Policy Compliance Checklist

What policies does your organisation need for ISO 27001, GDPR, SOC 2, and general HR compliance? Use this checklist to identify gaps.

How to use this checklist

Review each section below against your current policy library. Tick off what you have, mark what you need, and note any gaps. At the end, you will have a clear picture of your compliance readiness and exactly which policies to prioritise.

Organisation: _____ **Date:** _____

Completed by: _____ **Role:** _____

1. Information Security (ISO 27001)

Essential policies for ISO 27001 certification. These cover Annex A controls and are required for most information security management systems.

	Policy	Status	Notes
☐	Information Security Policy (A.5.1)		
☐	Acceptable Use Policy (A.5.10)		
☐	Access Control Policy (A.5.15)		
☐	Data Classification Policy (A.5.12)		
☐	Cryptographic Controls Policy (A.8.24)		
☐	Physical Security Policy (A.7.1)		
☐	Incident Management Policy (A.5.24)		
☐	Business Continuity Policy (A.5.29)		
☐	Change Management Policy (A.8.32)		
☐	Supplier Relationship Policy (A.5.19)		
☐	Asset Management Policy (A.5.9)		
☐	Secure Development Policy (A.8.25)		

	Policy	Status	Notes
■	Backup and Recovery Policy (A.8.13)		
■	Logging and Monitoring Policy (A.8.15)		
■	Network Security Policy (A.8.20)		

2. Data Protection (UK GDPR)

Required policies for GDPR compliance. Organisations processing personal data of UK/EU residents must have these documented.

	Policy	Status	Notes
■	Data Protection Policy (Art. 24)		
■	Privacy Notice — Employees (Art. 13)		
■	Privacy Notice — Customers/Website (Art. 13)		
■	Data Retention and Disposal Policy (Art. 5(1)(e))		
■	Data Subject Access Request (DSAR) Procedure (Art. 15)		
■	Data Breach Notification Procedure (Art. 33/34)		
■	Data Protection Impact Assessment (DPIA) Policy (Art. 35)		
■	International Data Transfer Policy (Art. 44-49)		
■	Cookie Policy (ePrivacy Regulation)		
■	Consent Management Policy (Art. 7)		
■	Records of Processing Activities (Art. 30)		
■	Data Processor Agreement Template (Art. 28)		

3. SOC 2 Trust Service Criteria

Policies mapped to the five SOC 2 Trust Service Criteria. Required for SOC 2 Type I/II audit readiness.

	Policy	Status	Notes
■	Information Security Policy (CC1.1)		
■	Risk Assessment Policy (CC3.1)		
■	Logical Access Controls Policy (CC6.1)		
■	System Operations Policy (CC7.1)		
■	Change Management Policy (CC8.1)		
■	Incident Response Plan (CC7.3)		
■	Vendor Management Policy (CC9.2)		
■	Data Integrity Policy (PI1.1) — Processing Integrity		

	Policy	Status	Notes
■	Privacy Policy (P1.1) — Privacy Criteria		
■	Availability and DR Policy (A1.1)		
■	Confidentiality Classification Policy (C1.1)		

4. HR and Employment Policies

Core workplace policies that every UK organisation should have. Many are legally required under employment law.

	Policy	Status	Notes
■	Employee Handbook / Code of Conduct		
■	Equal Opportunities and Diversity Policy		
■	Anti-Harassment and Bullying Policy		
■	Disciplinary and Grievance Procedure		
■	Health and Safety Policy (legally required if 5+ staff)		
■	Maternity, Paternity, and Parental Leave Policy		
■	Flexible Working Policy		
■	Sickness and Absence Policy		
■	Whistleblowing Policy		
■	Social Media and Communications Policy		
■	Remote / Hybrid Working Policy		
■	Training and Development Policy		

5. IT and Operational Policies

Practical policies for day-to-day IT governance and operational security.

	Policy	Status	Notes
■	Bring Your Own Device (BYOD) Policy		
■	Password and Authentication Policy		
■	Email and Internet Usage Policy		
■	Software Licensing and Installation Policy		
■	Mobile Device Management Policy		
■	Clean Desk and Clear Screen Policy		
■	Patch Management Policy		
■	Disposal and Decommissioning Policy		

Your Compliance Readiness Score

Tally your results from each section to see where you stand.

Section	Total Policies	You Have	You Need	Coverage
1. ISO 27001	15			%
2. UK GDPR	12			%
3. SOC 2	11			%
4. HR / Employment	12			%
5. IT / Operational	8			%
TOTAL	**58**			**%**

What your score means

90 - 100%	**Excellent**	Your policy library is comprehensive. Focus on keeping policies up to date and ensuring acknowledgem
70 - 89%	**Good**	Most foundations are in place. Identify the missing policies and prioritise those needed for upcoming aud
50 - 69%	**Needs Work**	Significant gaps exist. Consider a policy pack to quickly fill the most critical areas for your compliance re
Below 50%	**At Risk**	Major gaps across multiple frameworks. An unlimited licence would give you access to all 530+ policies

---

Fill your gaps instantly with PolicySuite

Every policy in this checklist is available as a professionally drafted, customisable template on PolicySuite. Buy individual policies, grab a framework pack, or get unlimited access to all 530+ policies.

Individual policies — buy exactly what you need, one-time purchase

Policy packs — framework-specific bundles from £199 (e.g., ISO 27001, GDPR, HR)

Unlimited annual licence — access every policy, lifecycle management, distribution, and tracking

Get started at app.policy-suite.com