Präqualifizierung Informationssicherheit OT

RWE Generation SE
RWE Platz 3
45141 Essen
Germany
www.rwe.com

RWE Power AG
RWE Platz 2
45141 Essen
Germany
www.rwe.com

RWE Generation NL
Amerweg 1
4931 NC Geertruidenberg
Netherlands

RWE Generation UK
Windmill Hill Business Park
Whitehill Way
SN5 6PB Swindon
United Kingdom

RWE

Präqualifizierung Informationssicherheit OT

1 Einleitung

RWE ist als Betreiber kritischer Infrastrukturen (KRITIS/SEWD) dazu verpflichtet, gesetzliche und innerbetriebliche Anforderungen zur Informationssicherheit der

- OT-Infrastruktur (Operational Technology),
- Prozessteuerungssysteme,
- Anlagentechnik, sowie
- Informationswerte

umzusetzen, um die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit zu gewährleisten.

Operational Technology (OT) bezeichnet in diesem Zusammenhang die Unterstützung technischer Prozesse und die Prozessautomatisierung. Dies beinhaltet insbesondere Anwendungen, Systeme und Komponenten zur Steuerung, Überwachung und Optimierung von Anlagen, die den Produktionsprozessen (wie z. B. Energieerzeugung) zugehörig sind.

Aus diesem Grund muss RWE bestimmte Anforderungen der Informationssicherheit auch innerhalb der Lieferkette sowie der Dienstleistungsverhältnisse sicherstellen, die diese Anlagen, Systeme und Komponenten betreffen.

Alle Lieferanten und Dienstleister müssen innerhalb ihrer eigenen Organisation ein Mindestmaß an Informationssicherheit bei der Erbringung von Dienstleistungen erfüllen.

Diese Präqualifizierung Informationssicherheit OT (PIO) ist ein Bestandteil der Verfahren, welche ein angemessenes Informationssicherheitsniveau in von RWE betriebenen OT-Infrastrukturen sicherstellen. Sie ist von allen Auftragnehmern auszufüllen, die relevante Leistungen erbringen.

Dieser Fragebogen dient daher als Selbstauskunft für alle Lieferanten und Dienstleister der RWE-Gesellschaften zur Einschätzung des aktuellen Informationssicherheitsniveaus Ihrer Organisation und der Systeme Ihrer Organisation, die für die Leistungserfüllung erforderlich sind.

Ziel dieser Präqualifizierung ist es **nicht**, das Sicherheitsniveau der zu liefernden Anlagen, Systeme und Komponenten zu evaluieren.

Bitte beantworten Sie die PIO möglichst detailliert, vollständig und ausschließlich wahrheitsgemäß.

2 Allgemeine Angaben

Angaben zum Unternehmen	
Name:	
Telefon:	
E-Mail:	
Anschrift:	

Es ist ein zentraler Ansprechpartner zu benennen, der verbindliche Auskünfte zur Informationssicherheit – sowohl im internen Bereich als auch im Außenverhältnis zum Auftraggeber – geben kann. Für den Fall der Abwesenheit ist eine Vertretung vorzusehen.

Kontaktdaten des zentralen Ansprechpartners Informationssicherheit	
Name:	
Telefon:	
E-Mail:	

Optional: Kontaktdaten des Vertreters	
Name:	
Telefon:	
E-Mail:	

3 Liefer- und Leistungsumfang

Damit diese Selbstauskunft der Informationssicherheit angemessen beantwortet werden kann, kreuzen Sie in der folgenden Tabelle alle relevanten Liefer- und Leistungsumfänge an und füllen Sie anschließend die nachfolgenden PIO-Kapitel aus.

Der Auftragnehmer erbringt Dienstleistungen in folgenden Bereichen:

3.1 Liefer- und Leistungsumfang

- ☐ Leit- / Automatisierungs- / Fernwirktechnik
- ☐ Mess-, Steuerungs- & Regelungstechnik (vernetzt)
- ☐ Prozessdatenverarbeitung / Prozessdatennetz / Expertensysteme
- ☐ Schaltanlagen Leit- / Sekundär- / Schutztechnik (vernetzt)
- ☐ Brandmelde-, Feuerlösch- / Gefahrenmeldeanlagen
- ☐ Softwareentwicklung
- ☐ Cloud (IaaS/PaaS/SaaS)
- ☐ Beratung / Projektmanagement / Projektunterstützung
- ☐ Penetrationstests / simulierte Angriffe in OT-Systemen

3.2 Bitte beschreiben Sie detailliert den zu erbringenden Leistungsumfang:

3.3 Für die Leistungserbringung ist ein Zugriff auf OT-Systeme erforderlich durch:

- ☐ Remote-Zugriff
- ☐ Vor-Ort-Einsatz
- ☐ Kein Zugriff auf OT-Systeme erforderlich

RWE

4 Zertifizierungen und Sicherheitsrichtlinien

Zertifizierungen und unabhängige Nachweise

4.1 Ist Ihre Organisation für den Liefer- und Leistungsumfang nachweislich von einem unabhängigen Dritten für den Betrieb eines Informationssicherheitsmanagementsystem (ISMS) zertifiziert? ☐ Ja ☐ Nein

4.2 Wenn ja: welche folgenden Zertifizierung(en)/Nachweis(e) können vorgelegt werden? (Mehrfachauswahl möglich)

☐ ISO/IEC 27001 Datum des Zertifikats:

☐ IT-Grundschutz (BSI) Datum des Zertifikats:

☐ Sonstige (z. B. TISAX, CSA STAR) Datum des Zertifikats:

Beschreibung:

4.3 Wenn ja: deckt der Geltungsbereich der Zertifizierung den zu erbringenden Liefer- und Leistungsumfang ab? ☐ Ja ☐ Nein

Bitte fügen Sie die angegebene(n) Zertifizierung(en) / Nachweis(e) bei, inkl. Geltungsbereich (Scope) und Erklärung zur Anwendbarkeit (SoA)

! Sollten Sie eine gängige und gültige Zertifizierung / unabhängigen Nachweis beigelegt haben, sind die folgenden Fragen 4.4 bis 4.10 obsolet und müssen nicht beantwortet bzw. angekreuzt werden.

Regelungen zur Informationssicherheit

4.4 Ist ein Mitglied der Geschäftsleitung Ihres Unternehmens für die Entwicklung, Pflege und Herausgabe einer Informations- und Cybersicherheitsrichtlinie verantwortlich? ☐ Ja ☐ Nein

4.5 Verfügt Ihr Unternehmen über eine dokumentierte Richtlinie zur Informationssicherheit? ☐ Ja ☐ Nein

RWE

4.6	Wählen Sie die Sicherheitsbereiche aus, die in Ihren Richtlinien und Vorgaben zur Informationssicherheit behandelt werden:		
a)	Zulässige Nutzung	☐ Ja	☐ Nein
b)	Datenschutz	☐ Ja	☐ Nein
c)	Fernzugriff /Kabellose Verbindungen	☐ Ja	☐ Nein
d)	Zugriffskontrolle	☐ Ja	☐ Nein
e)	Reaktion auf Informationssicherheitsvorfälle	☐ Ja	☐ Nein
f)	Verschlüsselungsstandards	☐ Ja	☐ Nein
g)	Daten- / Systemklassifizierung	☐ Ja	☐ Nein
h)	Antivirus	☐ Ja	☐ Nein
i)	Verbindungen für Drittanbieter	☐ Ja	☐ Nein
j)	Email / Instant Messaging	☐ Ja	☐ Nein
k)	Physische Sicherheit	☐ Ja	☐ Nein
l)	Personalsicherheit	☐ Ja	☐ Nein
m)	Netzwerk- / Perimetersicherheit	☐ Ja	☐ Nein
n)	Clean Desk	☐ Ja	☐ Nein
o)	Lieferanten / Dienstleister / Subunternehmer	☐ Ja	☐ Nein

4.7	Werden die Sicherheitsrichtlinien in regelmäßigen Abständen überprüft und auf den neuesten Stand gebracht?	☐ Ja	☐ Nein
4.8	Sind alle Sicherheitsrichtlinien für alle Nutzer einfach zugänglich (z. B. stehen im Intranet des Unternehmens)?	☐ Ja	☐ Nein
4.9	Führt Ihr Unternehmen Schulungen zum Thema Informationssicherheit für alle betroffenen Mitarbeiter durch?	☐ Ja	☐ Nein
4.10	Zusätzliche Dokumente als Nachweis (falls vorhanden): **Bitte als Anlage beifügen.**	☐ Ja	☐ Nein

5 Detailfragen OT

Allgemeine Sicherheitsanforderungen Informationssicherheit OT

Zutritts-, Zugangs- und Zugriffsschutz

5.1	Stellt Ihre Organisation sicher, dass alle Systeme, von denen unmittelbar oder mittelbar ein Zugriff auf Ressourcen aus dem OT-Bereich des Auftraggebers möglich ist, mit einem Zutritts-, Zugangs- und Zugriffsschutz versehen sind?	☐ Ja	☐ Nein
5.2	Stellt Ihre Organisation durch geeignete organisatorische und technische Maßnahmen sicher, dass nur die berechtigen Mitarbeiter des Auftragnehmers Zutritt, Zugang und Zugriff zu den Ressourcen des Auftraggebers erhalten?	☐ Ja	☐ Nein

Einsatz sicherer Passwörter

5.3	Stellt Ihre Organisation für alle zur Zugangssicherung verwendeten Passwörter eine nach dem aktuellen Stand der Technik hohe Passwortgüte (z. B. gemäß der Empfehlungen der CIS Benchmark, des Bundesamts für Sicherheit in der Informationstechnik (BSI) oder des UK National Cyber Security Centre (NCSC)) sicher? **Bitte beschreiben Sie Anforderungen an Passwörter:**	☐ Ja	☐ Nein
5.4	Liegt eine entsprechende Passwortrichtlinie vor?	☐ Ja	☐ Nein
5.5	Wird die Passwortgüte durch technische Maßnahmen erzwungen bzw. sichergestellt?	☐ Ja	☐ Nein
5.6	Kommen zusätzlich zu Passwörtern weitere Sicherungsmaßnahmen (z. B. Multi-Faktor-Authentifizierung) zum Einsatz?	☐ Ja	☐ Nein

Verbot der privaten Nutzung

5.7	Stellt Ihre Organisation durch organisatorische oder technische Maßnahmen sicher, dass alle Systeme und Komponenten, von denen unmittelbar oder mittelbar ein Zugriff auf OT-Ressourcen des Auftraggebers möglich ist, nur für dienstliche Zwecke genutzt werden und dass eine private Nutzung durch die Mitarbeiter nicht zulässig ist?	☐ Ja	☐ Nein

5.8	Stellt Ihre Organisation durch technische oder organisatorische Maßnahmen sicher, dass private Komponenten der Mitarbeiter nicht für den Zugriff auf OT-Systeme des Auftraggebers benutzt werden dürfen bzw. dass sie nicht an Systeme bzw. Netze des Auftragnehmers angeschlossen werden dürfen, die für den Zugriff auf Ressourcen des Auftraggebers vorgesehen sind?	☐ Ja	☐ Nein

Wirksamkeit der Maßnahmen

5.9	Gibt es in Ihrer Organisation einen definierten Prozess, um alle organisatorischen Prozesse und Maßnahmen zur Informationssicherheit regelmäßig auf deren Wirksamkeit zu überprüfen (z. B. Audits, Assessments)? **Bitte beschreiben Sie kurz den Prozess:**	☐ Ja	☐ Nein
5.10	Gibt es in Ihrer Organisation einen definierten Prozess, um alle technischen Prozesse und Maßnahmen zur Informationssicherheit regelmäßig auf deren Wirksamkeit zu überprüfen (z. B. Audits, PenTests, Red Teaming)? **Bitte beschreiben Sie kurz den Prozess:**	☐ Ja	☐ Nein

Die Ergebnisse sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Sichere Entwicklung

5.11	Stellt Ihre Organisation durch organisatorische und/oder technische Maßnahmen sicher, dass bei der Entwicklung von Software Hardwarekomponenten oder Systemen anerkannte Entwicklungsstandards und Qualitätsmanagement eingehalten und unsichere Programmiertechniken und Funktionen vermieden werden?	☐ Ja	☐ Nein
5.12	Werden in Ihrer Organisation im Rahmen des Entwicklungsprozesses automatisierte Verfahren zur Überprüfung des Quellcodes, verwendeter Bibliotheken und sonstiger Programmbestandteile auf Schwachstellen und unsicheren Programmiertechniken eingesetzt?	☐ Ja	☐ Nein

Umgang mit Sicherheitsvorfällen und Sicherheitslücken

5.13 Gibt es in Ihre Organisation einen definierten Prozess, um Informationssicherheitsvorfälle (Incidents), welche den Auftraggeber, die Systeme des Auftraggebers oder die Erbringung des Liefer- und Leistungsumgangs direkt oder indirekt betreffen, unverzüglich an den Auftraggeber zu melden? ☐ Ja ☐ Nein

Bitte beschreiben Sie kurz den Prozess:

5.14 Stellt Ihre Organisation sicher, dass Sicherheitslücken oder Schwachstellen in Software, Hardwarekomponenten und Systemen, welche von Ihrer Organisation entwickelt oder als Bestandteil des Liefer- und Leistungsumfangs bereitgestellt werden, dem Auftraggeber unverzüglich bekannt gemacht werden? ☐ Ja ☐ Nein

Bitte beschreiben Sie kurz den Prozess:

5.15 Stellt Ihre Organisation sicher, dass Sicherheitslücken oder Schwachstellen, welche über interne oder externe Kanäle gemeldet oder bekannt werden, in einem angemessen Zeitrahmen behandelt und kommuniziert werden? ☐ Ja ☐ Nein

Hinweis: Die Kommunikation sollte auch dann unverzüglich erfolgen, wenn noch kein Patch zur Verfügung steht.

Bitte beschreiben Sie kurz den Prozess:

5.16 Ist Ihre Organisation aufgrund gesetzlicher, regulatorischer oder vertraglicher Vorgaben dazu verpflichtet, Sicherheitslücken, Schwachstellen oder Sicherheitsvorfälle zu melden? ☐ Ja ☐ Nein

Bitte listen Sie die Organisationen auf, an die Sie o.g. Ereignisse melden:

Entsorgung und Reparatur von Systemen

5.17	Stellt Ihre Organisation durch einen definierten Prozess sicher, dass Systeme oder Komponenten , welche zur Reparatur oder Entsorgung gegeben werden, keine vertraulichen oder sicherheitsrelevanten Daten mehr enthalten?	☐ Ja	☐ Nein

Sicherheit von Systemen auf dem Transportweg

5.18	Stellt Ihre Organisation durch einen definierten Prozess sicher, dass Systeme oder Komponenten mit vertraulichen oder sicherheitsrelevanten Daten oder Systeme, die für den Einsatz in OT-Anlagen des Auftraggebers vorgesehen sind, auf dem gesamten Transportweg vor unbefugten Zugriff gesichert sind?	☐ Ja	☐ Nein

Einhalten gesetzlicher Anforderungen

5.19	Stellt Ihre Organisation durch einen definierten Prozess sicher, dass gesetzliche, regulatorische oder sonstige Anforderungen für die Informationssicherheit in den Regionen oder Ländern, in denen Lieferungen oder Leistungen erbracht werden, eingehalten werden? **Bitte beschreiben Sie kurz den Prozess:**	☐ Ja	☐ Nein

Business Continuity / Notfallmanagement

5.20	Stellt Ihre Organisation durch definierte Business Continuity Prozesse sicher, dass im Rahmen einer Notlage oder Großstörung die Aufrechterhaltung einer minimalen Servicequalität und die schnellstmögliche Wiederherstellung aller für den Auftraggeber bereitzustellenden Dienste sicherstellt ist?	☐ Ja	☐ Nein
5.21	Werden diese Business Continuity Prozesse in regelmäßigen Abständen getestet, z. B. im Rahmen von Notfall- oder Disaster Recovery-Übungen? **Bitte beschreiben Sie kurz den Prozess:**	☐ Ja	☐ Nein

Schutz vertraulicher Daten

5.22	Stellt Ihre Organisation durch organisatorische und/oder technische Maßnahmen sicher, dass vertrauliche oder sicherheitsrelevante Daten oder Informationen, welche die Liefer- und Leistungserbringung für den Auftraggebers oder die OT-Anlagen und Systeme des Auftraggeber betreffen, sicher und vor unberechtigtem Zugriff geschützt gespeichert werden? **Bitte beschreiben Sie kurz den Prozess:**	☐ Ja	☐ Nein
5.23	Sind diese Daten oder Informationen auch dann vor unberechtigtem Zugriff geschützt, wenn diese außerhalb der Räumlichkeiten oder Netze (z. B. in Cloud-Systemen oder auf mobilen Geräten oder tragbaren Speichermedien) des Auftragnehmers gespeichert werden?	☐ Ja	☐ Nein

Bemerkungen / Ausschlüsse (bitte begründen):

RWE

Verpflichtung von Mitarbeitern und Subunternehmern des Auftragnehmers

Sicherheitsüberprüfung

5.24	Stellt Ihre Organisation durch einen definierten Prozess sicher, dass neu eingestellte Mitarbeiter, welche Zugriff auf OT-Systeme oder Daten des Auftraggebers haben, vor Aufnahme der Beschäftigung einer Sicherheits- bzw. Hintergrundüberprüfung unterzogen werden? **Bitte beschreiben Sie kurz den Prozess:**	☐ Ja	☐ Nein
5.25	Führt Ihre Organisation regelmäßige (nachträgliche) Sicherheits- und Hintergrundprüfungen für alle Mitarbeiter durch, die Zugang zu OT-Systemen oder Daten des Auftraggebers haben?	☐ Ja	☐ Nein

Sicherheitsunterweisung

5.26	Stellt Ihre Organisation sicher, dass alle Mitarbeiter über die sicherheitstechnischen Anforderungen der Ressourcen des Auftraggebers informiert sind? Das betrifft insbesondere die möglichen Risiken, adäquate Gegenmaßnahmen sowie die persönlichen Verantwortungen der Mitarbeiter im Rahmen ihrer Tätigkeiten.	☐ Ja	☐ Nein
5.27	Sensibilisiert Ihre Organisation ihre Mitarbeiter zusätzlich in Bezug auf Informationssicherheit regelmäßig durch entsprechende Schulungen oder Mitteilungen? Hierzu gehören auch sicherheitsbezogene Informationen bei Einführung neuer Techniken und Verfahren.	☐ Ja	☐ Nein

Datenschutz und Vertraulichkeit

5.28	Hat Ihre Organisation ihre Mitarbeiter auf die Einhaltung der datenschutzrechtlichen Bestimmungen, sowie auf die Vertraulichkeit der ihnen zugänglichen Daten (auch über das Ende ihrer Tätigkeit hinaus) verpflichtet?	☐ Ja	☐ Nein

Unteraufträge und Subunternehmer

5.29	Beschäftigt Ihre Organisation Unterauftragnehmer, die für die Erbringung der Lieferungen und Leistungen bei dem Auftraggeber notwendig sind bzw. eingesetzt werden? **Bitte listen Sie die Subunternehmer auf:**	☐ Ja	☐ Nein
5.30	Wenn ja: sind diese auf die Einhaltung der Informationssicherheits- und Datenschutzrichtlinie(n) verpflichtet und wurde dies durch den Auftragnehmer dokumentiert? Dies gilt auch für Arbeitnehmerüberlassungskräfte, die beim Auftragnehmer eingesetzt werden.	☐ Ja	☐ Nein

Bemerkungen / Ausschlüsse (bitte begründen):

Grundsicherung der Systeme

Systemhärtung und sichere Grundkonfiguration

5.31	Stellt Ihre Organisation sicher, dass alle Systeme und Netzwerkkomponenten der Organisation, auf welchen Daten des Auftraggebers verarbeitet oder gespeichert werden oder mit denen auf OT-Systeme des Auftraggebers zugegriffen wird, nach aktuellem Stand der Technik (z. B. gemäß der Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) oder der CIS Benchmarks) gehärtet sind? Dies beinhaltet, dass unnötige Benutzerkonten, Applikationen, Netzwerkprotokolle, Dienste und Services zu deinstallieren, oder – falls eine Deinstallation nicht möglich ist – dauerhaft zu deaktivieren und gegen versehentliches Reaktivieren zu schützen sind. **Beschreibung der Maßnahmen:**	☐ Ja	☐ Nein

5.32	Stellt Ihre Organisation durch geeignete Maßnahmen sicher, dass die sichere Grundkonfiguration dieser Systeme regelmäßig überprüft und dokumentiert wird?	☐ Ja	☐ Nein
	Sicherheitsupdates		
5.33	Stellt Ihre Organisation sicher, dass alle Systeme und Netzwerkkomponenten, auf welchen Daten des Auftraggebers verarbeitet oder gespeichert werden oder mit denen auf Systeme des Auftraggebers zugegriffen wird, mit aktuellen Software-/ Firmwareversionen, Service-Packs und Sicherheits-Patches versehen sind? **Beschreibung der Maßnahmen:**	☐ Ja	☐ Nein
5.34	Stellt Ihre Organisation durch geeignete technische oder organisatorische Maßnahmen sicher, dass der Patchstatus dieser Systeme regelmäßig überprüft und dokumentiert wird?	☐ Ja	☐ Nein
5.35	Stellt Ihre Organisation durch geeignete technische oder organisatorische Maßnahmen sicher, dass Sicherheitsupdates für das Betriebssystem und für Kommunikationsprogramme, mit denen auf Internetdienste zugegriffen wird, auf allen Systemen umgehend eingespielt werden?	☐ Ja	☐ Nein
	Antiviren- / Malwareschutz		
5.36	Stellt Ihre Organisation sicher, dass alle Systeme der Organisation , auf welchen Daten des Auftraggebers verarbeitet oder gespeichert werden oder mit denen auf OT-Systeme des Auftraggebers zugegriffen wird, über einen ständigen Virenschutz (On-Access-Scanner) und (tages-)aktuelle Viren-Pattern verfügen?	☐ Ja	☐ Nein
5.37	Stellt Ihre Organisation sicher, dass neben dem Virenschutz auf Arbeitsplatzsystemen der Organisation gleichermaßen Viren-Scanner im Gateway- bzw. Serverbereich, bei Storagesystemen, sowie bei Systemen für den E-Mail-Versand, dem Webverkehr und dem Filetransfer eingesetzt werden?	☐ Ja	☐ Nein

Lokale Administrationsrechte

5.38	Haben Anwender lokale Administrationsrechte auf den Einzelarbeitsplatzcomputern der Organisation?	☐ Ja	☐ Nein
5.39	Haben Administratoren lokale Administrationsrechte auf den Einzelarbeitsplatzcomputern der Organisation?	☐ Ja	☐ Nein
5.40	Haben Entwickler lokale Administrationsrechte auf den Einzelarbeitsplatzcomputern der Organisation?	☐ Ja	☐ Nein
5.41	Haben Techniker lokale Administrationsrechte auf den Einzelarbeitsplatzcomputern der Organisation?	☐ Ja	☐ Nein

Schwachstellenscans

5.42	Stellt Ihre Organisation sicher, dass alle Systeme, auf welchen Daten des Auftraggebers verarbeitet oder gespeichert werden oder mit denen auf OT-Systeme des Auftraggebers zugegriffen wird, in regelmäßigen Abständen und nach dem aktuellen Stand der Technik auf Schwachstellen oder Verwundbarkeiten gescannt werden?	☐ Ja	☐ Nein

Bemerkungen / Ausschlüsse (bitte begründen):

Netzwerksicherheit

Fernzugang / Remoteeinwahl in Netze des Auftragnehmers

5.43	Stellt Ihre Organisation ihren Mitarbeitern oder (Sub-)Dienstleistern einen Fernzugang oder eine Remoteeinwahl zur Verfügung, mit denen diese direkt oder indirekt auf OT-Systeme oder OT-Komponenten des Auftraggebers zugreifen können?	☐ Ja	☐ Nein

Fernzugang / Remoteeinwahl in Netze des Auftraggebers

5.44	Nutzt Ihre Organisation einen Fernzugang / eine Remoteeinwahl, um auf OT-Systeme oder OT-Komponenten des Auftraggebers zuzugreifen?	☐ Ja	☐ Nein

Nur falls ja: Fragen 5.45 bis 5.48 beantworten.

5.45	Wird dieser Fernzugriff vom Auftraggeber betrieben und zur Verfügung gestellt?	☐ Ja	☐ Nein

Falls Nein, beschreiben Sie bitte Art und Funktion des Fernzugangs:

5.46	Stellt Ihre Organisation durch geeignete organisatorische und technische Maßnahmen sicher, dass nur explizit autorisierte Mitarbeiter auf den Fernzugang zugreifen können?	☐ Ja	☐ Nein
5.47	Stellt Ihre Organisation durch geeignete organisatorische und technische Maßnahmen sicher, dass die Zugriffsrechte zu den Fernwartungssystemen so restriktiv wie möglich gehandhabt werden?	☐ Ja	☐ Nein
5.48	Stellt Ihre Organisation sicher, dass, falls ein Mitarbeiter seinen Aufgabenbereich wechselt oder das Unternehmen des Auftragnehmers verlässt, ihm umgehend die Zugangs- und Zugriffsberechtigung für den Fernzugang entzogen wird?	☐ Ja	☐ Nein

Schutz des internen Netzes

5.49	Ist das interne Netz Ihrer Organisation gegenüber dem Internet am Netzübergang durch eine Firewall, welche mindestens Stateful Packet Inspection-Funktionalität aufweist, geschützt?	☐ Ja	☐ Nein
5.50	Ist diese Firewall mit einem maximal restriktiven Regelwerk versehen, welches nur explizit benötigte und freigegebene Dienste erlaubt?	☐ Ja	☐ Nein
5.51	Ist diese Firewall so konfiguriert, dass direkte Zugriffe aus dem Internet in das interne Netz Ihrer Organisation unterbunden sind?	☐ Ja	☐ Nein
5.52	Überwacht Ihr Unternehmen Internet-Gateways auf (versuchte) Einbrüche und anomale oder bösartige Aktivitäten?	☐ Ja	☐ Nein

Datenübertragung über öffentliche Netze

5.53	Stellt Ihre Organisation durch technische Maßnahmen sicher, dass nicht autorisierte oder ungewöhnliche Datentransfers (z. B. unüblich große Datenmengen, unerwartete Arten von Netzwerktraffic oder Traffic zu unbekannten Zielpunkten) zwischen internen und öffentlichen Netzen erkannt und unterbunden werden? **Beschreibung der Maßnahmen:**	☐ Ja	☐ Nein

Kabellose Netze

5.54	Nutzt Ihre Organisation zur Erbringung der Lieferung und Leistungen kabellose Netze?	☐ Ja	☐ Nein
5.55	Falls ja: ist sichergestellt, dass diese kabellosen Netze angemessen gesichert sind, insbesondere durch starke Authentisierung und Verschlüsselung auf aktuellem Stand der Technik? **Beschreibung der Maßnahmen:**	☐ Ja	☐ Nein

Bemerkungen / Ausschlüsse (bitte begründen):

RWE

Wartungssysteme

Wartungssysteme zur Vor-Ort-Wartung

5.56	Stellt Ihre Organisation sicher, dass auf Wartungs- und Administrationssystemen der Organisation, insbesondere auf mobilen Geräten, die beim Auftraggeber vor Ort direkt an OT-Systeme angeschlossenen werden, eine Firewall-Software (z.B. OS-integrierte Firewall) installiert und aktiviert ist, die unberechtigte Zugriffe von außen verhindert?	☐ Ja	☐ Nein
5.57	Ist sichergestellt, dass die Firewall-Software vom Benutzer nicht deaktiviert werden kann?	☐ Ja	☐ Nein
5.58	Stellt Ihre Organisation alternativ sicher, dass diese Systeme nie direkt an unsichere Netze wie z. B. das Internet angeschlossen werden?	☐ Ja	☐ Nein

Sichere Administrations- und Wartungstools

5.59	Stellt Ihre Organisation sicher, dass die Tools, die zur Administration und Wartung der OT-Systeme des Auftraggebers eingesetzt werden, über eine personalisierte Anmeldung, kryptographischen Schutz der Passworte, optional eine starke Authentisierung und eine Rechteverwaltung mit Einschränkung des Zugriffs auf den erforderlichen Umfang verfügen?	☐ Ja	☐ Nein

Überprüfung auf Schadsoftware

5.60	Stellt Ihre Organisation sicher, dass mobile Wartungs- / Administrations- und Parametrier- / Programmiergeräte über einen ständigen Virenschutz (On-Access-Scanner) und (tages-) aktuelle Viren-Pattern verfügen? Hinweis: Vor einem Zugang zum OT-Bereich des Auftraggebers ist dieser Virenschutz zu aktualisieren! **Der Auftragnehmer hat auf Anfrage des Auftraggebers die getroffenen Vorsorgemaßnahmen unverzüglich im Detail darzustellen.**	☐ Ja	☐ Nein

Verschlüsselung von Festplatten und Wechseldatenträgern

5.61	Stellt Ihre Organisation sicher, dass bei allen Systemen und Wechseldatenträgern, welche zur Vor-Ort- und Fernwartung der OT-Systeme des Auftraggebers verwendet werden, eine Datenträgerverschlüsselung nach Stand der Technik (z. B. Bitlocker) aktiviert ist?	☐ Ja	☐ Nein

Bemerkungen / Ausschlüsse (bitte begründen):

6 Bestätigung

Unterschrift des Auftragnehmers

Der Auftragnehmer versichert, dass alle oben gemachten Angaben vollständig, wahrheitsgemäß und korrekt sind.

Alle Abweichungen zu den hier getätigten Angaben sind dem Auftraggeber unmittelbar zu melden.

Name (in Druckbuchstaben)

Ort, Datum

Unterschrift / Digitale Signatur