IRM360
Integrated Risk Management Solutions

Absicherung eines ISMS mithilfe von Werkzeugen

Worauf ist bei der Auswahl der Werkzeuge zu achten?

ISO 27001

ISAE 3402

SOC2

White Paper

11. Januar 2022

Ref: White paper 2022-01-11 ISMS Tooling final v1.0.docx

Inhaltsverzeichnis

1. Warum dieses White Paper und für wen ist es gedacht?

Mit diesem White Paper möchten wir Interessierte über die Absicherung des Informationssicherheitsmanagementprozesses, auch bekannt als Informationssicherheitsmanagementsystem (ISMS), informieren. In diesem White Paper werden Themen wie Informationssicherheit, Normen wie ISO 27001 und die Frage, wann ein ISMS notwendig ist, erörtert. Verschiedene Arten von Werkzeugen sowie deren Auswahl werden besprochen.

2. Was ist Informationssicherheit?

Das Konzept der Informationssicherheit kann als Schutz und Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen beschrieben werden. Unter Informationssicherheit versteht man den Schutz von informationsverarbeitenden Einrichtungen wie Servern, Computern und Netzwerken sowie allen darauf gespeicherten Daten. Sie umfasst auch das Risikobewusstsein der Beschäftigten und die Notfallwiederherstellung zur Gewährleistung von Kontinuität nach einem Informationssicherheitsvorfall.

In diesem Zusammenhang sind alle Arten von Informationen gemeint. Dazu gehören das gesprochene Wort, Informationen auf Papier, vertrauliche Informationen, die auf einem Whiteboard geschrieben stehen, gespeicherte und übermittelte Informationen, also auch analoge Informationen. Für ein gutes Sicherheits- und Risikomanagement ist es unabdingbar, zu wissen, welche Informationen und Systeme genutzt werden und welche Abhängigkeiten es zu den Geschäftsprozessen gibt. Wir werden immer

abhängiger von digitalen Informationen und dies ist von entscheidender Bedeutung, denn bei unzureichender Sicherheit läuft ein Unternehmen Gefahr, dass es zu Zwischenfällen und Datenschutzverletzungen oder sogar zum Stillstand kommt.

2.1. Informationssicherheit und Cybersicherheit

In einer zunehmend digitalen Welt verlagert sich der Schwerpunkt von analogen Informationen hin zu digitalen Informationen. Die Cybersicherheit beschäftigt sich hauptsächlich mit digitalen (Cyber-)Informationen und ist daher ein Teil der Informationssicherheit. Cybersicherheit konzentriert sich insbesondere auf die folgenden Bereiche:

1) Malware, Ransomware
2) IoT (Internet der Dinge)
3) digitale Datenschutzverletzungen
4) DDoS-Attacken
5) Hackerangriffe zur Industriespionage oder auf die Lieferkette
6) Phishing (per E-Mail) oder Smishing (per SMS)

Technologie und Risiken ändern sich schnell. Vor 20 Jahren machten wir uns zum ersten Mal Sorgen über ‚Wardriving', als Hacker versuchten, sich über WLAN in das lokale Netzwerk zu hacken. Heute besteht die Gefahr, dass man über IoT-Geräte (Internet der Dinge) gehackt wird, z. B. über eine Kaffeemaschine, die über eine Internetverbindung verfügt.

Wir alle können uns die Bedrohung durch Einbrecher vorstellen und installieren ein gutes Schloss, Kameras und eine Einbruchmeldeanlage oder beauftragen auch einen Sicherheitsdienst. Werden diese Maßnahmen ergriffen, haben sie oft auch präventive Wirkung. Sie verringern die Chance, dass ein Einbruch erfolgreich ist, und erhöhen selbst bei ‚geringen' Maßnahmen die Wahrscheinlichkeit, erwischt zu werden.

Heute sind die Cyberrisiken völlig anders. Wir können die Bedrohung nicht mehr sehen. Die ganze Welt ist mit dem Internet verbunden, sodass die Bedrohung von überallher kommen kann. Daher verlagert sich ein Teil der Kriminalität auf die Cyberkriminalität. Auch wenn diese Bedrohung nicht mehr sichtbar ist, kann sie immer noch ein großes Risiko darstellen. Wenn sich Hacker Zugang zu wichtigen Geschäftsdaten verschaffen, haben sie die Möglichkeit, ein ganzes Unternehmen lahmzulegen oder zu erpressen.

3. Was ist ISO 27001 und was ein ISMS?

ISO 27001 ist die internationale Norm für Informationssicherheit. Sie beschreibt den Prozess des Managements von Informationssicherheitsrisiken, mit anderen Worten: das Informationssicherheitsmanagementsystem (ISMS). Das ISMS ist also kein System oder Werkzeug, sondern beschreibt die Gesamtheit der Aktivitäten zur Umsetzung des Informationssicherheitsmanagements. Diese Aktivitäten können auch als Normanforderungen angesehen werden, die gegenüber einer Prüfstelle nachgewiesen werden müssen, um für eine Zertifizierung nach ISO 27001 zugelassen zu werden.

Diese Anforderungen betreffen u. a. die Informationssicherheitsstrategie, Kontrollen, Risikoanalysen, Maßnahmen, die Überprüfung der Funktion des Prozesses, das Risikobewusstsein der Beschäftigten usw. Außerdem gibt es eine Übersicht über 114 Kontrollmaßnahmen (Anhang A), die umgesetzt werden müssen. Wenn eine Kontrollmaßnahme nicht anwendbar ist, kann sie als ‚nicht anwendbar' markiert werden. Die Maßnahmen sind in der Norm nicht im Detail beschrieben. In der Praxis können Sie Ihre eigenen Maßnahmen oder die Maßnahmen aus dem Leitfaden mit Best-Practice-Ansätzen für ISO 27002 sowie aus anderen Standards wie dem NIST umsetzen.

4. Warum eine Zertifizierung?

Es wird immer häufiger verlangt, dass Lieferanten nach ISO 27001 zertifiziert sind. Die Zertifizierung bietet einen Mehrwert, da sie zeigt, dass das ISMS als Prozess abgesichert ist und das Unternehmen die Informationssicherheit ernst nimmt. Sie zeigt auch, dass die notwendigen Maßnahmen ergriffen wurden, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten, und dass Verbesserungen angestrebt werden.

4.1 Ist das Zertifikat leicht zu erwerben?

Die Absicherung des ISMS und die Zertifizierung sind ein nicht zu unterschätzendes Unterfangen. Es handelt sich nicht um ein einmaliges Projekt, sondern um eine Prozessabsicherung mit jährlichen Aktivitäten. Ein ISMS erfordert auch ein gewisses Ausmaß an Dokumentation. Es wird ein dokumentiertes Managementsystem benötigt, in dem nicht nur IT-bezogene Angelegenheiten beschrieben werden, sondern auch die Durchführung von Risikobewertungen, die Strategie, Verfahren, Richtlinien wie Verhaltenskodizes für Beschäftigte und Aufmerksamkeit für das Risikobewusstsein. Das ISMS behandelt auch Themen wie Leitung, Planung, unterstützende Prozesse, rechtliche Anforderungen, Umsetzung, Überwachung, Messung, Bewertung und Verbesserung als wichtige Anforderungen. Für eine ordnungsgemäße Absicherung des Prozesses ist es ratsam, das erforderliche Wissen im Unternehmen zu gewährleisten. Sollten Sie nicht über dieses Wissen verfügen, empfiehlt sich eine zusätzliche Schulung oder die Beauftragung externer Fachleute.

Wir empfehlen daher, ein ISMS nur dann zu implementieren, wenn Sie sich nach ISO 27001 zertifizieren lassen müssen oder wollen und intern über die erforderlichen Ressourcen und Kenntnisse verfügen oder diese extern

zukaufen. Die Zertifizierungsstellen prüfen, ob die Norm bei der Umsetzung aller vorgenannten Punkte erfüllt ist. Nach Erhalt des Zertifikats wird ein jährliches Kontrollaudit durchgeführt, es handelt sich also nicht um eine einmalige Aktion. Nicht jedes Unternehmen ist reif genug dafür oder verfügt über ausreichende Ressourcen.

Ein ISMS ist keine Garantie dafür, dass Sie nicht von einem Sicherheitsvorfall betroffen sein können. Es verringert jedoch die Wahrscheinlichkeit eines Vorfalls und Sie können im Fall eines Vorfalls richtig handeln.
Kommt es zu einem Vorfall, sind Sie in der Lage, angemessener zu handeln und den Schaden zu verringern. Das erhöht die Cyber-Resilienz Ihres Unternehmens. Aber nicht jedes Unternehmen, das Cyber-Resilienz aufbauen möchte, braucht ein ISMS. Mehr dazu lesen Sie im nächsten Kapitel.

4.2 Brauche ich ein ISMS für unsere Cyber-Resilienz?

Im vorigen Kapitel haben wir festgehalten, dass die Einführung eines ISMS nicht einfach ist. Wenn Ihr Unternehmen über begrenzte Ressourcen verfügt, kann die Implementierung eines ISMS eine Herausforderung darstellen. Darüber hinaus ist die Absicherung eines ISMS nach ISO 27001 mit gewissen administrativen Verpflichtungen verbunden, aber genauso ist die Norm aufgebaut: eine Liste von Standardanforderungen. Darüber hinaus ist die Implementierung und Absicherung eines Prozesses, eines Plan-Do-Check-Act-Zyklus, kein einmaliges Projekt. Denn es gibt jedes Jahr wiederkehrende Aktivitäten. Wenn ein Zertifikat erforderlich ist, hat ein Unternehmen keine andere Wahl, als diese Standardanforderungen zu erfüllen, da es sonst das Zertifikat verliert. Wenn nicht, gibt es andere Möglichkeiten, die Cybersicherheit zu erhöhen.

4.3 Cybersicherheit und die Grenzen von ISO 27001

In Kapitel 3 wurde erläutert, dass ISO 27001 eine Norm für die Zertifizierung des Managementprozesses ist und sich nicht ausdrücklich mit Maßnahmen befasst. Die in Anhang A von ISO 27001 genannten Maßnahmen decken nicht alles ab.

Aus diesen Gründen gibt es auch verschiedene Ergänzungen zur Norm ISO 27001, darunter (wir zählen nicht alle auf, es gibt etwa 35 einschließlich ISO 27001 und ISO 27002):

- ISO/IEC 27017:2015 mit Leitlinien für Cloud-Dienste
- ISO/IEC 27018:2019: konzentriert sich auf den Schutz personenbezogener Daten in der Cloud
- ISO/IEC 27032:2012: Sicherheitsverfahren für Cybersicherheit
- ISO/IEC 27701:2019: Schwerpunkt auf Datenschutzmanagement

Ein Nachteil dieses Konzepts besteht darin, dass diese zusätzlichen Leitlinien meist auf der Tatsache beruhen, dass Sie bereits ein ISMS eingerichtet haben. Wenn Sie kein ISMS implementiert haben, aber nach Cloud- oder Anti-Ransomware-Maßnahmen suchen, ist ein ISMS möglicherweise nicht die richtige Lösung, und es ist besser, aus Standards zu wählen, die direkt auf den jeweiligen Bedarf zugeschnitten sind.

Viele Unternehmen sind derzeit zu Recht besorgt über die zahlreichen Ransomware-Angriffe. Die Absicherung des ISMS oder die Zertifizierung nach ISO 27001 werden dieses Risiko nicht sofort abdecken, aber langfristig verringern.

Die Absicherung eines Risikomanagementprozesses geht schließlich von einer Reihe von Risiken aus, deren Bedeutung durch ‚Wahrscheinlichkeit x

Auswirkung' bestimmt wird. Auf der Grundlage dieser Risikobewertung werden Maßnahmen ergriffen.

Anhand der in Kapitel 2.1 erwähnten Liste von Cyberbedrohungen sollte es möglich sein, eine Reihe von Basismaßnahmen zu ergreifen.
Ein Risiko wird nämlich auf der Grundlage von Wahrscheinlichkeit mal Auswirkung bewertet. Wenn die Basis ausreichend groß ist, wird die Wahrscheinlichkeit geringer und somit sinkt auch das Risiko. Ein Brand in einem Unternehmen kann katastrophale Folgen haben, aber mit einer Basismaßnahme zur Branderkennung und einem Feuerlöschsystem ist die Wahrscheinlichkeit geringer und damit auch das Risiko.

Die ISO-Normen konzentrieren sich auf den Prozess des Risikomanagements. Wenn man den Prozess ordnungsgemäß durchläuft, stößt man automatisch auf Risiken, und um diese Risiken zu verringern, ergreift man Maßnahmen, wobei man die Basismaßnahmen erfüllt. In der Praxis ist dies jedoch oft unabhängig von dem Druck, ein Zertifikat zu erlangen, und der Schwerpunkt liegt manchmal mehr auf ‚Prozess'-Fragen, die in der Norm enthalten sind, z. B. die ordnungsgemäße Beschreibung einer Ursache-Wirkungs-Analyse des Kontexts des Unternehmens und die korrekte sowie rechtzeitige Durchführung einer Managementbewertung. Selten werden die Basismaßnahmen (zuerst) betrachtet. Deshalb gibt es Unternehmen, die zertifiziert sind, aber anschließend gehackt werden, oder Unternehmen, die sich auf den Prozess konzentrieren, aber noch nicht die Basismaßnahmen ergriffen haben.

Derzeit gibt es verschiedene (Cyber-)Sicherheitsstandards, die auch hier zum Einsatz kommen können. Im letzten Kapitel werden wir die Cybersicherheitsaspekte ausführlicher behandeln.

5. Können Werkzeuge helfen?

Wie im vorigen Kapitel beschrieben, umfasst die Absicherung eines ISMS eine Vielzahl von Aktivitäten. ISMS-Tools sollten die Durchführung von Risikobewertungen, die Risikobehandlung, das Verbesserungs-/Aufgabenmanagement, Kontrollen, Audits, Nachweise, die Auditplanung und die Erstellung aller Arten von Zertifizierungsberichten unterstützen.

Fertige Vorlagen helfen bei der Einrichtung eines ISMS und beschleunigen die Umsetzung. Einige Werkzeuge beinhalten ein Managementsystem für Maßnahmen zur Vermeidung von Mehrfachnormen und doppelten Dokumentationen sowie Aktivitäten. Dies ist nützlich, wenn Sie mehrere Standards verwalten müssen. Natürlich können alle Aktivitäten auch z. B. über Tabellenkalkulationen erfasst werden, aber das ist zeitaufwändig und bei mehreren Standards schwierig zu verwalten.

5.1. Arten von Werkzeugen, ISMS vs. GRC vs. IRM

Es gibt verschiedene ISMS-Tools. Aber welches Werkzeug passt am besten zu meinem Unternehmen? In den folgenden Kapiteln wird eine Reihe von ISMS-Tooltypen erläutert. Diese lassen sich grob in 3 Arten einteilen.

5.1.1. ISMS-Tools

Diese sind hauptsächlich auf die Bereitstellung von ISMS-Funktionen ausgerichtet und konzentrieren sich auf eine begrenzte Anzahl von Normen wie ISO 27001. Einige Anbieter bieten auch Datenschutz an. In einigen Fällen sind solche Werkzeuge auf einer bestehenden Anwendung/Plattform

aufgebaut, z. B. SharePoint. Für eine angestrebte Zertifizierung nach ISO 27001 sind sie perfekt geeignet, insbesondere für KMU.

5.1.2 GRC-Tools

GRC konzentriert sich auf einen viel breiteren Bereich als ein ISMS. GRC als Konzept wurde Anfang 2002 aus den USA übernommen, um die Kontrolle und Performance börsennotierter Unternehmen nachweisen zu können. Dies war eine Reaktion auf eine Reihe von Börsenskandalen. GRC ist auf das gesamte Unternehmen ausgerichtet und hat seinen Ursprung in der Enterprise-Umgebung, um das Unternehmen nachweislich ‚unter Kontrolle' zu bringen. GRC-Tools können auch für eine ISMS-Anwendung verwendet werden, aber der Anwendungsbereich von GRC geht weit über die reine Informationssicherheit hinaus. Im Prinzip bedeutet dies, dass sie viele Funktionalitäten bieten, mehr als für ein ISMS erforderlich ist, und sie bringen mehr Komplexität in Bezug auf die Implementierung und Verwaltung mit sich, was sie für KMU oder für ein begrenztes Ziel wie die bloße Erlangung eines ISO 27001-Zertifikats weniger geeignet macht.

5.1.3. IRM-Tools

IRM-Tools sind in der Regel auf ein Managementsystem oder einen Risikobereich ausgerichtet. Aus dem Ansatz des Integrierten Risikomanagements (IRM) heraus bieten sie in der Regel die Möglichkeit, sie für ein (z. B. ein ISMS) oder mehrere Managementsysteme einzusetzen. Dies kann in Phasen erfolgen, sodass die Umsetzung gezielt erfolgen kann. Je größer die Bandbreite der verfügbaren Managementsysteme des IRM-Anbieters ist, desto größer ist die Überschneidung mit GRC.

GRC vs. IRM Solutions – What's the Difference?

Solution Characteristics	GRC	IRM
Architecture	Closed, Proprietary	Open, Integrated
Content	Compliance-driven	Risk-focused
Design	Technical, Control-based	Business-oriented, Process-based
Market Definition	Ubiquitous, meaningless	Targeted, purposeful
Features / Functions	Rigid	Flexible
Buyers / Influencers	Technical practitioners	Business leaders
Use	Internally-driven, departmental	Ecosystem-driven, cross-business unit, partners/suppliers

Gartner

Werkzeuge, die nach dem IRM-Konzept entwickelt wurden, sind weniger komplex aufgebaut, können gezielt eingesetzt werden, bieten Flexibilität/Skalierbarkeit und können in der Regel in relativ kurzer Zeit implementiert werden.
Daher eignen sich ISMS-Lösungen, die auf der IRM-Philosophie basieren, in der Regel für KMU, große Organisationen und Konzerne.

5.2. Worauf ist bei der Auswahl der Werkzeuge zu achten?

Die folgende Liste ist nicht erschöpfend, sondern bietet einen Überblick über die bei der Auswahl zu berücksichtigenden Aspekte. Die Antwort hängt von verschiedenen Faktoren ab, z. B. davon, ob Ihr Unternehmen groß oder klein, einfach oder komplex ist, ob es im Bereich der IT oder der Informationssicherheitsprozesse ausgereift oder unreif ist, ob es Stellen wie jene eines Informationssicherheitsbeauftragten gibt usw.

- Ist nur ein dokumentiertes ISMS ausreichend oder sind auch Funktionen für die korrekte Durchführung von Bewertungen, Risikomanagement, Auditmanagement usw. erforderlich?
- Sollen auch andere Managementsysteme (in Zukunft) unterstützt/integriert werden, z. B. Datenschutzmanagement, Betriebskontinuitätsmanagement, Cybersicherheit und Qualität?
- Sind Sie auf der Suche nach einer GRC-, IRM- oder ISMS-Lösung?

- Sollte das Risikobewusstsein der Beschäftigten Teil der Lösung sein?
- Sind Sie auf der Suche nach einem professionellen Werkzeug für das Informationssicherheitsteam?
- Sollten Kontrolltätigkeiten zusätzlich zu den internen Audits durchgeführt werden?
- Sollten Datenschutzaspekte wie das Management von Datenschutzverletzungen, das Verarbeitungsverzeichnis und die Durchführung von (Vorab-) Datenschutz-Folgenabschätzung integriert werden können?
- Ist eine schnelle Umsetzung aufgrund von Zertifizierungsanforderungen erforderlich?
- Sind Vorlagen wünschenswert, um eine schnelle Umsetzung zu erleichtern?
- Müssen mehrere Normen als nur ISO 27001 berücksichtigt werden?

- Soll ich mich für eine SaaS-Lösung oder eine On-Premise-Lösung entscheiden? Berücksichtigen Sie die folgenden Überlegungen, insbesondere bei SaaS:
  - Sind Sie der Eigentümer der Daten?
  - Gibt es eine SaaS-Vereinbarung, SLA, ist der Anbieter z. B. nach ISO 27001 zertifiziert?
  - Wo befinden sich die Daten? In den Niederlanden, innerhalb des EWR?
  - Entspricht die Lösung dem Modell der vorgesehenen Managementsystemlösung/-norm?
  - Gibt es Verknüpfungsmöglichkeiten, APIs? Gerade bei SaaS-Lösungen sollten diese vorhanden sein!
  - o Besteht die Gefahr eines Lock-in-Effekts? Vorsicht vor maßgeschneiderten Lösungen, diese sind zwar schön, machen aber das Lock-in-Risiko nur größer (siehe auch Kapitel 6.3).

  - o Die Stärke von SaaS liegt in der Investition und Verwaltung der Lösung durch den Anbieter. Dies sollte sich in niedrigen Lizenz- und Wartungskosten niederschlagen.
- Bietet die Software gute Sicherheitsfunktionen wie Verschlüsselung, Zwei-Faktor-Authentifizierung, Single Sign-on-Anwendungen (AD/ADFS)?
- Passen sie zu meinem Unternehmen/meinen Benutzern?
- Wie viele Benutzer sollen damit arbeiten?
- Wie hoch sind die einmaligen und jährlichen Kosten?
- Wie hoch sind die Kosten und die Dauer der Umsetzung?
- Gibt es Unterstützung bei der Umsetzung, möglicherweise über Partner?
- Bietet der Anbieter Schulungsmöglichkeiten an?

6. IRM360 CyberManager

6.1. CyberManager ISMS

Das ISMS-Managementsystem des CyberManagers basiert auf dem IRM-Konzept. Sie können alle Schritte zur Implementierung und Absicherung des ISMS-Prozesses durchführen.

Mit der Plan-Do-Check-Act-Funktionalität können Sie das Management Ihres ISMS-Prozesses umsetzen, nachweisen und zertifizierbar machen:

- ISMS-Dashboard für Informationssicherheit;
- verschiedene Bewertungen, Risikoanalysen und Risikoregister;
- Maßnahmenaufgaben (einschließlich Überprüfungen) und Normenverwaltung;
- Managementbewertung und Erklärung zur Anwendbarkeit;
- Management von Vorfällen;
- Management externer Audits;

- interne Audits, Auditplanung sowie -kontrolle und Verbesserungsaufgaben;
- E-Learning-Module für Risikobewusstsein;
- optionale Schwachstellen-Scans.

Es stehen Maßnahmenvorlagen für KMU, Buchhaltung, Gesundheitswesen, Kommunen und auch verschiedene andere Normenrahmen im Bereich Datenschutz oder Informationssicherheit wie MedMij, WPG, SUWI, COBIT, ISO 27017, ISO 27018, CSA-Star, ISAE-3402, SOC2, CSIR oder z. B. IEC-62443 zur Verfügung.
Kurzanleitungen machen die Einführung eines ISMS noch einfacher. Wenn zusätzliches Knowhow oder zusätzliche Ressourcen benötigt werden, können Implementierungspartner hinzugezogen werden.
Je nach CyberManager-Abonnement können Sie nicht nur ein Informationssicherheitsmanagementsystem (ISMS), sondern auch ein Datenschutz- (DIMS), Cybersicherheits- (CSMS) oder Betriebskontinuitätsmanagementsystem (BCMS) verwalten.

6.2 Umstellung auf CyberManager-ISMS ohne Anbieterbindung

Wie in Kapitel 5.1 erwähnt, gibt es verschiedene Arten von Werkzeugen, die Sie für ein ISMS verwenden können. Häufig wurden Entscheidungen bisher durch den Zustand des Unternehmens zu einem bestimmten Zeitpunkt oder durch die damaligen Möglichkeiten und die Verfügbarkeit bestimmt.
Sind Sie aufgrund der sogenannten Anbieterbindung an ein bestimmtes Tool gebunden? Sind Sie mit erheblichen (finanziellen) Konsequenzen konfrontiert, wenn Sie zu einer anderen Anwendung wechseln?

Dies hängt hauptsächlich von den Möglichkeiten der Anwendung ab, zu der Sie wechseln möchten! Bei Finanzlösungen sehen wir oft, dass es Import-/Migrationswerkzeuge für verschiedene Anwendungen gibt. Die

Verwaltungsseite ist viel weniger flexibel, ein Hauptbuch ist einfach ein Hauptbuch, und das gilt auch für Rechnungen, Journaleinträge usw.

Um Ihnen dennoch eine Möglichkeit zu bieten, haben wir eine Funktion eingebaut, mit der Sie schnell und einfach Design, Existenz und Funktion von Maßnahmen und Managementsystemen übertragen können, z. B. ein funktionierendes ISO 27001-Managementsystem mit Design-, Existenz- und Funktionsbewertungen, Dashboards und relevanten Nachweisen, und mit der Sie einen (bestehenden) Zertifizierungsprozess ohne hohe Kosten aufrechterhalten können.

Möchten Sie mehr über die IRM360-Managementsysteme und den CyberManager erfahren?

Besuchen Sie www.irm360.nl/de und fordern Sie eine Online-Demo an. Wir zeigen es Ihnen gerne!