



ISMS

Informationssicherheitsmanagementsystem

BLUVIT GmbH

Am alten Rathaus 5a
34253 Lohfelden
+49 (0) 561 94026666
service@bluvit.de
www.bluvit.de

Inhalt

Informationssicherheitsmanagementsystem – Warum sollte ich ein ISMS einführen?.....	3
Die Bedeutung von einem ISMS.....	4
Schutz vor Cyberbedrohungen	4
Einhaltung gesetzlicher Anforderungen und Vertrauensbildung bei Kunden und Partnern.....	5
Vorteile eines ISMS auf einen Blick	6
Kontinuierliche Verbesserung und Wettbewerbsvorteil.....	7
Implementierungskosten und Zertifizierungskosten.....	7
Fazit.....	8
Sie wollen mehr über Themen aus der IT erfahren?.....	9
Über uns.....	10



Informationssicherheitsmanagementsystem – Warum sollte ich ein ISMS einführen?

Unternehmen sind in der heutigen digitalen Zeit abhängiger denn je von einer sicheren und zuverlässigen IT. Mit einem Informationssicherheitsmanagementsystem (ISMS) werden Informationen und Informationswerte im Betrieb geschützt und es werden gesetzliche und branchenspezifische Anforderungen erfüllt.

In diesem Whitepaper erklären wir die Bedeutung von einem ISMS sowie die Vorteile eines ISMS und geben einen Überblick über die zu erwartenden Kosten.



Die Bedeutung von einem ISMS

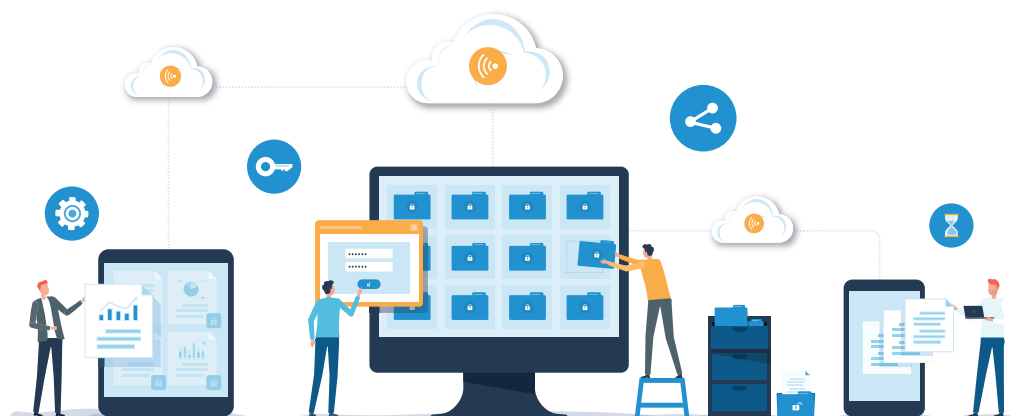
In einem ISMS werden mithilfe von Richtlinien, Abläufen und Maßnahmen die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen strukturiert bewahrt. Ein ISMS kann auf Grundlage verschiedener Regelwerke aufgebaut und zertifiziert werden wie z. B. der BSI-Standard 200-1 bis 200-3 oder die ISO 27001 in der aktuellen Fassung.

In einem ISMS werden Informationen nach ihrem Risiko und der Kritikalität analysiert, bewertet und angemessene Schutzmaßnahmen getroffen. Hierbei werden in einem selbst gewählten Rahmen oder auch Scope die eigene IT, das Personal, Gebäude und physische Sicherheit sowie externe Parteien und ihre Einflüsse berücksichtigt. Dadurch werden Vorfälle reduziert. Zusätzlich werden Pläne und Maßnahmen zur Geschäftsfortführung und dem Wiederanlauf entwickelt und damit Kosten im Schadensfall deutlich minimiert.

In dem festgelegten Scope berücksichtigt ein ISMS sämtliche Vorgänge und Abläufe und die damit verbundenen Informationen und Werte. Dabei unterlaufen diese einem immerwährenden Kreislauf der Optimierung, um den wachsenden Gefahren für die Informationssicherheit standzuhalten.

Schutz vor Cyberbedrohungen

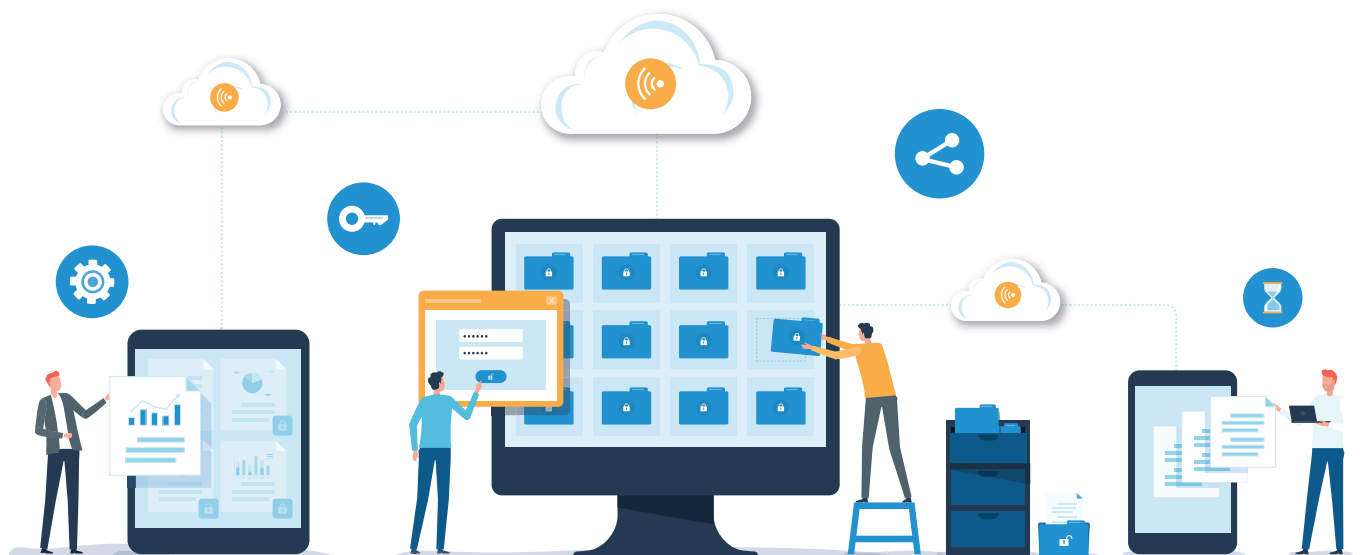
Jedes Unternehmen kann einem Cyberangriff zum Opfer fallen, dabei spielt die Größe, die Branche oder die Bekanntheit selten eine Rolle. Auf Grund der vorangehenden und ständigen Analyse seiner Informationen und Werte und die potenziellen Risiken erhöht man seine eigene Sicherheit zur Abwehr von Cyberbedrohungen. Sicherheitslücken lassen sich schnell identifizieren und schließen.



Einhaltung gesetzlicher Anforderungen und Vertrauensbildung bei Kunden und Partnern

Ein ISMS unterstützt nicht nur die Einhaltung von gesetzlichen Maßnahmen, sondern die Berücksichtigung von gesetzlichen und regulatorischen Anforderungen sind dabei eins der wichtigen Aspekte, die es bei den externen Einflüssen zu berücksichtigen gilt. Gesetze ändern sich in der Regel nicht all zu oft, doch es kommen immer mehr Anforderungen und Ansprüche, speziell im Bereich der Cybersicherheit, dazu. Auch hierauf gilt es zu reagieren.

Die Einhaltung von gesetzlichen Anforderungen wird dadurch gewährleistet und dies schafft Vertrauen bei Kunden und Partnern. Ein zertifiziertes ISMS kann dazu noch für manche gesetzlichen Anforderungen als Nachweis verwendet werden und bei Kunden und Partnern kann das Vertrauen nochmals gestärkt werden.



Vorteile eines ISMS auf einen Blick



Informationssicherheitsrisiken werden identifiziert und es werden Maßnahmen gegen diese entwickelt.



Gesetzliche und regulatorische Anforderungen werden erfüllt. Dadurch werden Strafen bei Verstößen verringert oder verhindert.



Das Vertrauen bei Kunden und Partnern wird gestärkt. Ein ISMS symbolisiert nicht nur Sicherheit, sondern auch kontinuierliche Verbesserung.



Notfallpläne und Wiederherstellungsstrategien tragen zur Verfügbarkeit von Informationen in Krisensituationen bei und stellen die Geschäftskontinuität sicher.



Durch die Reduzierung von Sicherheitsvorfällen und eine sinnvolle Verteilung der Ressourcen können langfristig Kosten eingespart werden.



Kontinuierliche Verbesserung und Wettbewerbsvorteil

Zu einem ISMS gehört die kontinuierliche Überprüfung und Verbesserung, was zu einer fortwährenden Sicherheit der Informationen führt. Dies fördert nicht nur die eigene Sicherheit, sondern sorgt auch dafür, dass man immer auf einem aktuellen Stand der Technik und Maßnahmen bleibt und gewährt dadurch einen Wettbewerbsvorteil. Zudem kann ein zertifiziertes ISMS noch einen zusätzlichen Vorteil bei Auftraggebern sein.

Implementierungskosten und Zertifizierungskosten

Die Kosten für die Implementierung eines ISMS können je nach Unternehmensgröße und Komplexität der IT-Infrastruktur unterschiedlich sein. Zu einer Implementierung gehören eine Analyse des aktuellen Stands, die Beratung zur Verbesserung und Umsetzung und gegebenenfalls Unterstützung sowie ein erstes internes Audit.

Die Kosten für die Zertifizierung nach ISO 27001 sind von der Größe des Unternehmens und dem Umfang des ISMS abhängig. Nach der Zertifizierung entstehen laufende Kosten für die Aufrechterhaltung und kontinuierliche Verbesserung des ISMS, einschließlich regelmäßiger interner und externer Audits. Die täglichen Auditgebühren liegen zwischen ca. 400,00 Euro und 1.250,00 Euro.

Fazit

Ein ISMS ist für Unternehmen unerlässlich, um die Sicherheit ihrer Informationen zu gewährleisten und gesetzliche Anforderungen zu erfüllen. Die Vorteile eines ISMS reichen von Risikomanagement und Vertrauensbildung bei Kunden bis hin zu Wettbewerbsvorteilen und Kosteneinsparungen. Die Investition in ein ISMS sollte als langfristige Investition in die Sicherheit und Zukunftsfähigkeit des Unternehmens betrachtet werden.



Sie haben Interesse an einer individuellen Beratung?

Dann können Sie hier direkt mit unserem Vertrieb sprechen:



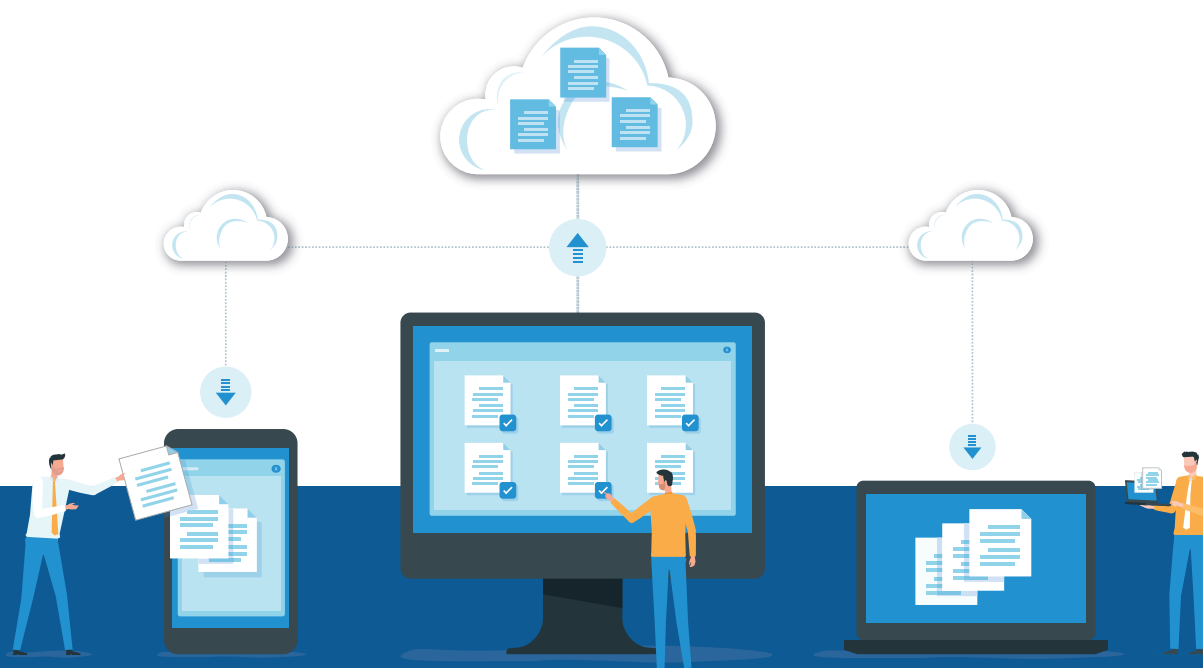
+49 (0) 561 94026666



vertrieb@bluvit.de

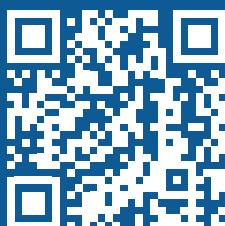
Sie wollen mehr über Themen aus der IT erfahren?

Besuchen Sie unseren Downloadbereich. Dort können Sie sich hier einfach weitere spannende Whitepaper zu den verschiedensten Themen herunterladen.



Jetzt kostenlos downloaden!

Alle Whitepaper, Checklisten und Factsheets auf einen Blick:



www.bluvit.de/downloads

Über uns

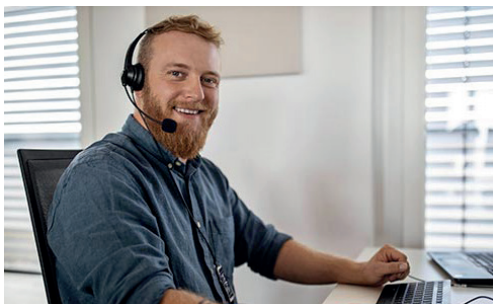


Managed Service

Über 11.500 Kaffees getrunken.

IT-Sicherheit

Über 310 Kunden vertrauen uns.



Telefonie

Über 6000 Supportanfragen
erfolgreich bearbeitet.

Aus der Vision, bezahlbare IT-Dienstleistungen für kleine und mittelständische Unternehmen anbieten zu können, entschloss sich Timm Vollmer die BLUVIT GmbH mit ihrem einzigartigen On-Demand-Modell zu gründen.

Mit einem besonderen Fokus auf IT-Sicherheit, Datenschutz und Informationssicherheit, bieten wir unseren Kunden ein leistungsorientiertes Portfolio aus Dienstleistung und Beratung, mit dem Ziel, die (IT-)Welt für die kleinen und mittelständischen Unternehmen sicherer zu gestalten.

Doch was bedeutet der Name BLUVIT eigentlich?

Die Idee hinter dem Namen BLUVIT war es, ein Akronym zu finden, das nicht nur das Unternehmen beschreibt, sondern auch die Kernidee wiedergibt. Deshalb steht BLUVIT für

Beraten, **L**ösen (und) **U**nterstützen von **IT**-Services.

Doch wer kommt darauf? Wir haben unsere Mitarbeitenden befragt und diese hatten folgende Idee zum Namen:

Blue Team. Das sind die Menschen, die die defensiven Cybersecurity-Aufgaben durchführen, wie z. B. Platzierung und Konfiguration von Firewalls, Durchsetzung von Authentifizierung und vieles mehr.

Least Privilege. Eine Sicherheitsmaßnahme, bei der Benutzern nur die notwendigen Zugriffe gewährt werden, die benötigt werden, damit sie ihre Aufgabe erfüllen können.

User Awareness. All die schönen Sicherheitsmaßnahmen bringen einem Unternehmen nichts, wenn die Benutzer nicht verstehen, wie sie die IT sicher verwenden.

Vulnerability Management. Die Verwaltung und Behebung von Sicherheitslücken in IT-Systemen, damit sich Unternehmen vor den Bedrohungen von Cyberangriffen schützen können.

IT. Diese zwei Buchstaben waren dann für unsere Mitarbeitenden eindeutig, was sie bedeuten sollen.

Wir finden diesen Einfall sehr schön und im Grunde bedeutet BLUVIT auch das, denn es sind Aufgaben und Maßnahmen, die wir für unsere Kunden übernehmen und umsetzen.

BLUVIT GmbH

 Am alten Rathaus 5a
34253 Lohfelden

 +49 (0) 561 94026666

 service@bluvit.de

 www.bluvit.de

