1	Regelung des Zuganges zu betrieblicher Hardware	
1-1		Sind Räume mit betrieblicher EDV-Ausstattung gesichert?
1-2		Verfügen Sie über Überwachungseinrichtungen (Zutrittssysteme, Videoüberwachung, etc.)?
1-3		Wurden Zugangsberechtigungen festgelegt?
1-4		Gibt es Sicherheitsvorkehrungen bei Reinigungs- und Wartungsarbeiten?
1-5		Gibt es Sicherheitsvorkehrungen bei Telearbeit (Netzwerkzugang von außen)?

2	Regelung des Zugriffes auf Daten	
2-1		Gibt es ein Benutzeridentifikations- und ein Passwortverfahren für technische Geräte?
2-2		Verfügen Sie über Systeme zur Protokollierung von Zugriffen auf Daten und deren Kontrolle?
2-3		Verfügen Sie über eine Dokumentation der Eingabeverfahren?
2-4		Sind automatische Bildschirmsperren (Passwortschutz bei Arbeitspausen) aktiviert?
2-5		Sind automatische Zugangssperren bei wiederholten Anmelde-Fehlversuchen aktiviert?
2-6		Gibt es individuelle Benutzerkonten für Mitarbeiter/innen?
2-7		Werden Datenträger verschlüsselt, insbesonders jene mit personenbezogenen Daten?
2-8		Gibt es ein Berechtigungskonzept und ein Verfahren für die Vergabe von Zugriffsrechten auf Basis des Betriebssystems?
2-9		Verfügen Sie über einen Schutz vor unberechtigten Zugriffen auf IT-Systeme (Firewall, etc.)?
2-10		Werden mobile Datenträger verwaltet, damit bekannt ist, wo diese sich gerade befinden um Verluste etc. zu entdecken?
2-11		Gibt es ein Verfahren zur Datenlöschung im Sinne der DSGVO?
2-12		Erfolgt die Entsorgung von alten Datenträgern, Fehldrucken mit sensiblen Informationen etc. auf einem sicheren Weg?
2-13		Gibt es eine interne Regelung für das Kopieren von Datenträgern? (z.B. Wer darf, wer nicht, …)
2-14		Gibt es schriftliche Regelungen für den Umgang mit mobile Devices (USB-Sticks, externe Festplatten, Tablets, Smartphones)?
2-15		Ist die Fernwartung von Servern und PCs so geregelt, dass Sie entweder über einen Verarbeitervertrag verfügen oder jederzeit Fernwartungen nachvollziehen können und die Geheimhaltung durch den Dienstleister sichergestellt ist?

3	Regelungen zur Weitergabe von Daten und Zugängen	
3-1		Ist ein sicherer Transport analoger Datenträger sichergestellt? (Boten, Post, etc.)
3-2		Ist ein sicherer elektronischer Datenversand sichergestellt? (z.B. Anhänge in E-Mails)
3-3		Erfolgt die Auswahl von Auftragnehmern mit Zugriffsberechtigungen unter Berücksichtigung der DSGVO bzw. deren Qualifikation zur Einhaltung der DSGVO?
3-4		Erfolgt die Weitergabe von Zugriffsberechtigungen an Subunternehmen im Sinne der DSGVO?
3-5		Gibt es eine schriftliche Regelung für Auftragnehmer mit Datenzugang im Sinne der DSGVO (Geheimhaltungsvereinbarung oder Verarbeitervertrag)?
3-6		Werden Kontrollmaßnahmen durch eine/einen Datenschutzkoordinatorin/en durchgeführt?

4	Regelungen zur Umsetzung einer "Datensicherung" zzgl. Datensicherheit	
4-1		Sind Brandschutz- und Wasserschutzmaßnahmen vorhanden?
4-2		Verfügen Sie über eine unterbrechungsfreie Stromversorgung für neuralgische IKT Geräte? (USV)
4-3		Werden Sicherungsdatenträger sicher und störungsfrei aufbewahrt?
4-4		Wurden Backup-Verfahren eingeführt, die den Anforderungen des Betriebes entsprechen?
4-5		Ist der Einsatz von Cloud-Lösungen geregelt und sind Sie sich der damit verbundenen Sicherheitsrisiken bewusst?
4-6		Ist ein Virenschutz auf allen Geräten eingeführt?
4-7		Erfolgen Funktionstests und Überprüfungen der Wiederherstellbarkeit des Backups?
4-8		Gibt es einen Notfallplan für externe (oder interne) Angriffe oder für Extremsituationen wie Schäden durch Feuer, Wasser etc. um eine Weiterführung des Betriebes sicher zu stellen?

5	Regelungen der organisatorischen Datenschutz- und Sicherungsmaßnahmen	
5-1		Gibt es innerbetriebliche Regelungen zur Datensicherheit?
5-2		Gibt es ein IT-Sicherheitskonzept (Richtlinien, Arbeitsanweisungen, etc.)?
5-3		Sind die organisatorischen Maßnahmen zum Schutz personenbezogener Maßnahmen konform mit der Datenschutz-Grundverordnung?
5-4		Erfolgt eine interne Kontrolle der Datenverarbeitungen?

5-5		Die stichprobenartige Überprüfung von Protokollen und Login-Daten erfolgt regelmäßig durch einen Professionisten?
5-6		Ist die Vertretung von mit der EDV befassten Mitarbeiter/innen im Urlaub- und Krankheitsfall geregelt?
5-7		Sind Ihre elektronischen Zutrittssysteme separat abgesichert? (z.B. Schlüsselkarten, etc.)

6	Regelung der externen/internen IT-Betreuung	
6-1		Verfügt der Dienstleister/Mitarbeiter über Qualifizierungsnachweise (Zertifikate z.B. incite, WIFI, …)?
6-2		Gibt es Vertretungsregelungen oder Notfallvorsorgen für den Fall der Nichtverfügbarkeit des Admins?
6-3		Werden bei der Beendigung der Tätigkeit als IT-Administrator dessen Zugangsmöglichkeiten gesperrt?
6-4		Gibt es dokumentierte Regelungen für Wartungs- und Reparaturarbeiten?
6-5		Sind die Administrations-Kennungen (Benutzerdaten und Kennwörter) vor Zugriffen Dritter geschützt?
6-6		Wird Ihr System mittels Monitoring-Systeme (MDM) überwacht?
6-7		Ist der Administrator für die laufende Aktualisierung der Dokumentation verantwortlich?
6-8		Wurden "Auto-Update-Mechanismen" aktiviert/eingerichtet?

7	Regelungen zum Schutz von WLANs	
7-1		Erfolgte nachweislich eine sichere Basiskonfiguration Ihres Accesspoints oder WLAN-Routers (Einhaltung der WLAN-Sicherheitsstandards)?
7-2		Ist sichergestellt, dass die Mitarbeiter/innen das betriebliche WLAN mit privaten Geräten nicht benutzen können?
7-3		Ist sichergestellt, dass Gäste/Besucher/private Endgeräte in einem separaten WLAN abgetrennt werden und so keinen Zugriff auf Unternehmensdaten haben?
7-4		Sind Ihre Mitarbeiter/innen darauf geschult, die Zugangsdaten des WLANs nicht an Dritte weiter zu geben?
7-5		Führen Sie eine regelmäßige Überprüfung der im WLAN angemeldeten Benutzer und Endgeräte durch?

8	Regelungen zur sicheren Einrichtung einer Firewall	
8-1		Ist eine sichere Grundkonfiguration dieser Firewall dokumentiert und sichergestellt?
8-2		Werden regelmäßig Updates und Patches (Firmware) auf dem Gerät eingespielt?

8-3		Ist die Administrationsschnittstelle geschützt?
8-4		Erfolgt die Absicherung von grundlegenden Internetprotokollen?
8-5		Haben Sie geeignete Filterregelungen am Paketfilter eingerichtet?
8-6		Sind Reaktionszeiten für den Fall des Ausfalles der Firewall mit internem Personal bzw. externen Dienstleistern geregelt?
8-7		Wurde eine Betriebsdokumentation erstellt und wird diese laufend aktualisiert?

9	Regelungen zum Schutz von Fernzugriffen	
9-1		Ist ein externer Zugriff mittels VPN eingerichtet?
9-2		Wurde eine Sicherheitsrichtlinie zur VPN-Nutzung erstellt?
9-3		Werden nicht mehr benötigte VPN-Zugänge gesperrt?
9-4		Werden Zugriffsvorgänge über die VPN-Zugänge protokolliert und regelmäßig geprüft?

10	Regelungen zur Schulung von Mitarbeiter/innen	
10-1		Sind Reaktionen auf Verletzungen der Sicherheitsvorgaben in Ihrem Betrieb definiert und geschult?
10-2		Werden Fremdpersonen in sensiblen Bereichen beaufsichtigt und begleitet?
10-3		Erfolgt eine geregelte (dokumentierte) Einarbeitung/Einschulung neuer Mitarbeiter/innen?
10-4		Haben Sie eine Rollenbeschreibung der Arbeitsplätze?
10-5		Gibt es eine geregelte (dokumentierte) Verfahrensweise beim Weggang eines Mitarbeiters/einer Mitarbeiterin?
10-6		Werden Ihre Mitarbeiter/innen regelmäßig auf IT-sicherheitsrelevante Verfahren geschult?
10-7		Erfolgt eine Sensibilisierung Ihrer Mitarbeiter/innen hinsichtlich Informationssicherheit?
10-8		Werden Ihre Mitarbeiter/innen im sicheren Umgang mit IT-Systemen geschult?
10-9		Gibt es eine schriftliche Richtlinie zur sicheren IT-Nutzung?
10-10		Gibt es Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal? (inkl. Putzpersonal)
10-11		Haben Sie eine schriftliche Verschwiegenheits-/Vertraulichkeitsvereinbarung mit Ihren Mitarbeiter/innen?

11	Regelungen zum Umgang mit mobilen Endgeräten	
11-1		Ist eine sichere Grundkonfiguration für mobile Geräte sichergestellt?
11-2		Ist die Verwendung eines erweiterten Zugriffsschutz (Passwort statt PIN) sichergestellt?
11-3		Erfolgen regelmäßige Updates von Betriebssystem und Applikationen?
11-4		Wurden nichtbenutzte Kommunikationsschnittstellen deaktiviert (Ortungsdienste, ...)?
11-5		Gibt es schriftliche Richtlinien zur Benutzung von betrieblichen Mobilen Endgeräten?
11-6		Ist die Auswahl und Freigabe von Applikationen vor der Installation sichergestellt?
11-7		Gibt es eine Definition von erlaubten Informationen (Dateien, Kontakte, E-Mail-Konten) auf mobilen Geräten?
11-8		Ist sichergestellt, dass bei betrieblicher Nutzung von privaten Endgeräten eine explizite/schriftliche Regelung vorliegt?
11-9		Nutzen Sie zur Verwaltung der (betrieblichen) mobilen Endgeräte ein Mobile-Device-Management (MDM)?
11-10		Ist die Nutzung von privaten Endgeräten für betriebliche Zwecke erlaubt? (Dulden = erlauben)
11-11		Verwenden Sie auf dem mobilen Endgerät einen lokalen Virenschutz?
11-12		Ist die "automatische Sperre" in den Einstellungen aktiviert?
11-13		Ist die Möglichkeit einer Fernlöschung sichergestellt?

12	Erfüllen Sie die Voraussetzungen nach dem Cyber Risk Rating?	
12-1		Haben Sie eine aktuelle Informationssicherheitsrichtlinie (bzw. IT-Sicherheitsrichtlinie), die für Ihr Unternehmen gültig ist?
12-2		Schulen Sie Ihre Mitarbeiter regelmäßig in IT-Sicherheit und Datenschutz?
12-3		Gibt es in Ihrem Unternehmen eine oder mehrere Personen, die für das Thema Informationssicherheit und Datenschutz zuständig sind?
12-4		Pflegen Sie regelmäßig ein Verzeichnis all Ihrer Datenverarbeitungsprozesse, IT-Systeme und der damit verbundenen Verantwortlichkeiten?
12-5		Verwalten Sie den Zugang zu Ihren Systemen nach einem Berechtigungskonzept, das jedem nur die für seine Arbeit notwendigen Rechte einräumt?
12-6		Verlangen Sie von Ihren Mitarbeitern für alle Anwendungen Passwörter mit einer sicheren Mindeststärke zu verwenden?
12-7		Verwenden Sie die vom Hersteller empfohlenen Sicherheitseinstellungen und achten Sie auf eine sichere Konfiguration all Ihrer IT-Systeme?
12-8		Überprüfen Sie – sofern vorhanden – individuell entwickelte, aus dem Internet zugängliche Anwendungen auf Sicherheitslücken vor Inbetriebnahme?

12-9		Aktualisieren Sie al Ihre IT-Systeme und Anwendungen regelmäßig mit Sicherheitsupdates?
12-10		Sichern Sie Ihr Netzwerk vor unberechtigtem Zugriff von Außen ab?
12-11		Überwachen Sie Ihre IT-Systeme auf Malware und IT-Sicherheitsvorfälle?
12-12		Verschlüsseln Sie sensible Daten bei der Übertragung im Internet?
12-13		Protokollieren Sie die Nutzung Ihrer IT-Systeme, um Malware und IT-Sicherheitsvorfälle nachvollziehbar zu machen?
12-14		Haben Sie einen Notfallplan, anhand dessen Sie auf einen IT-Sicherheitsvorfall reagieren?