ist zudem von der Gesellschaft für Datenschutz und Datensicherheit (GDD) sowie vom TÜV Nord zertifizierter Datenschutzbeauftragter.

Thomas Milde (CGEIT, CISA, CISM, CRISC) ist als Information Security Officer bei der T-Systems International GmbH tätig und dort für Netze öffentlicher Auftraggeber im Bereich Telecommunication Services & Solutions & TC Portfolio verantwortlich. Im Zeitraum von 2009 bis 2015 verantwortete er die Konzeption, Planung und den Aufbau des integrierten Managementsystems für Informationssicherheit und Business Continuity für die Deutsche Telekom Gruppe nach ISO/IEC 27001 und ISO/IEC 22301. Bis Ende 2008 war er mehrere Jahre weltweit als Audit Manager im IT-Umfeld der Deutschen Telekom AG tätig. Thomas Milde ist Master of Science in Enterprise Information Management (University of Reading (UK)), zertifizierter CIA und hält das „Certificate of the BCI (CBCI)“.

Wilhelm Dolle (CISA, CISM) arbeitet als Partner Cyber Security bei der KPMG AG Wirtschaftsprüfungsgesellschaft und ist zudem Geschäftsführer der KPMG Cert GmbH. Er verfügt über mehr als 20 Jahre Berufserfahrung und ist Experte sowohl für technische als auch organisatorische Aspekte der Informationssicherheit. Dazu gehören etwa Risiko- und Sicherheitsanalysen, der Aufbau von Informationssicherheits-Managementsystemen bis zur Zertifizierungsreife, aber auch Themen wie Penetrationstests und digitale Forensik. Wilhelm Dolle beschäftigt sich ebenfalls intensiv mit regulatorischen Anforderungen an die Informationssicherheit und das IT-Risikomanagement. Er hat einige Studien zum IT-Sicherheitsgesetz und zur Sicherheit in kritischen Infrastrukturen verfasst, ist Autor zahlreicher Artikel in Fachzeitschriften, zertifizierter CISSP und hat Lehraufträge an verschiedenen Hochschulen inne.