Making a Career in Governance, Risk & Compliance (GRC)

The strategic side of cybersecurity. Frameworks, risk and policy explained.

AUTHOR	Babashaheer
VERSION	1.0
DATE	April 2026
SERIES	Cybersecurity Career Series — Document 09 of 12
AUDIENCE	Students and professionals considering a GRC or risk management career

Contents

Digitally signed by Baba Shaheer Gutappa
Date: 2026.04.23 18:23:38 +01'00'

1. What Is GRC — and Is It a Real Career?

GRC stands for Governance, Risk and Compliance. It is the part of cybersecurity that deals not with technical attacks and defences, but with the strategy, policy and management layer above them. While a penetration tester asks 'can I break in?', a GRC professional asks 'what are our risks, do we manage them properly, and can we prove it to regulators and auditors?'

It is a genuine, well-paid and highly in-demand career. GRC professionals are often the people in the room with the board of directors. They write the policies that govern how every technical control is implemented. They manage regulatory relationships. They are frequently the highest-earners in a security team — and the most likely to progress into leadership roles such as CISO, DPO or Head of Risk.

> **GRC is where cybersecurity meets business, law and strategy.**
> It is the most accessible entry point for people without a deep technical background — and one of the clearest paths to senior leadership in the security industry.

The three components

Component	What It Means	What GRC Professionals Do
Governance	The framework of policies, procedures and accountability structures that define how an organisation manages security	Write security policies. Define roles and responsibilities. Report to the board. Ensure accountability at every level.
Risk	The identification, assessment and treatment of threats to the organisation — evaluating likelihood and potential impact	Conduct risk assessments. Maintain risk registers. Recommend controls. Present risk appetite decisions to leadership.
Compliance	Ensuring the organisation meets its legal, regulatory and contractual security obligations	Map controls to standards (ISO 27001, GDPR, PCI DSS). Manage audits. Maintain evidence. Report compliance status.

Table 1: The three pillars of GRC and what professionals do in each area

Level	Typical UK Salary	Common Roles
Junior	£28,000 – £42,000	GRC Analyst, Information Security Analyst, Compliance Analyst
Mid-level	£45,000 – £70,000	Risk Manager, Information Security Manager, Data Protection Officer (SME)
Senior	£70,000 – £100,000+	Head of GRC, Senior ISMS Manager, Enterprise Risk Manager
Leadership	£90,000 – £160,000+	CISO, DPO (large org), VP Risk & Compliance, Group Head of Information Security

Table 2: UK salary ranges for GRC and security management roles (CW Jobs, 2024)

2. How GRC Differs from Technical Cybersecurity Roles

Understanding what makes GRC different from roles like penetration testing or forensics is important — because the day-to-day work, the skills needed and the kind of person who thrives are quite different. Neither is more important than the other; they just require different strengths.

	GRC / Risk / Compliance	Technical Cybersecurity (e.g. Pentest)
Primary output	Policies, reports, risk registers, audit evidence	Technical findings, exploit code, tools
Core skill	Written communication, analytical thinking	Technical hands-on, problem-solving
Biggest tools	Word, Excel, GRC platforms (ServiceNow, Archer)	Nmap, Metasploit, Burp Suite, Wireshark
Works closely with	Legal, HR, senior leadership, auditors	IT teams, developers, security operations
Regulated skill?	Law, GDPR, ISO standards, frameworks	Exploit techniques, programming, networking
Suits people who...	Enjoy writing, strategy and influencing decisions	Enjoy breaking things and solving technical puzzles
Entry point	Business, law or IT degree; CISM or CISSP	CompTIA Security+ / CEH / TryHackMe
Career ceiling	CISO, DPO, Board-level risk committee	Principal Consultant, Technical Director

Table 3: GRC compared to technical cybersecurity roles

Do you need to be technical to work in GRC?
Not in the traditional hacking sense — but you must understand what technical controls do, why they matter, and whether they are implemented correctly. You do not need to write the code — but you must be able to read the audit evidence and ask the right questions.

3. The GRC Landscape — Key Frameworks and Standards

One of the first things that overwhelms people entering GRC is the volume of standards, frameworks and regulations. ISO 27001. NIST. GDPR. PCI DSS. NIS2. Cyber Essentials. SOC 2. DORA. Each one serves a different purpose and applies to different organisations. The diagram below maps the most important ones — and the table explains when each applies.

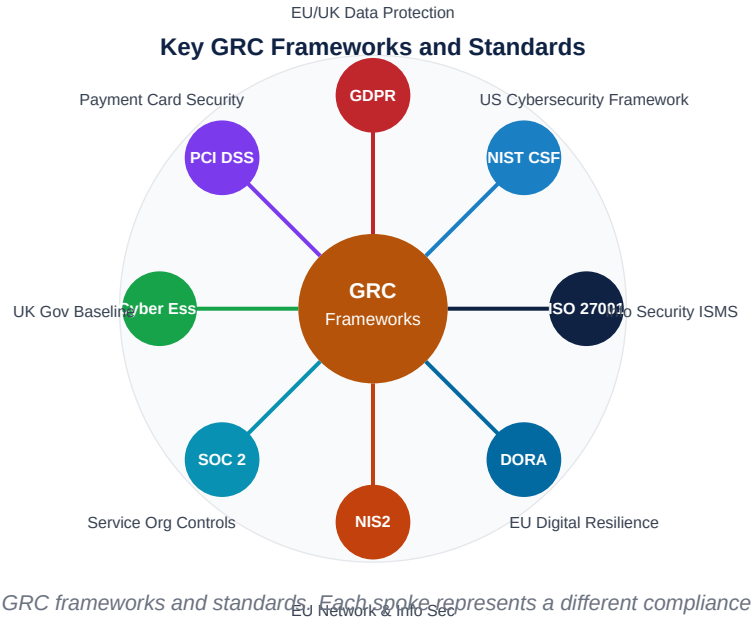


Figure 1: Key GRC frameworks and standards. Each spoke represents a different compliance requirement.

Framework / Regulation	Type	Who Must Comply	Managed By
ISO/IEC 27001:2022	International Standard	Any organisation wanting to certify their ISMS. Voluntary but frequently required by contracts.	BSI, UKAS-accredited certification bodies
NIST Cybersecurity Framework (CSF 2.0)	US Framework	US federal agencies; widely adopted globally as best practice. Not mandatory in UK but highly referenced.	NIST (US Gov)
UK GDPR / GDPR	UK/EU Law	Any organisation processing personal data of UK/EU residents — regardless of where they are based.	ICO (UK), EU Data Protection Authorities
PCI DSS v4.0	Industry Standard	Any organisation that processes, stores or transmits payment card data.	PCI Security Standards Council
Cyber Essentials / CE Plus	UK Gov Scheme	Required for UK government contracts. Highly recommended for all UK businesses.	NCSC / IASME
NIS2 Directive	EU Law	Operators of Essential Services and Digital Service Providers in the EU. Applies to UK supply chains.	EU Member State authorities

Framework / Regulation	Type	Who Must Comply	Managed By
SOC 2 Type II	US Audit Standard	SaaS and service companies handling customer data — frequently required by US enterprise clients.	AICPA-licensed auditors
DORA — Digital Operational Resilience Act	EU Financial Law	Financial institutions and their ICT suppliers operating in the EU. Comes into force January 2025.	European Supervisory Authorities (ESAs)

Table 4: Key GRC frameworks and regulations — what they are and who they apply to

4. Risk Management — The Core of GRC

Everything in GRC flows from risk management. Before you can write a policy, implement a control or demonstrate compliance, you need to understand what risks you are managing and why. Risk management is not about eliminating all risk — that is impossible. It is about understanding which risks are acceptable and which must be treated.

The risk management process

- **1. Identify the assets:** What does the organisation have that is worth protecting? Servers, data, applications, people, intellectual property, reputation.
- **2. Identify the threats:** What could go wrong? Phishing, ransomware, insider theft, accidental data loss, supplier failure, regulatory change.
- **3. Identify the vulnerabilities:** What weaknesses could a threat exploit? Unpatched software, weak passwords, no MFA, third-party access without review.
- **4. Assess the risk:** For each combination of threat and vulnerability, estimate the likelihood and the impact. This produces a risk score — usually plotted on a risk matrix.
- **5. Choose a treatment:** For each risk, decide whether to avoid, reduce, transfer or accept it (see the diagram below).
- **6. Implement controls:** Apply the chosen treatment — technical controls, procedural controls or contractual protections.
- **7. Monitor and review:** Risks change. The risk register must be a living document, reviewed at least annually and whenever significant changes occur.

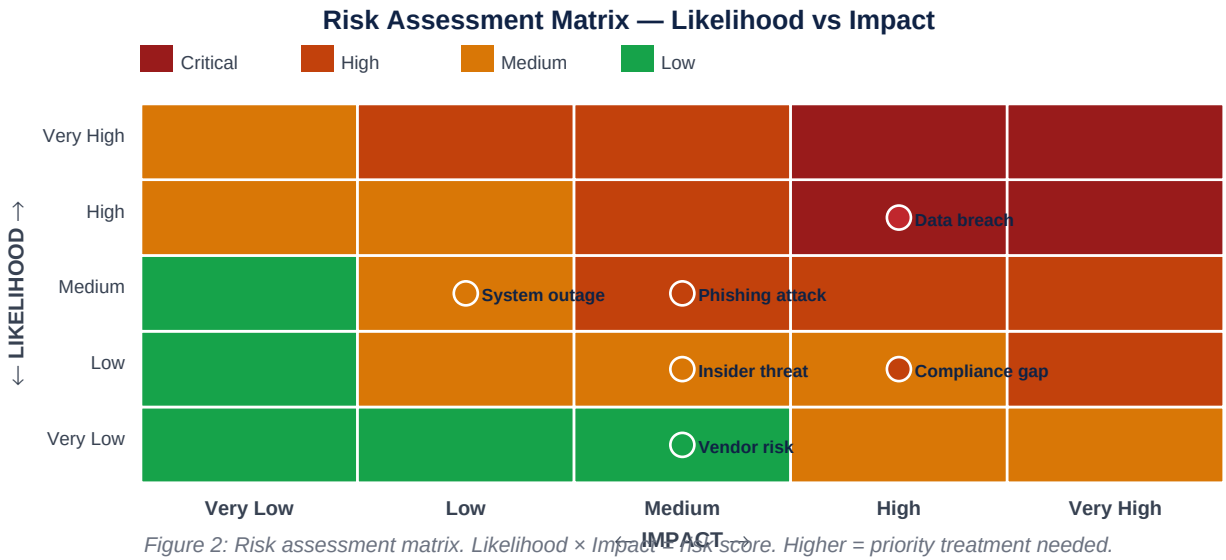


Figure 2: Risk assessment matrix. Likelihood × Impact = risk score. Higher = priority treatment needed.

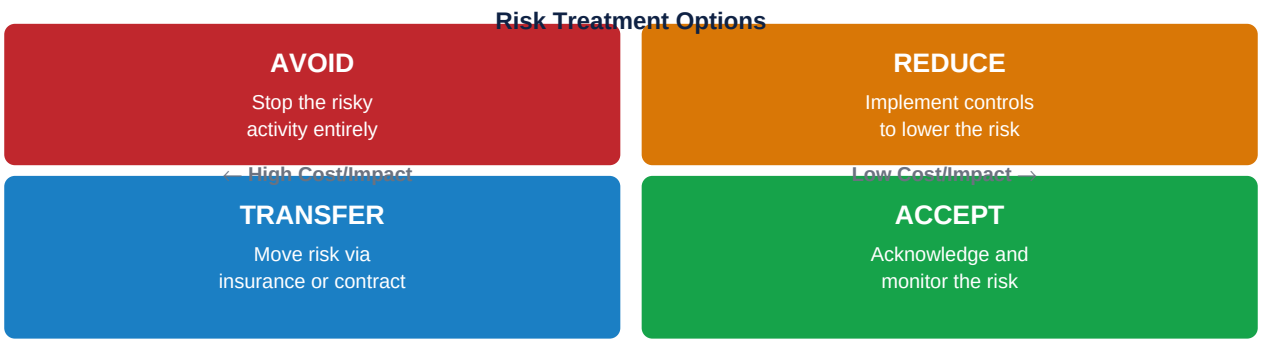


Figure 3: The four risk treatment options. Every identified risk must be assigned one.

5. ISO 27001 — The International Security Standard

ISO/IEC 27001 is the international standard for Information Security Management Systems (ISMS). An ISMS is a documented, systematic approach to managing information security risk across an organisation. Achieving ISO 27001 certification means an independent auditor has verified that your security management processes meet the standard. It is the most widely recognised security certification for organisations in the UK and globally — and it frequently appears as a contractual requirement for doing business with large enterprises and government.

What ISO 27001 actually requires

The standard is built around 10 clauses (the management system requirements) and Annex A, which contains 93 security controls across 4 themes. Organisations do not have to implement all 93 controls — they must assess which apply to their environment and document why they have included or excluded each one in a Statement of Applicability (SoA).

ISO 27001 Annex A Theme	Number of Controls	Examples of Controls Covered
Organisational Controls	37	Information security policies, risk management, supplier relationships, incident management, business continuity
People Controls	8	Background verification, security awareness training, disciplinary process, remote working policies
Physical Controls	14	Physical security perimeters, clear desk policy, equipment security, secure disposal of media
Technological Controls	34	Access control, cryptography, network security, vulnerability management, logging and monitoring, SIEM

Table 5: ISO 27001:2022 Annex A control themes

The ISO 27001 certification process

- **Stage 1 audit (documentation review):** The external auditor reviews your ISMS documentation — policies, risk assessment, Statement of Applicability, risk treatment plan.
- **Stage 2 audit (implementation review):** The auditor visits (or connects remotely) to verify that what is documented is actually implemented. They test controls, interview staff and examine evidence.
- **Certification granted:** If both stages pass, certification is granted. It is valid for three years, with annual surveillance audits.
- **Recertification:** A full recertification audit is conducted at the end of the three-year cycle.

ISO 27001 implementation typically takes 6–18 months for a mid-sized organisation.
A GRC professional managing this project will touch every team in the business — IT, HR, legal, finance, operations, procurement. It is a leadership role in practice.

6. GDPR and Data Protection Law

The UK General Data Protection Regulation (UK GDPR) and its EU equivalent (EU GDPR) are the most significant data protection laws in the world. Any organisation that handles personal data about UK or EU residents must comply — regardless of where the organisation itself is based. For most UK businesses this is simply a fact of operation. GRC professionals are frequently the people responsible for ensuring compliance.

GDPR Principle	What It Means in Practice	GRC Responsibility
Lawful basis	Every piece of data processing must have a legal basis — consent, contract, legitimate interest or legal obligation.	Maintain a Record of Processing Activities (RoPA). Review and document legal basis for each processing activity.
Data minimisation	Only collect the data you actually need. Do not store it longer than necessary.	Data mapping exercises. Retention schedule implementation. Advising teams on what data to collect.
Purpose limitation	Data collected for one purpose cannot be used for a different, incompatible purpose.	Review new data uses. Flag scope creep to legal and DPO.
Accuracy	Personal data must be kept accurate and up to date.	Data quality processes. Rights of individuals to correct inaccurate data.
Storage limitation	Do not keep personal data indefinitely. Define and enforce retention periods.	Retention schedules. Automated deletion where possible.
Security	Implement appropriate technical and organisational measures to protect personal data.	Risk assessment. Control selection. Security awareness. Incident reporting.
Accountability	Demonstrate compliance — not just claim it. Keep records. Conduct DPIAs.	Maintain compliance records. Conduct Data Protection Impact Assessments (DPIAs). Manage the RoPA.

Table 6: UK GDPR principles and the GRC professional's role in each

Maximum GDPR fine: 4% of global annual turnover or £17.5 million — whichever is higher.
In 2023 alone, the ICO issued fines totalling over £6 million in the UK.
The DPO (Data Protection Officer) role is a legal requirement for many organisations.

7. Other Key Regulations and Standards

Regulation / Standard	Applies To	Key Requirement	GRC Role
PCI DSS v4.0	Any business accepting card payments	12 requirements covering network security, access control, encryption, testing and monitoring	Manage compliance programme. Coordinate QSA audits. Ensure controls meet cardholder data environment requirements.
Cyber Essentials	UK businesses (mandatory for gov contracts)	Five controls: firewalls, secure configuration, user access control, malware protection, patch management	Implement and maintain the 5 controls. Coordinate annual self-assessment or Plus certification.
NIS Regulations 2018 (UK)	Operators of Essential Services (energy, water, transport, health, digital infrastructure)	Appropriate network/information security measures. Incident reporting to regulator.	Risk assessment. Incident reporting procedures. Regulatory relationship management.
DORA (EU)	Financial entities and their ICT suppliers in the EU	Digital operational resilience — ICT risk management, testing, incident reporting, third-party risk	Third-party risk management programme. Resilience testing coordination. ICT risk framework.
NHS Data Security & Protection Toolkit	NHS organisations and suppliers	Annual self-assessment against 10 standards covering data security, staff training and IG governance	Complete annual DSPT submission. Evidence collection. Staff training coordination.

Table 7: Additional regulations and standards relevant to UK GRC professionals

8. What a GRC Professional Actually Does

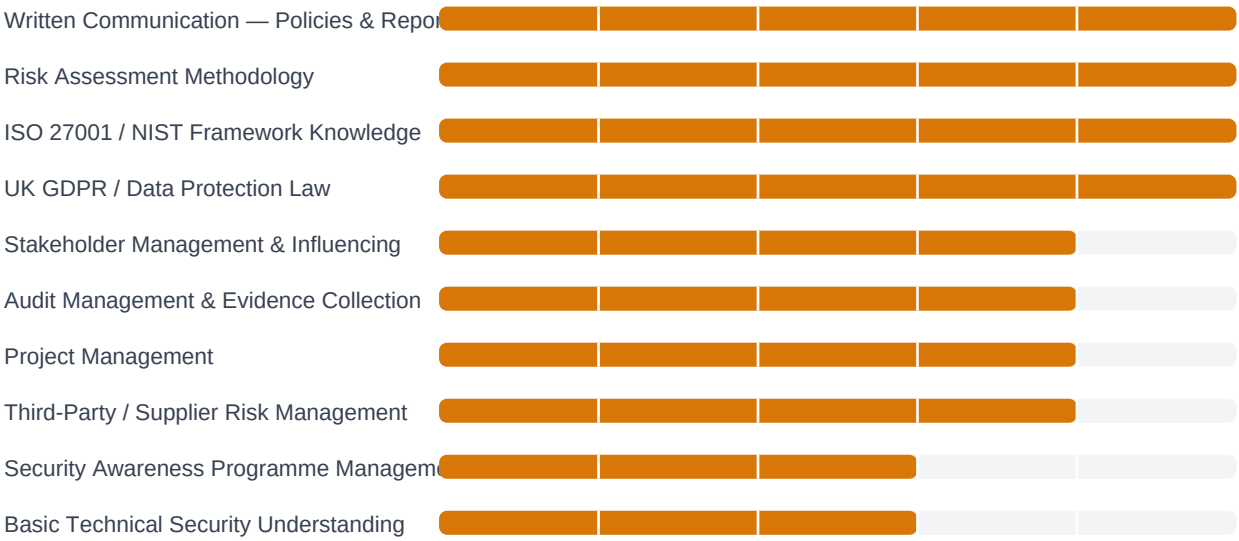
GRC is not a passive, paper-pushing job. The best GRC professionals are strategists, communicators and project managers. They spend their time influencing decisions, managing competing priorities, and translating complex regulatory requirements into practical actions that real teams can implement. Here is what a typical week might look like.

Activity	% of Time	What This Looks Like in Practice
Policy writing and review	15–20%	Drafting, updating and reviewing information security policies. Ensuring they reflect current standards, legal requirements and business practice.
Risk assessments	20–25%	Facilitated workshops with business units to identify and score risks. Updating the risk register. Recommending treatments to management.
Audit and compliance management	20–25%	Preparing for audits — gathering evidence, coordinating with IT teams, managing auditor queries, tracking remediation of findings.
Regulatory monitoring	10–15%	Staying current with changes to GDPR guidance, new ICO decisions, NIS2 implementation, DORA updates. Assessing impact on the organisation.
Stakeholder management	15–20%	Presenting the risk position to the board. Briefing the CISO. Working with procurement on supplier assessments. Training non-technical staff.
Incident support	5–10%	When a breach or incident occurs, the GRC team leads the regulatory notification process — reporting to the ICO within 72 hours if required.

Table 8: Typical time split for a mid-level GRC professional

9. Core Skills You Need to Build

GRC requires a different skills profile from technical roles. Technical knowledge matters, but communication, analytical thinking and the ability to manage projects and people are equally important — and often harder to find.



What 'basic technical understanding' actually means in GRC

You do not need to know how to configure a firewall. But you do need to understand what a firewall does, why it matters, and how to evaluate whether the organisation's firewall controls are adequate. The same applies to encryption, access control, patch management and logging. You are the person who reads the technical evidence and decides whether it is sufficient.

The most important skill in GRC is clear writing.
Policies nobody reads are useless. Risk reports the board cannot understand achieve nothing.
The ability to communicate security risk in plain business English is rare and highly valued.

10. Career Paths in GRC

GRC offers some of the clearest career progression in cybersecurity. The path from analyst to senior leader is well-defined, and the skills you build translate directly into some of the most senior and best-paid roles in the industry.

Role	What You Do	Where You Work	UK Salary
GRC / IG Analyst	Maintain policies and risk registers. Support audits. Draft compliance reports.	Financial services, healthcare, public sector	£28k–£42k
Information Security Analyst	Broader security role — risk assessment, policy, incident support, awareness training.	Any sector, especially regulated industries	£32k–£50k
Compliance Manager	Manage a specific compliance programme (GDPR, PCI DSS, ISO 27001). Own audit relationships.	Financial services, tech companies, law firms	£45k–£65k
Risk Manager / IS Risk Manager	Own the enterprise risk management function. Present to the board. Manage the risk register.	Banks, insurers, large enterprises	£55k–£80k
Information Security Manager	Manage the ISMS — policies, controls, risk, awareness, supplier security, incident response coordination.	Medium-large enterprises	£60k–£85k
Data Protection Officer (DPO)	Legal requirement for many organisations. Owns GDPR compliance. Reports to board level.	Healthcare, public sector, tech, financial services	£60k–£90k
Head of GRC / Head of Information Security	Leads the GRC function. Budget holder. Direct board access. Manages a team.	Large enterprises, Group-level roles	£80k–£120k
CISO — Chief Information Security Officer	Owns the entire security strategy. C-suite position. Reports to CEO or board.	All large organisations	£120k–£200k+

Table 9: Career progression in GRC — from analyst to CISO (Reed, 2024; CW Jobs, 2024)

11. The Learning Roadmap

GRC is one of the most accessible entry points into cybersecurity for people without a technical background. The learning path is structured and the progression to senior roles is clear. Here is the roadmap.

1 — Understand cybersecurity fundamentals
CompTIA Security+ gives you the technical foundation you need. You do not need to become a hacker — but you must understand what the controls you are assessing actually do. Professor Messer's free course is the most efficient way. 6–8 weeks.

2 — Learn the ISO 27001 standard
Download the BSI pocket guide (free). Read the actual standard if you can access it. Study the 10 clauses and Annex A controls. ISO 27001 Lead Implementer courses (4–5 days) give structured learning. This should be your priority. 4–8 weeks.

3 — Study UK GDPR in depth
Read the ICO's Guide to UK GDPR (free at ico.org.uk). Understand the 7 principles, lawful bases, data subject rights and breach notification requirements. BCS Data Protection Foundation is a recognised starting cert. 3–4 weeks.

4 — Learn the risk management methodology
Read ISO 31000 (risk management framework). Practice risk assessment with a fictional scenario — create a risk register, score risks, choose treatments. Many GRC platforms have free training. 2–3 weeks.

5 — Get hands-on with a GRC platform
ServiceNow GRC and Archer are the enterprise standards — both have free trial access. Practice building a risk register, managing control evidence and tracking audit findings. This differentiates you immediately from candidates with only theoretical knowledge. 2–3 weeks.

6 — Study PCI DSS and Cyber Essentials
These are the two most common compliance programmes you will encounter in UK GRC roles. Read the PCI DSS v4.0 requirements document (free from pcisecuritystandards.org). Complete the Cyber Essentials self-assessment. 2 weeks.

7 — Get your first certification
CISM (ISACA) for risk management focus. CISSP (ISC2) for breadth. ISO 27001 Lead Implementer for standard-specific depth. BCS Practitioner Certificate in Information Security Management is a respected UK entry-level qualification. Choose based on your target role.

8 — Build your portfolio and apply
Write a mock information security policy. Create a risk register for a fictional company. Write a DPIA for a hypothetical new product. These demonstrate GRC thinking in practice — not just knowledge of the theory. Share them on LinkedIn. Apply for junior GRC analyst roles.

Timeline from zero to first GRC role: 9–15 months.
If you already have a law, business or IT background: 6–9 months.
GRC has one of the shortest entry timelines of any cybersecurity specialism.

12. Certifications That Matter

GRC certifications carry significant weight — more so than in some technical roles — because they validate judgement and knowledge of legal and regulatory frameworks rather than just technical skill. Employers use them as a reliable screening criterion.

Certification	Level	Focus	Why It Matters
CompTIA Security+	Beginner	Broad security foundations — threats, controls, cryptography, compliance	Recommended baseline even for GRC. Demonstrates understanding of what the controls you manage actually do.
BCS Practitioner Certificate in IS Management	Beginner–Mid	UK-focused ISMS management — ISO 27001, risk, policy, legal requirements	Highly regarded by UK employers for junior to mid-level information security management roles.
CISM — Certified Information Security Manager	Mid–Senior	Information risk management, IS governance, incident management, programme development	One of the most respected GRC certifications globally. Strongly preferred for manager and head of security roles.
CISSP — Certified Information Systems Security Professional	Mid–Senior	Broad security management across 8 domains — risk, governance, architecture, operations	The gold standard of security management certifications. Opens senior and leadership doors.
ISO 27001 Lead Implementer	Mid	Designing and implementing an ISMS to ISO 27001 standard	Demonstrates practical ability to build and manage an ISMS. Often required for Head of GRC roles.
ISO 27001 Lead Auditor	Mid	Auditing an ISMS against ISO 27001	Required for internal and external auditor roles. Highly valued in consulting and assessment firms.
CRISC — Certified in Risk & Information Systems Control	Mid–Senior	IT risk and control management	Specifically focused on risk — ideal for risk manager career track. Pairs well with CISM.
BCS Foundation Certificate in Data Protection	Beginner	UK GDPR and data protection law fundamentals	Best starting point for a career track focused on data protection and DPO roles.
CDPO / CIPP/E — Certified Data Protection / Privacy Professional	Mid	EU/UK GDPR in depth — rights, legal bases, international transfers	Leading privacy professional certifications. Required or strongly preferred for DPO roles.

Table 10: GRC certifications in order of progression

13. Case Study — A GDPR Breach and Its Fallout

> This is a fictional case study based on common real-world GDPR incident patterns.
> It illustrates the GRC professional's role before, during and after a data breach.

The Organisation

Meridian HR Solutions is a mid-sized UK HR software company with 250 employees. They process personal data for over 400 client companies — including salary details, performance reviews, absence records and disciplinary histories for approximately 85,000 employees. They hold ISO 27001 certification and have a nominated Data Protection Officer, Claire, who also carries the title Head of GRC.

The incident — Tuesday, 3pm

15:00 — Phishing email lands in the HR Director's inbox

The HR Director, David, receives an email appearing to come from the company's CEO. It asks him to urgently authorise a payroll transfer by logging into a link. David clicks the link, enters his credentials, and receives an error message.

At 15:47, the IT team detects an unusual login to David's account from an IP address in Eastern Europe. The attacker has accessed the HR portal and exported a CSV file containing names, salaries and personal data for 12,400

The GRC team's immediate response

16:30 — Claire, the DPO, is notified

Claire's first question is not 'how did this happen?' — it is 'have we breached UK GDPR?' The answer is yes: personal data has been accessed by an unauthorised third party. The GDPR 72-hour notification clock starts now.

Claire immediately convenes a breach response team: IT, legal, communications and senior management. She activates the organisation's Data Breach Response Plan — a document she had written and tested six months earlier. Without it, the next 72 hours would be chaotic.

The 72-hour window

Time	Action	GRC / DPO Lead Activity
T+0 (15:47)	Breach detected by IT	Claire notified. Breach Response Plan activated.
T+2h	Scope confirmed	Claire drafts initial breach assessment — 12,400 individuals affected across 37 clients.
T+6h	Legal counsel engaged	Claire briefs external lawyers. Confirms ICO notification required.
T+18h	Client notification begins	Claire drafts client breach notification letters. Legal reviews.
T+36h	ICO notified	Claire submits breach notification to ICO via online portal within 72-hour window.
T+48h	Affected individuals notified	Letters sent to all 12,400 affected employees explaining what data was accessed.

Time	Action	GRC / DPO Lead Activity
T+72h	Interim report to board	Claire presents a formal incident report to the board with root cause, remediation plan and regulatory status.

Table 11: 72-hour GDPR breach response timeline

The ICO investigation and outcome

The ICO opened a formal investigation. Claire's thorough documentation — the breach notification filed within 72 hours, evidence of prior security measures (ISO 27001 certification, phishing awareness training records, MFA enforcement policy), and a clear remediation plan — worked significantly in the organisation's favour.

The ICO issued a **reprimand** rather than a fine — noting that while the breach had occurred, the organisation had appropriate policies in place, had responded promptly, had notified both the regulator and affected individuals within the required timeframe, and had proactively implemented further controls. Organisations that lack documentation and respond poorly typically face fines.

> **What saved Meridian HR Solutions from a significant fine:**
> A tested Data Breach Response Plan. ICO notification within 72 hours.
> Evidence of prior security measures. Transparent communication with clients.
> A competent, prepared DPO who owned the process from the first hour.

What the GRC team implemented afterwards

- Mandatory MFA enforced for all users accessing the HR portal — previously it was optional
- Phishing simulation programme introduced — quarterly simulated campaigns with mandatory retraining for those who click
- Data minimisation review — the exported CSV contained more fields than necessary; export permissions now restricted by role
- Client contract review — updated data processing agreements to clearly document notification obligations
- Tabletop incident response exercises — twice-yearly simulations of breach scenarios involving GRC, IT and legal

14. Breaking In — Getting Your First Role

GRC is genuinely one of the most accessible cybersecurity career paths. People enter it from legal backgrounds, business analysis, project management, IT, academia and internal audit. The common thread is not a technical degree but analytical thinking, clear writing and the ability to manage complexity.

Build visible evidence of GRC capability

- **Write a sample information security policy:** Pick a topic — acceptable use, remote working, password management — and write a professional policy document. This demonstrates you understand what policy writing actually involves
- **Create a sample risk register:** Take a fictional company and identify 10 information security risks. Score them by likelihood and impact. Recommend treatments. Format it properly. This is one of the most requested outputs in GRC interviews
- **Write a mock DPIA:** Pick a hypothetical new system that handles personal data and write a Data Protection Impact Assessment. This shows GDPR knowledge in practice, not just theory
- **Blog about a relevant topic:** Write about a recent ICO enforcement decision, a new GDPR guidance document, or the difference between ISO 27001 and Cyber Essentials. GRC employers value clear communication above almost anything else
- **Join the ISACA community:** ISACA has UK chapters with free or low-cost events, webinars and networking. The people in these rooms are exactly where you want to be

Where to Look	Notes
CyberSecurityJobs.com	Filter by 'GRC analyst', 'information security manager', 'compliance analyst', 'DPO'
LinkedIn	GRC roles post heavily. Join ISACA and (ISC)2 LinkedIn groups. Engage with content.
Public sector / NHS / Government	Public sector GRC roles are plentiful, entry-level accessible and provide structured training
Financial services	Banks, insurers and payment firms have dedicated GRC teams — highest salaries but most competitive
Compliance recruitment agencies	Badenoch & Clark, Barclay Simpson and Michael Page all specialise in GRC and IG placements
Internal audit departments	Many GRC professionals start in internal audit — strong pathway into IS risk management

Table 12: Where to find GRC and information security management roles

Interview questions to prepare for

- What is the difference between a risk and a vulnerability? Give an example of each.
- Walk me through how you would conduct an information security risk assessment.
- What are the seven principles of UK GDPR? Give an example of how one applies in practice.

- What does ISO 27001 certification mean for an organisation — and what does it not mean?
- A supplier tells you they are 'GDPR compliant'. What questions would you ask to verify this?
- We had a data breach last year. How would you approach improving our breach response capability?
- What is a Statement of Applicability and how is it used in an ISO 27001 implementation?
- How would you explain cyber risk to a board of directors who have no technical background?

The best GRC interview answer:
"Here is a risk register I prepared. Here is a policy I wrote."
Evidence of practical GRC thinking beats a list of certifications every time.

15. References

1. Barclay Simpson (2024) *GRC Salary Survey 2024.* Available at: https://www.barclaysimpson.com/salary-survey [Accessed: 10 April 2026].
2. BCS (2024) *Practitioner Certificate in Information Security Management.* Available at: https://www.bcs.org/qualifications-and-certifications/certifications-for-professionals/security-certifications [Accessed: 10 April 2026].
3. CW Jobs (2024) *Technology Salary Survey 2024.* Available at: https://www.cwjobs.co.uk/salary-checker [Accessed: 10 April 2026].
4. ICO (2024) *Guide to the UK GDPR.* Information Commissioner's Office. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ [Accessed: 11 April 2026].
5. ISACA (2024) *CISM and CRISC Certification Overview.* Available at: https://www.isaca.org/credentialing [Accessed: 11 April 2026].
6. ISO/IEC (2022) *ISO/IEC 27001:2022 — Information Security Management Systems.* Available at: https://www.iso.org/standard/27001 [Accessed: 12 April 2026].
7. ISO (2018) *ISO 31000:2018 — Risk Management Guidelines.* Available at: https://www.iso.org/iso-31000-risk-management.html [Accessed: 12 April 2026].
8. ISC2 (2024) *CISSP and CCSP Certification Overview.* Available at: https://www.isc2.org/certifications [Accessed: 12 April 2026].
9. NCSC (2024) *Cyber Essentials Scheme.* National Cyber Security Centre. Available at: https://www.ncsc.gov.uk/cyberessentials/overview [Accessed: 12 April 2026].
10. PCI Security Standards Council (2022) *PCI DSS v4.0.* Available at: https://www.pcisecuritystandards.org/document_library/ [Accessed: 13 April 2026].
11. Reed (2024) *Cybersecurity Salary Guide UK 2024.* Available at: https://www.reed.co.uk/career-advice/cybersecurity-salary [Accessed: 13 April 2026].
12. UK Government (2018) *The Network and Information Systems (NIS) Regulations 2018.* Available at: https://www.legislation.gov.uk/uksi/2018/506/contents [Accessed: 14 April 2026].

This is the final document in the Cybersecurity Career Series by Babashaheer.

Document 01 — Making a Career in Ethical Hacking
Document 02 — The Cybersecurity Career Tree
Document 03 — Digital Forensics & Incident Response
Document 04 — Network Security
Document 05 — Cloud Security
Document 06 — Governance, Risk & Compliance (this document)

This is Document 09 in the Cybersecurity Career Series by Babashaheer.

Document 01 — Ethical Hacking | Document 02 — Career Tree | Document 03 — DFIR
Document 04 — Malware Analysis | Document 05 — Network Security | Document 06 — AppSec
Document 07 — Cloud Security | Document 08 — SOC / Blue Team | Document 09 — GRC (this document)
Document 10 — Threat Intelligence | Document 11 — OT/ICS/SCADA | Document 12 — IAM

Document prepared by Babashaheer. Version 1.0 — April 2026. Cybersecurity Career Series — Document 09 of 12.