MATERNA
Information & Communications

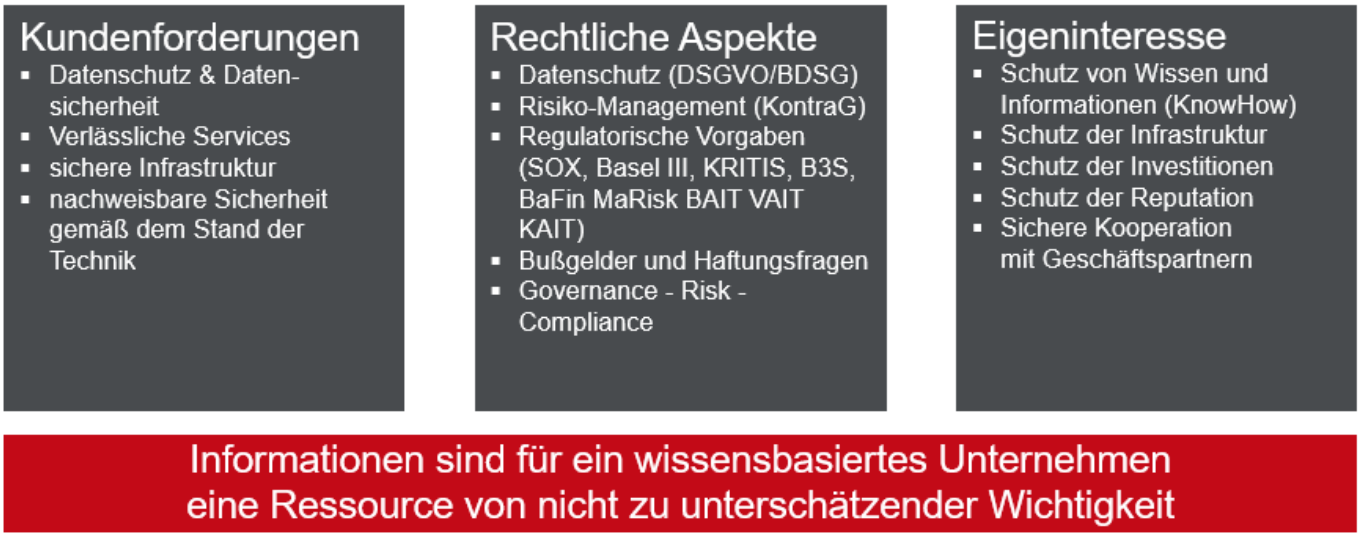
Whitepaper

Information Security Management System

Grundpfeiler der Informationssicherheit

Welche Werte gilt es zu schützen?

In unserer immer stärker vernetzten Gesellschaft nimmt die Bedeutung von Informationen völlig neue Dimensionen an. Die richtigen Informationen zum richtigen Zeitpunkt verfügbar zu haben und zielgerichtet nutzen zu können, wird zum entscheidenden Wettbewerbs- und Erfolgsfaktor. Informationen müssen darum - neben Werkstoffen, Betriebsmitteln und Arbeit – als weitere wichtige Ressource angesehen werden. Konsequenterweise rückt damit aber auch verstärkt der Bedarf an nachhaltigem Schutz dieser Informationen in den Vordergrund.



Kundenanforderungen, rechtliche Vorgaben und Eigeninteressen sind Gründe, die Informationssicherheit zu verbessern

Informationen brauchen Sicherheit, Sicherheit braucht Management

Ob klein, mittel oder groß, ob lokal, regional oder global tätig, Unternehmen aller Branchen, alle Behörden, Anstalten und Organisationen benötigen und verarbeiten Informationen unterschiedlichster Art. Damit stellt sich aber auch die Herausforderung, die Vertraulichkeit, Integrität und Verfügbarkeit dieser Informationen zu bewahren und zu schützen. Treiber hierfür können die Anforderungen und Erwartungen von Kunden und Partnern sein, gesetzliche Vorgaben, regulatorische Auflagen und nicht zuletzt auch das eigene Interesse daran, unangenehme rechtliche Konsequenzen, finanzielle Verluste und Reputationsschäden zu vermeiden. Und hier kommt Informationssicherheit ins Spiel.

Beim Thema Informationssicherheit gilt der altbekannte Spruch: „Wer aufhört, besser zu werden, hat aufgehört, gut zu sein.“. Das gilt nicht zuletzt, weil die Verarbeitung von Informationen und das zugehörige Umfeld ständigen Änderungen unterworfen ist. Es werden neue Informationen benötigt, deren Kritikalität neu eingeschätzt werden muss. Anforderungen und Ansprüche an die Organisation ändern sich, IT unterliegt einem ständigen Wandel, neue Sicherheitslücken und Angriffsvektoren werden bekannt. Mit anderen Worten, Informationssicherheit ist kein einmaliges Projekt („100% Sicherheit erreicht, fertig!“), sondern eine auf Dauer angelegt Aufgabe.

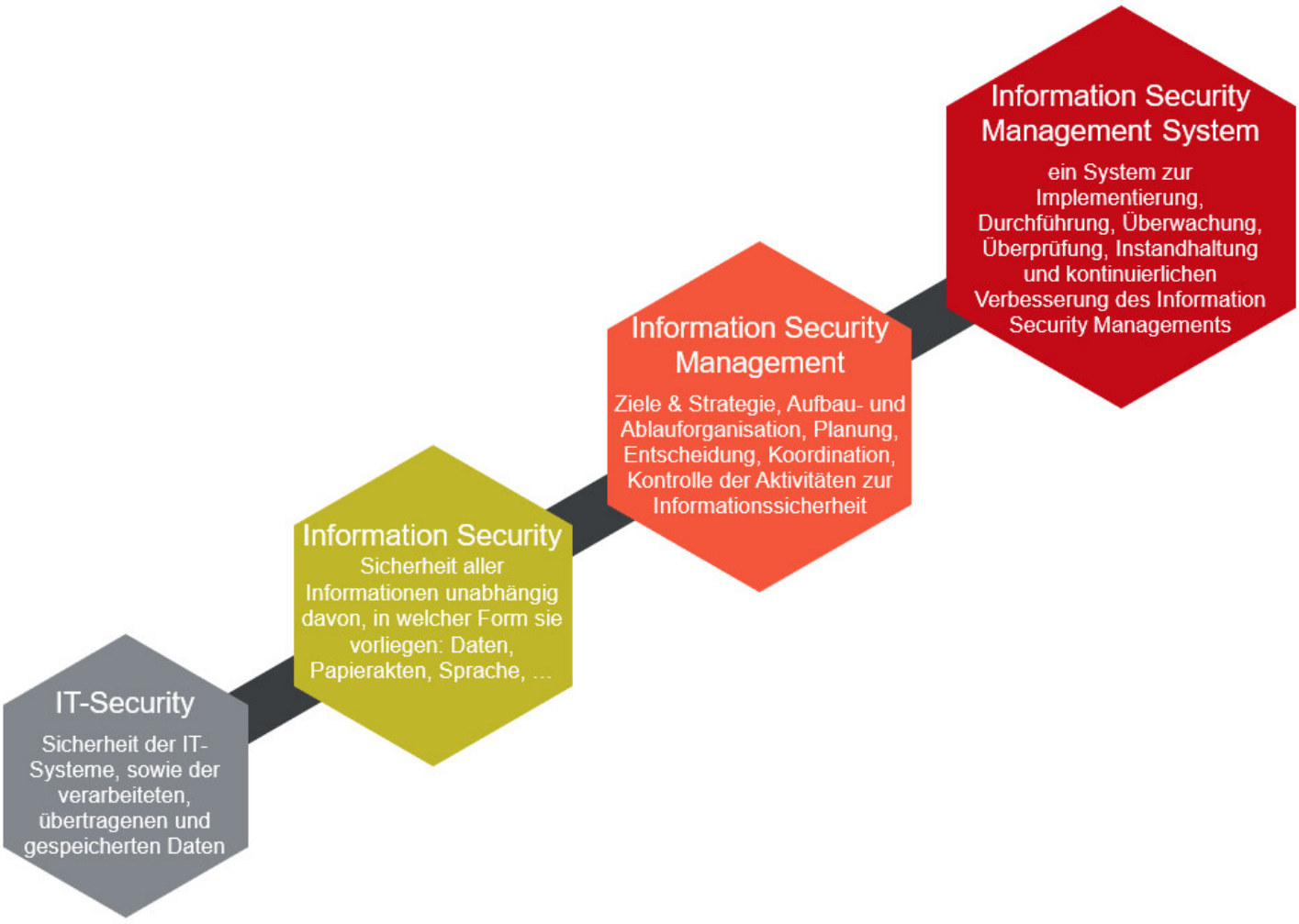
Um sicherzustellen, dass die richtigen Dinge in der richtigen Weise getan werden, benötigt Informationssicherheit Planung, Steuerung und Kontrolle, also „Management“ und das optimalerweise unterstützt durch ein passendes System, also durch ein Informationssicherheitsmanagementsystem (ISMS). Informationssicherheit ist viel zu wichtig, um lediglich kurzfristig auf bekanntgewordene Probleme zu reagieren und ansonsten nur abzuwarten; allzu oft wird dabei dann Panik und Aktionismus das Feld überlassen. Mit Hilfe eines ISMS werden Probleme frühzeitig erkannt und können geplant und geordnet angegangen werden.

Ein ISMS dient dazu, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen auf einem angemessenen Niveau sicherzustellen und sorgt durch das Risikomanagement für eine angemessene Steuerung von Risiken. Dabei hilft ein ISMS die für die Informationssicherheit notwendigen Ressourcen optimal zu planen und effizient zu verwenden.

Die Überwachung der Leistungsfähigkeit eines ISMS und dessen kontinuierliche Verbesserung tragen entscheidend dazu bei, einen einmal erreichten Stand zu sichern und weiter auszubauen.

Ein ISMS trägt durch kontrollierbare und steuerbare Informationssicherheitsprozesse zu einer transparenten, effektiven und effizienten Umsetzung der notwendigen Sicherheitsmaßnahmen bei. Immer mehr Organisationen erkennen daher die Notwendigkeit eines systematischen Vorgehens und bauen ein ISMS auf. Dabei orientieren sie sich wahlweise an der internationalen Normenreihe der ISO/IEC 27001 oder an der IT-Grundschutz-Methodik mit den Standards BSI 200-1, 200-2, 200-3, 100-4 bzw. 200-4 und dem IT-Grundschutz-Kompendium.

Diese Standards beruhen auf Best Practices und werden kontinuierlich weiterentwickelt. Sie beschreiben den Aufbau und Betrieb eines Managementsystems für Informationssicherheit, typische Aspekte der Informationssicherheit, sowie grundlegende Anforderungen für Sicherheitsmaßnahmen. Daher basieren auch viele weitere Standards und Vorgaben auf dem Framework zur Informationssicherheit ISO/IEC 27001; beispielsweise TISAX für den Autovotive-Sektor und der IT-Sicherheitskatalog der Bundesnetzagentur.



Ein Information Security Management System berücksichtigt alle potenziellen Risikofaktoren. Um die Sicherheit des Systems zu gewährleisten, muss es kontinuierlich überprüft und verbessert werden

Wie ist ein ISMS aufgebaut und wie funktioniert es?

Unabhängig davon, nach welcher Norm (ISO 27001) oder welchem Standard (BSI 200-1) ein ISMS aufgebaut wird – die zugrunde liegenden Prinzipien, Rollen und Prozesse sind stets die gleichen. Eine wesentliche Rolle nimmt hierbei das Top-Management ein. Diese oberste Führungsebene ist verantwortlich dafür, dass die Informationssicherheit in der Organisation etabliert und gelebt wird. Sie hat hierbei eine Vorbildfunktion zu erfüllen. Ohne den Rückhalt und die Unterstützung des Managements kann kein ISMS in der Organisation eingeführt und auf Dauer erfolgreich betrieben werden.

Verantwortung bedeutet hierbei auch die Bereitstellung von ausreichenden finanziellen und personellen Ressourcen für den Betrieb und die Aufrechterhaltung des ISMS.

Dokumentiert wird diese Management-Verantwortung in der Informationssicherheitsleitlinie, die vom Top-Management als Aussage und Verpflichtung zugleich bekanntgegeben wird – sie gibt den Rahmen und die generelle Richtung für alle weiteren ISMS-Aktivitäten vor.

Je nach Größe der Gesamtorganisation ist die Rolle eines Beauftragten für Informationssicherheit zu besetzen oder eine Abteilung bzw. Stabsstelle zu errichten, sowie das benötigte Personal bereitzustellen und zu qualifizieren.

Geltungsbereich des ISMS

Für jedes ISMS muss als Erstes ein geeigneter Geltungsbereich definiert und dokumentiert werden. Dieser muss nicht gleich die gesamte Organisation umfassen, sondern kann auf bestimmte Geschäftsprozesse, Organisationseinheiten sowie Standorte eingeschränkt werden und zu einem späteren Zeitpunkt optional auf einen umfassenderen Geltungsbereich ausgeweitet werden.

Regelungen zur Informationssicherheit

Neben der übergeordneten Informationssicherheitsleitlinie gibt es noch weitere spezifische Sicherheitsrichtlinien, die jeweils für einen bestimmtes Thema oder einen bestimmten Bereich gelten (z.B. für den Passwortgebrauch, die Cloud-Nutzung, Zugangskontrolle) und jeweils verbindlich für alle Beteiligten und Mitarbeiter die Regelungen vor geben, die hier zu beachten sind. Die Informationssicherheitsleitlinie wird in weitern Vorgaben konkretisiert, beispielsweise in Informationssicherheitsrichtlinien, Sicherheits- und Notfall-Konzepten, Arbeitsanweisungen, etc.

Dokumente dienen keinesfalls nur formalen Aspekten. Sie stellen sicher, dass Regeln und Festlegungen für alle Beteiligten klar nachvollziehbar sind und erleichtern die Überprüfung, ob bei der Planung und dem Betrieb von IT-Systemen alle wichtigen Sicherheitsmaßnahmen bedacht wurden und Informationen somit tatsächlich ausreichend geschützt sind. Genauso wie IT-Systeme unterliegen auch die Dokumentationen einem Lebenszyklus und müssen regelmäßig gepflegt werden.

Dokumenten-Ebenen eines ISMS

Schutzbedarf und Risiken

Ziel eines ISMS ist es, Risiken zur erkennen und zu behandeln. Dazu muss festgestellt werden, was in welchem Maße für die Organisation wichtig und schützenwert bzw. bedroht ist. Hier hat sich das Mittel der Schutzbedarfsfeststellung bewährt. Dabei wird der Schutzbedarf hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit anhand von Schadenszenarien ermittelt.

Um die Risiken bei der Verarbeitung und Speicherung der Informationen erkennen, beurteilen und behandeln zu können, muss eine geeignete Risikoanalysemethodik festgelegt werden. Die Risikoanalysemethodik kann sich dabei an Normen und Standards orientieren, wie z.B. ISO 31000, ISO 27005, BSI 200-3, sollte aber individuell an die Bedürfnisse der Organisation angepasst werden.

Schutzmaßnahmen

Um die Informationen der Organisation vor Risiken zu schützen, sind personelle, organisatorische und technische Maßnahmen festzulegen und umzusetzen, die einen adäquaten Schutz der Informationen sicherstellen. Dazu sollten die Maßnahmen weder willkürlich noch einfach nach „Schema F" ausgewählt werden. Es ist hilfreich, sich an Best Practices zu orientieren. Auf jeden Fall aber müssen die Maßnahmen durch einen risiko-basierten Ansatz an die Organisation angepasst werden. Je höher das Risiko ist, desto umfangreicher und damit ggf. auch aufwendiger kann die betreffende Maßnahme ausfallen. Die ausgewählten Maßnahmen müssen nach sinnvoller Priorisierung projektmäßig geplant und umgesetzt werden.

Sensibilisierung / Awareness

Schulung und Sensibilisierung aller Beteiligten zum Thema Informationssicherheit ist eine Kernaufgabe des ISMS. So schaffen Organisationen das Bewusstsein, dass Informationssicherheit ein wesentlicher Bestandteil der Aufgabenerfüllung ist.

Erkennung und Behandlung von Sicherheitsvorfällen

Organisationen müssen sicherstellen, dass sie Sicherheitsvorfälle frühzeitig erkennen und rechtzeitig darauf reagieren können. Wie Presseberichten immer wieder zu entnehmen ist, werden schwerwiegende Angriffe meist erst mit großer Verzögerung entdeckt. Für eine Abwehr des Angriffs oder eine Begrenzung des Schadens ist es dann häufig zu spät. Zur frühzeitigen Erkennung ist eine zentrale Protokollierung sicherheitsrelevanter Ereignisse und deren zeitnahe Auswertung unabdingbar. Fortgeschrittene Angriffe (APT) können nur erkannt werden, wenn unterschied-

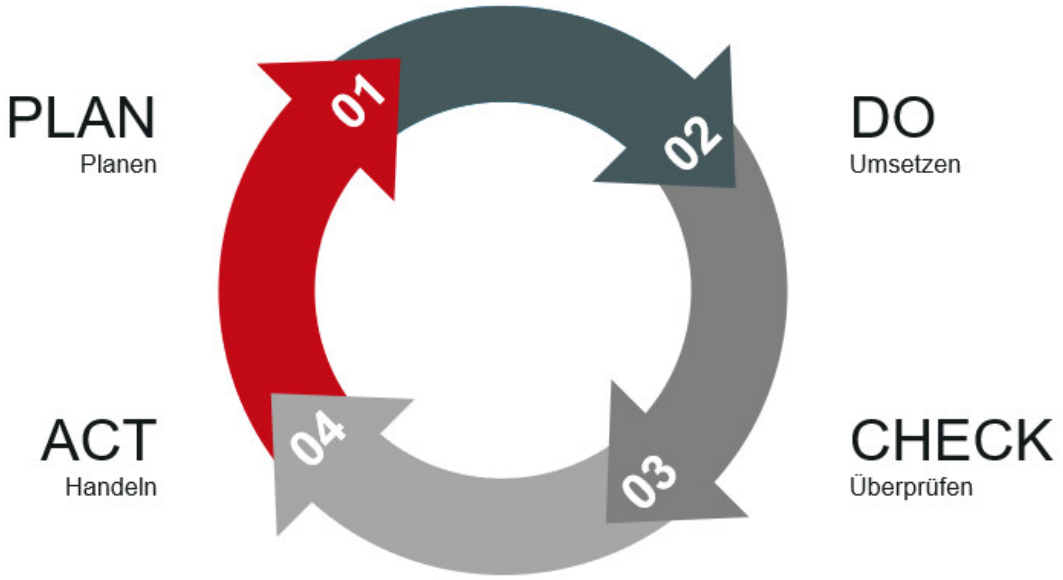
liche, scheinbar unabhängige Ereignisse miteinander korreliert werden. Optimalerweise wird diese Aufgabe durch ein Security Operations Center (SOC) wahrgenommen.

Kontinuierliche Verbesserung

Ein ISMS ist eine auf Dauer angelegt Aufgabe, die Arbeit endet also nicht mit Abschluss der Implementierung.

Weil sich die Sicherheitsanforderungen oder Gefährdungen im Laufe der Zeit ändern können – sei es durch neue Geschäftsfelder oder Änderungen der globalen Bedrohungslage – muss das ISMS im laufenden Betrieb überprüft und verbessert werden. Hierzu dient der kontinuierliche Verbesserungsprozess (KVP), der das Ziel hat, ein nachhaltiges, stabiles und effizientes ISMS zu betreiben, das den Schutz des Wertes „Information" nachhaltig gewährleistet.

Ein KVP nach dem PDCA-Zyklus („Plan·Do·Check·Act") trägt dazu bei, den Reifegrad eines zuvor definierten Sicherheitsniveaus zu festigen und bei Bedarf zu steigern. Der kontinuierliche Verbesserungsprozess hat zum Ziel die Wirksamkeit und Effizienz der Informationssicherheit aufrecht zu erhalten und an veränderte Bedingungen anzupassen. Hierzu werden regelmäßige interne Audits zur Beurteilung des ISMS durchgeführt. Auf Basis der Auditergebnisse und weiteren Berichten führt das Management der Organisation regelmäßig Reviews des ISMS durch und entscheidet über dessen Angemessenheit und Weiterentwicklung.



PDCA-Zyklus (auch als Deming-Kreis u.a. aus der Qualitätssicherung bekannt)

Vorteile eines ISMS

Informationssicherheitsmanagementsysteme dienen dazu IT-Risiken für die Organisation zu identifizieren, zu analysieren und durch entsprechende Maßnahmen beherrschbar zu machen. Durch einen ganzheitlichen Ansatz erzielen die Organisationen dabei entscheidende Vorteile:

- Stärkung des Bewusstseins für Belange der Informationssicherheit bei allen Beteiligten
- Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit
- Unterstützung der Datenschutzaufgaben durch technische und organisatorische Maßnahmen
- Beitrag zur Aufrechterhaltung der Geschäftskontinuität und damit zur Erreichung der Organisationsziele
- Einhaltung der rechtlichen, regulatorischen und vertraglichen Anforderungen zur Informationssicherheit
- Kosteneinsparungen durch Begrenzung und Vermeidung von Sicherheitsvorfällen
- Orientierung durch ein Rahmenwerk mit bewährten Methoden und Vorgehensweisen

Mehr Sicherheit durch Materna Cyber Security

Unsere Informationssicherheitsspezialisten unterstützen Sie in allen Bereichen der Informationssicherheit. Wir bieten keine Lösungen von der Stange, sondern eine für den jeweiligen Kunden maßgeschneiderte und dem Reifegrad angepasste Beratung und Unterstützung.

Die Experten von Materna verfügen über langjährige Erfahrung im Umgang mit Methoden, internationalen Standards und Best Practices. Das Materna-Portfolio umfasst sowohl Beratungsleistungen zu den Verfahren und Methodiken des BSI IT-Grundschutzes, der ISO 27001, TISAX, Aktives Regelungsmanagement 960-1 (bzw. ZDv 54/100), ISIS12, BCM/Notfallmanagement sowie zur Erfüllung regulativer Vorgaben (z.B. DSGVO, KRITIS, B3S, IT-Sicherheitskatalog (BNetzA), MaRisk, BAIT, VAIT, KAIT, Basel III, SOX).

Auch als Partner für die Informationssicherheitsbeauftragten und -verantwortlichen bei Planung, Aufbau, Betrieb, Überprüfung und Weiterentwicklung eines ISMS stehen unsere qualifizierten Experten mit Rat und Tat zur Verfügung. Bei Bedarf unterstützen wir Sie auf Ihrem Weg zur erfolgreichen ISMS-Zertifizierung durch Planung, Vorbereitung und Begleitung des Zertifizierungsprozess.

Unsere Leistungen

- Beratung zur ISO/IEC 27001 und BSI IT-Grundschutz (Methodik, Standards, Anforderungen)
- Beratung, Planung, Aufbau, Betrieb und Optimierung eines Informationssicherheitsmanagementsystems
- Unterstützung bei der Planung und Umsetzung von Sicherheitsmaßnahmen (Sicherheitskonzepte)
- Beratung zu Governance, Risc und Compliance (Erfüllung normativer und regulativer Vorgaben)
- Risiko-Management (Erarbeitung einer Risikomethodik, Durchführung von Risiko- und Schwachstellenanalysen)
- IT-Notfall-Management (Notfallhandbuch, Notfallvorsorge, Notfallbewältigung, Notfallübungen, BCM, BIA)
- Datenschutz (Konzepte, Maßnahmen, Datenschutzaudit, externer Datenschutzbeauftragter)
- Mitarbeitersensibilisierung (Konzeption und Realisierung von Kampagnen und Lernwelten)
- Ganzheitliche Lösungen aus dem Cyber Defence Center (CDC)
- Betrieb eines Security Operation Centers (SOC) für Kunden als Managed Service

MATERNA
Information & Communications

Kontakt
Materna Information & Communications SE
Voßkuhle 37, 44141 Dortmund
Tel.: +49 231 5599-00
E-Mail: marketing@materna.de
www.materna.de

Über Materna

Materna ist ein Familienunternehmen der IT-Branche und realisiert seit fast vier Jahrzehnten sehr erfolgreich IT-Projekte für Kunden im öffentlichen und privaten Sektor. Weltweit arbeiten über 2.500 Mitarbeiter für das Unternehmen. Wir decken das gesamte Leistungsspektrum eines Dienstleisters ab: von der Strategie und Beratung über Implementierung bis zum Betrieb.