Bundesamt
für Sicherheit in der
Informationstechnik

Nutzung des branchenspezifischen Sicherheitsstandards Wasser/Abwasser (B3S WA) in Verbundunternehmen

Ausgangssituation – Analyse – Empfehlungen

- Version 1.01

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: kritische.infrastrukturen@bsi.bund.de
Internet: https://www.bsi.bund.de

Änderungshistorie

Version	Datum	Name	Beschreibung
1.0	01.10.2018		
1.01	30.11.2018	BSI	Korrekturen Einleitung

Autoren:

Uwe Marquardt,
Assetmanagement – Technische Koordination,
GELSENWASSER AG, Gelsenkirchen
Obmann DVGW W-GTK-2-8 „IT-Sicherheit“

Dr. Ludger Terhart,
Abteilungsleiter Informationstechnologien,
EMSCHERGENOSSENSCHAFT/LIPPEVERBAND, Essen
Obmann DWA AG WI-5.4 „Cyber-Sicherheit“

Peter Thanisch,
IT Strategie und IT Architektur, Sparte Netz & Infrastruktur,
innogy SE, Essen

Inhaltsverzeichnis

Einleitung 1
1 Ausgangssituation 2
2 Analyse ISMS und B3S 2
3 Empfehlungen 5
4 Fazit 6

Einleitung

Viele Verbundunternehmen der Sektoren Energie und Wasser stehen derzeit vor der Herausforderung, die Vorgaben aus Energiewirtschaftsgesetz (EnWG) und BSI-Gesetz (BSIG) umsetzen zu müssen. Einerseits besteht aus dem EnWG die Verpflichtung den IT-Sicherheitskatalog (ITSiKat) der Bundesnetzagentur (BNetzA) umzusetzen und damit ein Informationssicherheits-Managementsystem (ISMS) auf Grundlage der ISO/IEC 27001 unter Berücksichtigung der ISO/IEC 27019 einzuführen. Andererseits fordert das BSIG den Nachweis über die Einhaltung des Standes der Technik für den KRITIS-Sektor Wasser gegenüber dem BSI, was durch Umsetzung des Branchenspezifischen Sicherheitsstandards Wasser/Abwasser (B3S WA) erfolgen kann.

Es ist grundsätzlich sinnvoll, wenn in den betroffenen Unternehmen ein beide Bereiche umfassendes ISMS etabliert wird, statt für beide Bereiche separate Systeme einzuführen.

Das vorliegende Dokument stellt dar, wie in Verbundunternehmen der B3S WA für die Anlagen der Wasserver- bzw. Abwasserentsorgung effektiv und wirtschaftlich genutzt und in ein bestehendes ISMS auf Grundlage der ISO/IEC 27001 integriert werden kann, so dass sowohl die Vorgaben aus EnWG als auch BSIG erfüllt werden.

1 Ausgangssituation

Energieerzeugungsanlagen und -netze sowie Wasserver- und Abwasserentsorgungsanlagen sind grundsätzlich Kritische Infrastrukturen.

Betreiber von Energienetzen sind nach § 11 (1a) EnWG und den Vorgaben der Bundesnetzagentur (BNetzA) dazu verpflichtet, ein ISMS auf Basis der DIN EN ISO/IEC 27001 einzuführen, sofern sie Systeme betreiben, die gemäß IT-Sicherheitskatalog (IT-SiKat) der BNetzA für einen sicheren Netzbetrieb notwendig sind und für die ein entsprechendes Gefährdungs-potenzial besteht.

Betreibern Kritischer Infrastrukturen gemäß der BSI-Kritisverordnung (BSI-KritisV) im Bereich der Wasserver- und Abwasserentsorgung ermöglicht der B3S WA für die relevanten Anlagen auf angemessene und branchenspezifisch angepasste Weise die Anforderungen des § 8a (2) BSIG nach Einhaltung des „Stands der Technik“ für die relevanten IT-Prozesse und IT-Systeme zu erfüllen. Unabhängig von den aus der BSI-KritisV resultierenden Anforderungen können auch mittlere und kleinere Unternehmen auf Basis des B3S WA den Stand der Technik erreichen.

Betreiber von Energienetzen, die nach den Vorgaben der BNetzA verpflichtet sind, ein ISMS nach DIN EN ISO/IEC 27001 einzuführen, und zusätzlich eine kritische Infrastruktur eines anderen Sektors betreiben (sog. Verbundunternehmen), stehen vor der Herausforderung, die Anforderungen des EnWG und des BSIG an die IT- und Informationssicherheit für die unterschiedlichen Sektoren erfüllen und nachweisen zu müssen.

Es ist daher zu prüfen, ob und wie in diesen Verbundunternehmen der B3S WA für die kritischen Anlagen der Wasserver- bzw. Abwasserentsorgung effizient und wirtschaftlich genutzt und in ein bestehendes ISMS integriert werden kann.

2 Analyse ISMS und B3S

Für viele Verbundunternehmen besteht die Verpflichtung, ein ISMS auf Grundlage der DIN EN ISO/IEC 27001 unter Berücksichtigung der ISO/IEC 27019 bis zum 31.01.2018 einzuführen und durch ein Zertifikat nachzuweisen, wenn sie als Betreiber von Energienetzen IT-Systeme betreiben, die gemäß IT-SiKat für einen sicheren Netzbetrieb notwendig sind und für die ein entsprechendes Gefährdungspotenzial besteht und andererseits die Anforderung des BSIG bezüglich der Einhaltung des Standes der Technik für den KRITIS-Sektor Wasser bis zum 03.05.2018 gegenüber dem BSI nachzuweisen.

Das BSI hat zur Fragestellung, inwiefern ISO/IEC 27001-Zertifikate für Nachweise im Rahmen des § 8a (3) BSIG verwendet werden können, bereits die wichtigsten Punkte herausgearbeitet und veröffentlicht.

In der nachfolgenden Darstellung werden die grundsätzlichen Vorgehensweisen zur Anwendung der DIN EN ISO/IEC 27001 und des B3S WA am Beispiel des Sektors Energie und Wasser gegenübergestellt.

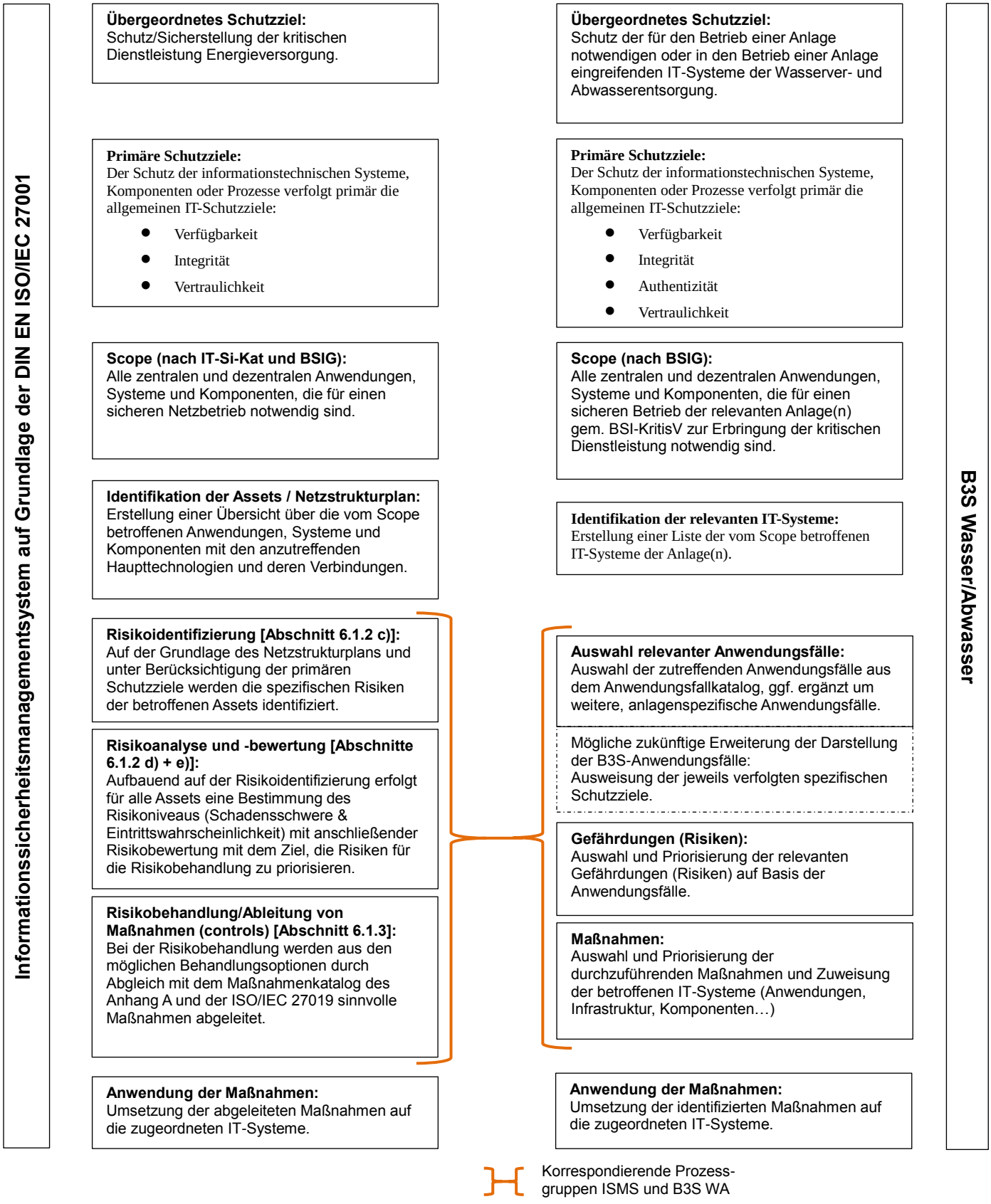

Abb. 1: Vergleich ISMS nach DIN EN ISO/IEC 27001 (am Beispiel des Sektors Energie) und B3S WA

Da der B3S WA vollständig die Methodik des BSI IT-Grundschutzes übernommen hat und letzterer eine mögliche Implementierung der DIN EN ISO/IEC 27001 darstellt, zeigt sich eine grundsätzlich weitgehende Übereinstimmung zwischen beiden Vorgehensweisen.

Allerdings werden im B3S WA insbesondere die Phasen „Risikoidentifizierung, -analyse, -bewertung und -behandlung“ der nativen DIN EN ISO/IEC 27001-Vorgehensweise vereinfacht und zusammengefasst, da diese bereits im Rahmen der Erstellung des BSI IT-Grundschutzes abgearbeitet wurden und damit implizit im B3S WA enthalten sind.

Auch wenn die Vorgehensweise bei der Anwendung beider Regelwerke grundsätzlich gleich ist, so gibt es in Bezug auf die Erfüllung der Anforderungen nach BSIG einige Unterschiede. Während der B3S WA zur Gewährleistung der Anforderungen nach § 8a (1) sowohl im Bereich der technischen wie auch der organisatorischen Vorkehrungen geeignet ist, gilt dieses für die DIN EN ISO/IEC 27001 zunächst nur für den organisatorischen Teil. Die Ableitung technischer Maßnahmen auf Basis der Maßnahmenkataloge des Anhang A der DIN EN ISO/IEC 27001 und der ISO/IEC 27019 muss durch den Betreiber selbst erfolgen.

Sofern ein Verbundunternehmen bereits ein ISMS zur Erfüllung der Anforderungen des EnWG §11 eingeführt hat oder sich in der Umsetzung befindet und nunmehr dieses auf die Kritische(n) Infrastruktur(en) aus dem Bereich Wasserver- bzw. Abwasserentsorgung erweitern möchte, stellt sich die Frage, inwieweit die Anwendung des B3S WA möglich und/oder sinnvoll ist.

Ein wesentlicher Vorteil der Umsetzung des B3S WA liegt darin, dass die Maßnahmen zum Erreichen des Stands der Technik bereits definiert sind und es keinen Zweifel daran gibt, was „Stand der Technik“ ist. Diese Vorgehensweise des B3S WA lässt sich aber nicht ohne weiteres auf die übrigen Sektoren des Verbundunternehmens übertragen. Folgt ein Verbundunternehmen der Methode der DIN EN ISO/IEC 27001, kann es sein, dass die selbst abgeleiteten Maßnahmen nicht mit den vom B3S WA vorgeschlagenen Maßnahmen übereinstimmen, da sich gleiche Sicherheitsziele unter Umständen mit unterschiedlichen Maßnahmen erreichen lassen. Ein Abgleich rein auf der Maßnahmenebene ist insofern nur bedingt möglich.

Der Nachweis des Erreichens des „Stands der Technik“ kann aber über einen Abgleich auf Ebene der Sicherheitsziele erfolgen. Sind alle Schutzziele des B3S WA im ISMS berücksichtigt und erreicht, kann davon ausgegangen werden, dass die Maßnahmen ausreichend sind, um den Stand der Technik zu erreichen und die Anforderungen des BSIG zu erfüllen.

Derzeit werden allerdings im B3S WA die Schutzziele nicht explizit ausgewiesen, da sie bereits bei Erstellung des IT-Grundschutzes berücksichtigt wurden. Grundsätzlich erscheint es möglich, zukünftig die Schutzziele auch im B3S WA anzuführen, so dass ein Abgleich auf Ebene der Schutzziele möglich wäre. In welcher Weise die Schutzziele im B3S WA ausgewiesen werden können, wird durch die gemeinsame Arbeitsgruppe von DVGW und DWA geklärt und in die nächste Fassung des B3S WA aufgenommen werden.

Durch die in der DIN EN ISO/IEC 27001 geforderte Anwendbarkeitserklärung (SOA – Statement of Applicabillity) – vgl. DIN EN ISO/IEC 27001, Kapitel 6.1.3.d – können spartenbezogen Verweise auf die ISO/IEC 27019:2017 (vgl. BNetzA Konformitätsbewertungsprogramm – Nov. 2017, Kapitel 6) für die Sparten nach §11 1a EnWG und für die Sparte(n) Wasser/Abwasser auf die Maßnahmen nach B3S WA aufgenommen werden.

Da die Anwendbarkeitserklärung der Kapitelstruktur der DIN EN ISO/IEC 27001 selbst folgt, sollten für die Sparte(n) Wasser/Abwasser zu den Punkten

- Abschnitt 6.1.2 c,
- Abschnitt 6.1.2 d
- Abschnitt 6.1.2 e

auf die vergleichbaren Abschnitte des B3S WA gemäß Abb. 1 verwiesen werden

3 Empfehlungen

Für die unterschiedlichen Fallkonzepte lassen sich in Bezug auf die Anwendung des B3S WA in Verbundunternehmen folgende Empfehlungen geben:

1. Unternehmen, das ausschließlich im Sektor Wasser eine Kritische Infrastruktur betreibt und nicht zur Umsetzung eines ISMS nach DIN EN ISO/IEC 27001 verpflichtet ist:

   Empfehlung: Es empfiehlt sich die Verwendung des B3S WA, da hierdurch einerseits das Erreichen des Stands der Technik und andererseits der entsprechende Nachweis gegenüber dem BSI für die Kritische(n) Infrastruktur(en) im Sektor Wasser gesichert ist.

   Bei Anwendung des B3S WA prüft das Unternehmen zunächst, inwieweit die relevanten Maßnahmen aus dem IT-Sicherheitsleitfaden bereits durch vorhandene Maßnahmen abgedeckt werden. In diesen Fällen reicht ein entsprechender Verweis in der spezifischen Maßnahmenliste des B3S WA auf die bestehenden Maßnahmen des Unternehmens. Nachfolgend müssen dann nur noch die Maßnahmen behandelt werden, die noch nicht abgedeckt sind.

2. Verbundunternehmen, das neben dem Sektor Wasser verpflichtet ist (z. B. nach § 11 (1a) EnWG) ein ISMS auf Basis der DIN EN ISO/IEC 27001 einzuführen:

   a. Aufgrund der Anforderungen aus dem (den) anderen Sektor(en) wurde bereits ein ISMS nach DIN EN ISO/IEC 27001 für alle Sparten eingeführt bzw. befindet sich in der Einführung:

      Empfehlung: In diesem Fall kann davon ausgegangen werden, dass die beschriebenen Maßnahmen im Rahmen des ISMS grundsätzlich auch die Anforderungen für den Sektor Wasser erfüllen. Dabei ist es ausreichend, wenn das Erreichen der Schutzziele nachgewiesen wird, also alle Schutzziele in Bezug auf die Kritischen Infrastrukturen im Sektor Wasser auch im vorhandenen ISMS berücksichtigt werden.

      In diesem Fall kann das Nachweisverfahren des B3S WA nicht genutzt werden, sondern das Erreichen des Stands der Technik ist vom Unternehmen individuell gegenüber den Auditoren und dem BSI nachzuweisen.

   b. Aufgrund der Anforderungen aus dem (den) anderen Sektor(en) wurde bereits ein ISMS auf Basis der DIN EN ISO/IEC 27001 eingeführt bzw. befindet sich in der Einführung, in das der B3S WA integriert werden soll:

      Empfehlung: In diesem Fall gibt das ISMS gemäß DIN EN ISO/IEC 27001 den organisatorischen Rahmen vor, das Vorgehen in den Phasen „Risikoidentifizierung, -analyse, -bewertung und -behandlung" wird ergänzt durch die Vorgehensweise des B3S WA. Damit ist auch das Nachweisverfahren des B3S WA gegenüber dem BSI nutzbar.

Dieser Nachweis sollte durch sorgfältige Erstellung der Anwendbarkeitserklärung des ISMS gemäß DIN EN ISO/IEC 27001 und Zuordnung der konkreten Maßnahmen des B3S WA für die Sparte Wasser/Abwasser erreicht werden. Wenn darüber hinaus ausgeführt wird (z. B. mittels Erläuterung zur Anwendbarkeitserklärung), aus welchem Grund Maßnahmen des B3S WA nicht umgesetzt wurden (z. B. aufgrund anderer Maßnahmen mit vergleichbarem Schutzniveau), sollte die erfolgreiche Integration der Maßnahmen des B3S WA in den organisatorischen Überbau der DIN EN ISO/IEC 27001 belastbar (gegenüber dem BSI/ISMS Auditor) erfolgt sein.

c. Aufgrund der Anforderungen aus dem (den) anderen Sektor(en) wurde bereits ein ISMS auf Basis der DIN EN ISO/IEC 27001 ausschließlich für den (die) anderen Sektor(en) eingeführt, der B3S WA wird unabhängig davon umgesetzt:

   Empfehlung: Diese mögliche Vorgehensweise wird nicht empfohlen, da der B3S WA grundsätzlich die Einführung eines ISMS empfiehlt. Sofern ein ISMS bereits vorhanden ist oder sich in Einführung befindet, sollten die aufgebauten Strukturen auch für den Bereich Trinkwasserver- bzw. Abwasserentsorgung genutzt werden.

d. Aufgrund der Anforderungen aus dem (den) anderen Sektor(en) wurde bereits ein ISMS nach BSI IT-Grundschutz eingeführt und auf Basis der DIN EN ISO/IEC 27001 zertifiziert

   Empfehlung: Die Einführung eines ISMS nach BSI IT-Grundschutz ist bei entsprechendem Scope dazu geeignet, die Anforderungen des EnWG und des BSIG umzusetzen. Aufgrund der gleichen Systematik kann der B3S WA ohne weiteres in die Vorgehensweise integriert werden. Die Maßnahmen des B3S WA müssen angewandt werden, um den Stand der Technik der Sparte Wasser zu erreichen.
   Um weitere Sektoren abzudecken kann der Sicherheitsleitfaden um entsprechende Anwendungsfälle ergänzt werden. Dabei spielt es keine Rolle, ob diese aus dem Sektor Wasser oder anderen Sektoren kommen. Es wird empfohlen, den B3S WA für den Sektor Wasser anzuwenden und die Vorgaben des B3S WA für den (die) anderen Sektor(en) als „Muster“ zu verwenden, ggf. weitere Anwendungsfälle zu beschreiben.

4 Fazit

Der B3S WA schließt ausdrücklich die Einführung eines ISMS – z. B. nach DIN EN ISO/IEC 27001 – mit ein.

Die Integration des B3S WA in ein bestehendes ISMS nach DIN EN ISO/IEC 27001 eines Verbundunternehmens, welches unterschiedliche medienspezifische Anforderungen (u. a. aus dem EnWG und dem BSIG) zu erfüllen hat, ist unter Berücksichtigung bestimmter Randbedingungen möglich. Die Integration erfolgt dabei im Wesentlichen im Bereich der Phasen „Risiko-identifizierung, -analyse, -bewertung und -behandlung" der DIN EN ISO/IEC 27001 und wird maßgeblich durch eine entsprechend gestaltete Anwendbarkeitserklärung nach DIN EN ISO/IEC 27001, Abschnitt 6.1.3.d gesteuert.

Der B3S WA eignet sich darüber hinaus auch als Grundlage zur Erarbeitung von Maßnahmenkatalogen für Kritische Infrastrukturen anderer Sektoren.