INSTANT DOWNLOAD

EMPOWER YOUR CYBER GRC CAREER OR PROGRAM: ONE TOOLKIT AT A TIME

FREE CYBER GRC TOOLKIT

SkillWeed

WHAT'S INSIDE THE TOOLKIT?

A complete starter-to-pro-level bundle that equips you with tools, guides, templates, and checklists to confidently manage cyber risks, ensure compliance, and build a winning GRC strategy.

CONTENTS

WHO IS THIS TOOLKIT FOR?

- Aspiring Cyber GRC Analysts
- Current GRC Professionals
- Cybersecurity Students
- Compliance Managers
- Business Owners & Startups
- Consultants & Trainers

HOW TO USE THE TOOLKIT

- Step-by-step guide on applying tools
- Suggested weekly plan to build skills
- Guidance on customizing templates for your organization

TOOLKIT USE CASES

- Build your cyber GRC portfolio
- Conduct a self-assessment of your business
- Prepare for your first GRC job
- Train your internal GRC team
- Audit-readiness for HIPAA or ISO 27001

CYBER GRC JUMPSTART GUIDE

Kickstart Your Governance, Risk, and Compliance
Career or Program with Confidence

1. WHAT IS CYBER GRC?

Cyber GRC stands for **Cyber Governance, Risk, and Compliance**—a strategic framework that ensures organizations manage information security risks effectively, comply with regulatory requirements, and align cybersecurity activities with business goals.

At its core, Cyber GRC is about:

- **Governance**: Defining responsibilities, policies, and decision-making processes.
- **Risk Management**: Identifying, analyzing, and responding to cyber threats and vulnerabilities.
- **Compliance**: Meeting legal, regulatory, and contractual security obligations.

> *"Cyber GRC turns chaos into clarity. It connects policies to practice, risks to reality, and frameworks to execution."*

2. CYBER GRC ROLES & CAREER ROADMAP

Cyber GRC is one of the fastest-growing cybersecurity career paths. Whether you're entering from IT, audit, compliance, or business, there's a roadmap for you.

CORE CYBER GRC ROLES:

Role	Description
GRC Analyst	Conducts assessments, maintains risk registers, supports audits
Risk Manager	Leads risk assessments, develops mitigation plans
Compliance Officer	Ensures adherence to regulations (HIPAA, PCI, etc.)
Policy & Governance Specialist	Develops and maintains policies & frameworks
Audit Coordinator	Manages internal and external audits and documentation
Third-Party Risk Analyst	Evaluates vendor risks and contractual security compliance

CAREER ROADMAP EXAMPLE:

1. **Entry-Level**: IT Support → Compliance Assistant → GRC Intern
2. **Mid-Level**: GRC Analyst → Risk Manager or Compliance Lead
3. **Advanced**: GRC Program Manager → Director of Risk → CISO

Certifications that can help: CISA, CRISC, ISO 27001 Lead Implementer, CGEIT, CompTIA Security+ (entry), and CISSP (advanced).

3. KEY CYBERSECURITY FRAMEWORKS TO KNOW

A strong GRC program relies on adopting and aligning with proven frameworks. These frameworks guide how you manage risk, protect assets, and stay compliant.

TOP FRAMEWORKS YOU MUST KNOW:

Framework	Purpose	Best Used In
NIST CSF	Risk-based cybersecurity control structure	Government, SMEs, critical infrastructure
ISO 27001	International standard for information security	Global companies, supply chain partners
PCI-DSS	Protects cardholder data and payments	Retail, eCommerce, finance
HIPAA	Safeguards health data privacy and security	Healthcare providers and partners
SOC 2	Assurance on data controls (Security, Privacy, Availability)	SaaS companies, tech firms, service providers

🧭 *Your job as a GRC professional is to determine which frameworks apply, how to align controls, and how to document evidence of compliance.*

4. SAMPLE GRC WORKFLOWS

Here are two critical workflows every GRC practitioner should understand and implement.

A. RISK REGISTER WORKFLOW

1. **Identify**: Assets, threats, vulnerabilities
2. **Assess**: Likelihood × Impact = Risk Score
3. **Mitigate**: Define controls and response plan
4. **Monitor**: Periodic reviews and status updates
5. **Document**: Track ownership, status, and evidence

🎯 *Tool: Use a spreadsheet or platform like RiskRhino, Archer, or LogicGate.*

B. CONTROL MAPPING WORKFLOW

1. **Select Framework**: (e.g., NIST CSF or ISO 27001)
2. **List Controls**: Define required controls
3. **Map to Policies**: Connect control to existing or needed policy
4. **Assign Ownership**: Link each control to an individual/team
5. **Track Maturity**: Evaluate if the control is documented, implemented, and monitored

Pro Tip: Mapping across frameworks (e.g., NIST CSF to CIS v8) helps unify audits and reduce duplication.

CONCLUSION: YOU'RE NOW GRC-READY

The Cyber GRC Jumpstart Guide is your springboard into the world of security governance, risk, and compliance. Whether you're building a career or launching a program, mastering the roles, frameworks, and workflows above is foundational.

TOP 10 CYBERSECURITY FRAMEWORKS CHEAT SHEET

"The Ultimate Snapshot of the Most Important Frameworks Every GRC Professional Must Know"

WHY FRAMEWORKS MATTER

Cybersecurity frameworks provide **standardized structures** for managing risk, protecting assets, and ensuring compliance across industries. They form the **backbone of any Governance, Risk, and Compliance (GRC)** program.

🎯 *Think of frameworks as blueprints—they tell you what to do, not necessarily how to do it.*

TOP 10 CYBERSECURITY FRAMEWORKS YOU SHOULD KNOW

#	Framework	Purpose	Best For	Compliance Type
1	**NIST CSF (Cybersecurity Framework)**	A flexible, risk-based framework for improving cyber resilience	SMEs, critical infrastructure, U.S. businesses	Voluntary, but widely adopted
2	**ISO/IEC 27001**	International standard for establishing an Information Security Management System (ISMS)	Multinationals, global supply chains	Certifiable
3	**PCI DSS**	Protects credit cardholder data and secures payment systems	Retail, fintech, eCommerce	Mandatory for payment processors
4	**SOC 2 (Trust Services Criteria)**	Audits for security, availability, processing integrity, confidentiality, and privacy	SaaS providers, cloud-based firms	Attestation audit
5	**HIPAA**	Ensures the privacy and security of personal health information	Healthcare providers and partners	U.S. federal law
6	**NIST 800-53**	A deep catalog of security controls for federal information systems	Government, contractors, regulated sectors	Mandatory for federal use
7	**NIST 800-171**	Safeguards Controlled Unclassified Information (CUI) in non-federal systems	Defense contractors, research orgs	DFARS requirement
8	**COBIT**	Focuses on IT governance and management	CIOs, IT auditors, enterprise architects	Strategic framework
9	**CIS Controls v8**	18 prioritized security best practices (formerly 20)	SMEs, GRC newcomers, technical teams	Voluntary, action-based
10	**GDPR**	Governs the privacy and protection of personal data for EU citizens	Any business handling EU data	Mandatory, legal regulation

QUICK COMPARISON MATRIX

Framework	Risk-Based	Technical Controls	Privacy Focus	Certification Possible
NIST CSF	✅	⚠️ Limited	⚠️ Partial	❌
ISO 27001	✅	✅	⚠️ Optional	✅
PCI-DSS	✅	✅	❌	✅
SOC 2	✅	✅	✅	✅
HIPAA	✅	✅	✅	❌
NIST 800-53	✅	✅	✅	❌
NIST 800-171	✅	✅	✅	❌
COBIT	✅	⚠️ High-Level	❌	❌
CIS Controls	✅	✅	❌	❌
GDPR	✅	❌	✅	❌ (but legal requirement)

PRO TIPS FOR GRC PROFESSIONALS

- **NIST CSF + CIS Controls** is a great combo for small-to-midsize businesses.
- **ISO 27001** is ideal for companies that want global recognition or certification.
- **SOC 2** is critical for SaaS companies working with B2B clients.
- **HIPAA + NIST 800-66** pairing is perfect for healthcare environments.
- Use **COBIT** for board-level conversations about cyber risk and IT alignment.

HOW TO CHOOSE THE RIGHT FRAMEWORK

Ask these key questions:

1. Do we need a **certification** (e.g., ISO 27001)?
2. Are we in a **regulated industry** (e.g., healthcare, finance)?
3. Are we handling **global data** (GDPR, CCPA)?
4. Do we need **quick wins** or a **comprehensive system**?
5. Who is the **audience**? (Tech team, board, regulators?)

CYBER RISK ASSESSMENT TEMPLATE GUIDE

"Easily Identify, Score, and Mitigate Cyber Risks Using a Proven Template"

OVERVIEW

The **Cyber Risk Assessment Template** is your go-to tool for evaluating and managing cybersecurity threats. It enables GRC professionals, IT teams, and business leaders to **quantify risks**, prioritize mitigation efforts, and track residual risk over time.

> *"What gets measured gets managed—and this template helps you measure risk with clarity and confidence."*

WHAT'S INCLUDED IN THE DOWNLOAD

You'll receive:

- ✅ **Editable Excel File** – Pre-built with dropdowns, scoring logic, and automation
- ✅ **PDF Version** – For print-and-use or internal reference
- ✅ **NIST CSF Sample** – A fully pre-filled example showing how to score and mitigate a risk using the NIST Cybersecurity Framework

TEMPLATE FEATURES AT A GLANCE

Feature	Description
Risk Scoring Matrix	Likelihood × Impact = Risk Score (1–25 scale)
Pre-Filled Sample	Includes risks aligned with NIST CSF Functions (Identify, Protect, Detect, Respond, Recover)
Editable Fields	Asset, Threat, Vulnerability, Impact, Likelihood, Risk Owner, Mitigation
Drop-down Lists	Standardized scoring options (e.g., Likelihood: Rare to Almost Certain; Impact: Low to Critical)
Risk Heatmap-Ready	Easily plug values into a heatmap chart for visual risk analysis

UNDERSTANDING THE SCORING MODEL

1. LIKELIHOOD SCORE (1–5)

Score	Rating	Example
1	Rare	No known incidents, highly unlikely
3	Possible	Could occur occasionally
5	Almost Certain	Expected in most environments

2. IMPACT SCORE (1–5)

Score	Rating	Example
1	Low	Minor inconvenience, no data loss
3	Moderate	Partial data exposure, limited downtime
5	Critical	Major data breach, legal/regulatory impact, public trust loss

3. RISK SCORE = LIKELIHOOD × IMPACT

Risk Score	Risk Level
1–4	Low
5–9	Medium
10–15	High
16–25	Critical

SAMPLE USE CASE: NIST CSF MAPPING

Let's say you're assessing **PR.AC-1 (Identities and credentials are issued, managed, and revoked properly)**.

Field	Example
Asset	Identity and Access Management System
Threat	Compromised credentials
Vulnerability	Weak password policy
Impact	5 (Critical – could lead to full access)
Likelihood	4 (Likely – due to no MFA)
Risk Score	20 (Critical)
Mitigation Plan	Enforce MFA, update password policy, conduct training
Risk Owner	IAM Manager

COLUMNS INCLUDED IN THE TEMPLATE

Column Name	Purpose
Asset	What's at risk (system, data, service)
Threat	What could exploit the vulnerability
Vulnerability	The weakness being exploited
Likelihood	Chance of occurrence (1–5)
Impact	Severity of outcome (1–5)
Risk Score	Auto-calculated (L × I)
Risk Level	Low, Medium, High, Critical
Mitigation Plan	Steps to reduce risk
Residual Risk	Risk after mitigation
Owner	Person accountable for action
Status	Open, Mitigated, Accepted, etc.

WHY THIS TEMPLATE IS A MUST-HAVE

- 💼 Used by cybersecurity analysts, GRC teams, and auditors
- 🔁 Repeatable for vendor risk, internal assessments, and compliance audits
- 📊 Clear visibility into top risks and mitigation priorities
- 💡 Beginner-friendly yet professional-grade

CONTROL MAPPING TEMPLATE GUIDE

"Easily Align ISO 27001 Controls to NIST CSF and CIS Controls with This Editable Tool"

WHAT IS CONTROL MAPPING?

Control mapping is the practice of **aligning security controls across different cybersecurity frameworks** to:

- Avoid duplication of effort
- Ensure comprehensive coverage
- Streamline audits and assessments
- Support unified reporting and governance

> *"Mapping controls helps you speak multiple compliance languages at once."*

KEY FRAMEWORKS IN THE MAPPING

Framework	Description
ISO/IEC 27001:2022	Global standard for information security management systems (ISMS)
NIST CSF 2.0	U.S. Cybersecurity Framework focusing on 6 core functions
CIS Controls v8	Prioritized set of 18 security actions for cyber defense

HOW MAPPING WORKS

ISO 27001 Control	Mapped To	Notes
A.5.1: Policies for Information Security	NIST CSF: GV.PO-01	Aligns with Governance function (Policies established and communicated)
A.9.2.3: Management of Privileged Access Rights	CIS Control 5.3	Requires tracking and limiting administrative privileges
A.12.6.1: Management of Technical Vulnerabilities	NIST CSF: ID.RA-1, PR.IP-12	Supports risk assessment and mitigation planning
A.16.1.1: Responsibilities and Procedures	NIST CSF: RS.RP-01	Response planning and escalation protocols

TEMPLATE COLUMNS & STRUCTURE

Column Name	Description
ISO 27001 Clause	The original control identifier (e.g., A.5.1.1)
ISO Control Description	Summary of the control requirement
NIST CSF Function/Subcategory	Mapped equivalent under NIST CSF (e.g., PR.AC-1)
CIS Control	Corresponding CIS Control (e.g., 4.2 or 16.1)
Control Owner (Editable)	Department or person responsible
Implementation Status	Planned, In Progress, Complete
Best Practice Guidance	Tips and examples for implementing the control
Notes	Room for internal comments or auditor feedback

BENEFITS OF USING THIS MAPPING TEMPLATE

- 🗒️ **Unify Audits**: Use one spreadsheet for ISO, NIST, CIS reviews
- 🔍 **Find Gaps Fast**: See where one framework lacks coverage
- 🧠 **Train Teams Easily**: One view for multiple roles and requirements
- 🔁 **Update-Friendly**: Editable format means easy customization
- 🧪 **Supports Assessments**: Use as a base for internal maturity scoring

BEST PRACTICES FOR USING THE MAPPING

1. **Start with your primary compliance framework** (e.g., ISO 27001).
2. **Map only applicable controls** – some may not be relevant to your environment.
3. **Use filters** to focus on domains like Access Control, Incident Response, or Data Protection.
4. **Assign ownership** for implementation and tracking.
5. **Update status** regularly to support audits and risk reporting.
6. **Add cross-links** to your policy and procedure documents for traceability.

"When controls are mapped, risk becomes measurable and compliance becomes manageable."

POLICY & PROCEDURE TEMPLATES GUIDE

"Foundational Documents for Building a Robust Cybersecurity Program"

OVERVIEW

Well-crafted cybersecurity policies and procedures are the backbone of any effective Governance, Risk, and Compliance (GRC) program. They:

- Define **organizational expectations**
- Guide **day-to-day operations**
- Support **regulatory compliance**
- Help prepare for **audits and certifications**

> *"Without documentation, security is just hope. These templates give you a structured place to start."*

Template Name	Description	Use Case
✅ **Information Security Policy**	Sets the overall tone and strategic direction for cybersecurity in the organization	Required for ISO 27001, NIST CSF, and SOC 2 readiness
✅ **Access Control Policy**	Outlines rules for granting, managing, and revoking access to systems and data	Supports least privilege, user provisioning, and MFA enforcement
✅ **Incident Response Policy**	Provides a framework for detecting, reporting, containing, and recovering from security incidents	Core for HIPAA, NIST 800-61, and tabletop exercises
✅ **Vendor Risk Management Policy**	Establishes guidelines for onboarding, monitoring, and offboarding third-party vendors	Critical for SOC 2, ISO 27036, and TPRM programs

WHAT'S INSIDE EACH TEMPLATE

Each policy includes:

- 📌 **Purpose and Scope**
- 👤 **Roles and Responsibilities**
- 🔐 **Applicable Controls**
- 🔄 **Process Workflow**
- 📊 **Monitoring & Review**
- 📚 **References to Frameworks (ISO, NIST, CIS, etc.)**
- ✅ **Editable Placeholders** for company name, roles, and toolsets

SAMPLE POLICY SNAPSHOT: INFOSEC POLICY

1.0 Purpose

This Information Security Policy defines how [Company Name] will protect its information assets from threats to ensure business continuity, minimize risk, and ensure compliance.

2.0 Scope

Applies to all employees, contractors, systems, and third-party service providers.

3.0 Responsibilities

- CISO: Owns the policy
- IT Manager: Implements controls
- Employees: Comply with acceptable use standards

4.0 Policy Statements

- All data must be classified per the Data Classification Policy
- Access must be based on least privilege
- MFA is mandatory for all remote access
- Quarterly access reviews are required

5.0 Enforcement

Non-compliance may result in disciplinary action.

HOW TO USE THE TEMPLATES

1. **Customize the placeholders** (company name, contact roles, system references)
2. **Align with your selected framework** (use Control Mapping Template from Toolkit)
3. **Review with stakeholders** (legal, IT, HR, Compliance)
4. **Train your team** on the finalized policies
5. **Monitor and update annually** or after major incidents

BEST PRACTICES FOR POLICY MANAGEMENT

- Keep policies **concise, actionable, and accessible**
- Link policies to **specific controls** (e.g., NIST CSF PR.AC-1 → Access Control Policy)
- Store in a **version-controlled, centralized repository**
- Require **read-and-acknowledge** tracking for employees
- Use policies as **baseline evidence during audits**

"Auditors don't just want to see your policies—they want to see that you're living them."

CYBERSECURITY MATURITY ASSESSMENT TOOL GUIDE

"Measure What Matters – Know Where You Stand. Plan Where to Go."

OVERVIEW

The **Cybersecurity Maturity Assessment Tool** helps you quickly assess how mature your organization's cybersecurity program is across core domains—**Access Control**, **Incident Response**, **Privacy**, and more.

It uses a **CMMI-based scoring system (1–5 scale)** to measure the **documentation, implementation, consistency, and optimization** of your controls.

> *"Maturity is not about being perfect. It's about knowing where you are and how to level up strategically."*

SCORING MODEL: CMMI-BASED LEVELS

Score	Maturity Level	Meaning
1	**Initial (Ad Hoc)**	No formal process, reactive approach
2	**Repeatable (Basic)**	Processes exist but are inconsistent or undocumented
3	**Defined (Standardized)**	Documented and consistent processes across the org
4	**Managed (Measured)**	Controls are monitored and reviewed regularly
5	**Optimized (Continual Improvement)**	Processes are refined through feedback and innovation

CORE DOMAINS COVERED

Domain	Sample Control Areas
Access Control	Role-based access, MFA, least privilege
Incident Response	IR plan, tabletop exercises, breach reporting
Privacy	Consent, data minimization, data subject rights
Asset Management	Inventory, classification, ownership
Risk Management	Risk register, scoring, mitigation tracking
Vulnerability Management	Scanning, patching, remediation SLAs
Vendor Security	Due diligence, contracts, assessments
Data Protection	Encryption, backup, DLP tools

HOW IT WORKS

1. **Rate each control area** from 1 to 5 using the definitions provided.
2. **Auto-calculate average scores** by domain.
3. **Identify gaps** using built-in conditional formatting (e.g., red = ≤2).
4. **Use the prioritization tab** to flag high-risk, low-maturity areas.
5. **Generate visuals** (bar charts or radar plots) for reporting to leadership.

SAMPLE OUTPUT SNAPSHOT

Domain	Avg Score	Risk Level	Priority	Action Plan
Access Control	2.3	Medium	Short Term	Implement centralized IAM and MFA
Incident Response	4.0	Low	Long Term	Maintain current processes and train annually
Privacy	1.7	High	Immediate	Develop privacy policy, appoint DPO
Risk Management	3.5	Medium	Mid Term	Automate risk scoring dashboard

BENEFITS OF THIS TOOL

- 🧭 **Know where you stand** – instantly visualize your current posture
- 📈 **Track improvement** over time with quarterly or annual assessments
- 🧠 **Make strategic decisions** based on actual data
- 🛠️ **Tailor remediation efforts** by priority, not assumptions
- 🎯 **Support certification readiness** (ISO 27001, SOC 2, etc.)

"Leaders don't manage what they don't measure. This tool creates visibility that leads to maturity."

COMPLIANCE CHECKLISTS GUIDE

"Step-by-Step Checklists for HIPAA, PCI-DSS, NIST, and SOC 2 Readiness"

OVERVIEW

This module provides **simple, clear, and actionable checklists** to help your organization assess its compliance posture and close critical gaps across key regulations and standards:

- **HIPAA** – Healthcare data privacy & security
- **PCI-DSS** – Payment card data protection
- **NIST 800-53/800-171** – Federal system & contractor security controls
- **SOC 2** – Assurance for service organizations

> *"Compliance doesn't start with tools. It starts with checklists. These guides break complexity into action."*

1. HIPAA READINESS CHECKLIST

Covers all three HIPAA safeguard categories:

Safeguard	Sample Checklist Items
Administrative	✅ Security Officer assigned ✅ Risk assessment conducted ✅ Workforce training completed
Technical	✅ Access controls defined ✅ Audit controls implemented ✅ Data encrypted in transit and at rest
Physical	✅ Facility access controls ✅ Device/media disposal policy ✅ Secure workstation practices

2. PCI-DSS GAP CHECKLIST

Covers all 12 PCI-DSS requirement groups:

Req. #	Focus Area	Example
1	Install & maintain a firewall	Documented rules for inbound/outbound traffic
3	Protect stored cardholder data	Tokenization or strong encryption used
10	Track & monitor all access	Logging enabled on all systems handling CHD

Includes:

- ❗ Gap severity column (None, Partial, High)
- 📎 Evidence required column
- 👤 Owner & due date fields

3. NIST 800-53 & 800-171 QUICK ASSESSMENT GUIDE

This mini-guide helps you quickly assess your alignment with two foundational federal standards.

Control Family	Focus	Sample Controls
Access Control (AC)	User permissions	AC-2: Account management
Risk Assessment (RA)	Risk evaluation	RA-3: Risk assessment update
System & Comm. Protection (SC)	Encryption, boundaries	SC-12: Cryptographic key establishment

Self-Scoring Scale (1–5):
1 = Not Started
2 = Initial Awareness
3 = In Progress
4 = Implemented
5 = Fully Documented & Tested

4. SOC 2 READINESS MINI CHECKLIST

Covers the 5 Trust Services Criteria:

Criteria	Sample Questions
Security	Do you have firewalls and intrusion detection?
Availability	Do you monitor uptime and recovery?
Processing Integrity	Are systems accurate and timely?
Confidentiality	Are encryption and access restrictions applied?
Privacy	Do you collect, store, and use data lawfully?

Includes:

- 📝 Evidence column for each domain
- 🚦 Traffic light status (Red/Yellow/Green)
- 📌 Notes section for audit prep

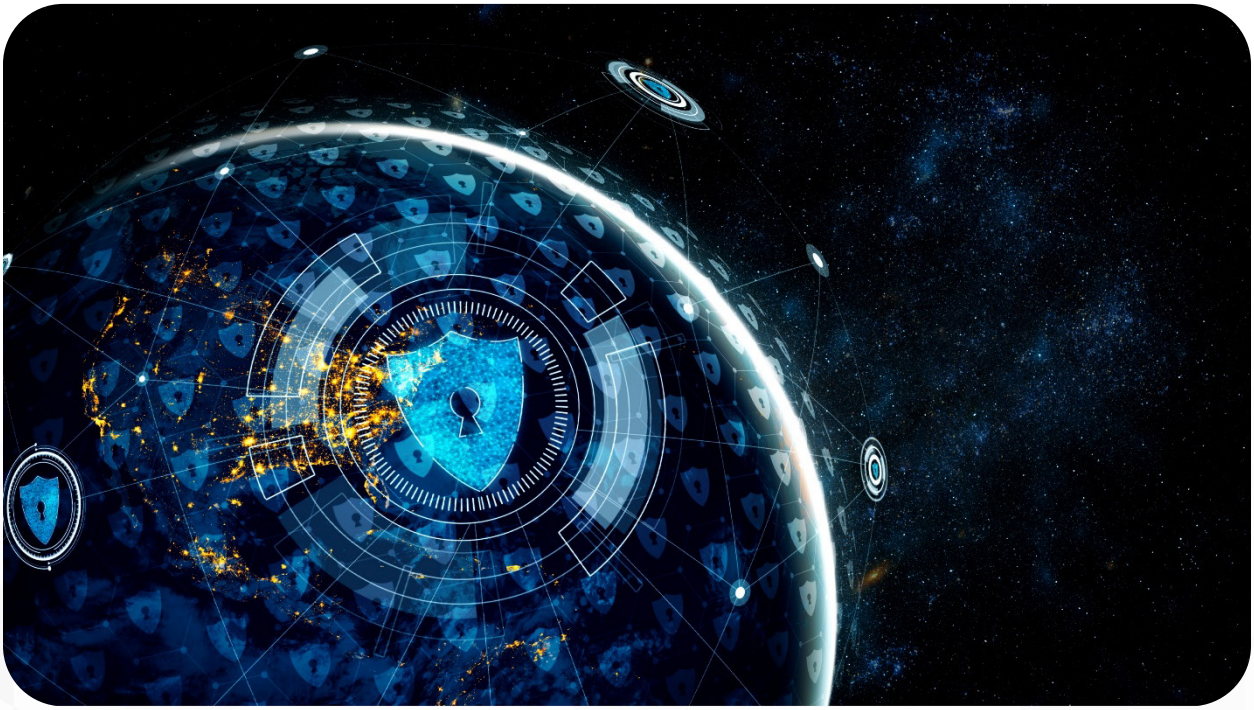
HOW TO USE THESE CHECKLISTS

1. **Download and customize** based on your environment
2. **Assign responsibility** for each item to owners
3. **Conduct internal review** or pre-audit walkthroughs
4. **Track progress** using checklist status (Not Started → In Progress → Complete)
5. **Attach evidence** directly or via linked documentation

"Auditors love organized documentation. These checklists help you speak their language."

THIRD-PARTY RISK MANAGEMENT (TPRM) TOOLKIT GUIDE

"Control the Risk. Empower the Business. Master Your Vendor Ecosystem."



OVERVIEW

Third-party vendors can be your greatest enablers—or your biggest cybersecurity threat. This **TPRM Toolkit** helps you evaluate, onboard, monitor, and manage vendors **systematically and securely**.

Whether you're a small business or an enterprise, this toolkit simplifies the process with:

- Visual lifecycle
- Templates
- Scorecards
- Risk tiering models

"You can outsource the service—but not the risk. TPRM helps you manage both."

TPRM LIFECYCLE VISUAL

Visually map the entire process from procurement to offboarding:

1. Vendor Request →
2. Due Diligence →
3. Risk Assessment →
4. Contracting & Controls →
5. Onboarding →
6. Continuous Monitoring →
7. Offboarding & Data Disposal

SAMPLE VENDOR RISK QUESTIONNAIRE

Ask the right questions before onboarding any third-party. The editable template includes over **30 questions** across the following categories:

Category	Sample Questions
Security	Do you encrypt data in transit and at rest?
Privacy	Do you have a Data Processing Agreement (DPA)?
Compliance	Are you compliant with ISO 27001, SOC 2, HIPAA, etc.?
Access Control	How is access to our data restricted and monitored?
Incident Response	What is your breach notification timeline?
Business Continuity	Do you have a disaster recovery plan?

Use this questionnaire during onboarding, annual reviews, or audits.

VENDOR SCORECARD TEMPLATE

Evaluate vendors **objectively and consistently** using this weighted scorecard:

Domain	Weight	Sample Metric	Scoring Range
Security Controls	30%	Encryption, patching, firewall use	1–5
Compliance Alignment	20%	Frameworks adhered to (ISO, NIST)	1–5
SLA & Uptime	15%	Uptime guarantee & penalties	1–5
Support Quality	10%	Response time and resolution	1–5
Privacy Practices	25%	DSR process, consent management	1–5

Outputs:

- Final risk score (0–100)
- Score interpretation: Low, Medium, High risk
- Customizable color-coded risk flags

📊 Use this scorecard to make onboarding decisions or monitor existing vendor health.

RISK TIERING GUIDE

Not all vendors carry equal risk. This guide helps you **categorize vendors into risk tiers** for prioritized oversight.

Tier	Criteria	Oversight Needed
High Risk	Handles sensitive data, critical operations, or customer-facing platforms	Full security assessment + quarterly reviews
Medium Risk	Internal tools or partial access to data	Standard due diligence + annual reassessment

HOW TO USE THIS TOOLKIT

1. **Start with the lifecycle visual** – understand the process
2. **Use the vendor questionnaire** to assess risks before contracts
3. **Score vendors** using the objective, weighted template
4. **Assign risk tiers** and define monitoring frequency
5. **Track status** across all vendors in a simple dashboard

"Effective TPRM isn't just about avoiding breaches—it's about building secure partnerships."

INCIDENT RESPONSE PLAN QUICK BUILDER

"Respond Fast. Recover Smarter. Minimize Impact."

OVERVIEW

Cyber incidents are no longer a matter of *if*—but *when*. This **Incident Response (IR) Quick Builder** gives you a battle-tested, easy-to-follow playbook to build or refine your IR process **in one day**.

THE 7-STEP INCIDENT RESPONSE PLAN TEMPLATE

Step	Action
1 **Preparation**	Policies, tools, training, contacts list
2 **Identification**	Detect & confirm incident (SIEM, logs, alerts)
3 **Containment**	Short-term: isolate systems; long-term: block reentry
4 **Eradication**	Remove malware, compromised accounts, backdoors
5 **Recovery**	Restore from backups, monitor systems, re-enable access
6 **Lessons Learned**	Conduct post-incident review, root cause analysis
7 **Documentation**	Log timeline, decisions, actions, and evidence for audit

Each step comes with pre-written guidance and editable sections.

ROLES & RESPONSIBILITIES MATRIX

Assign clear accountability using **RACI (Responsible, Accountable, Consulted, Informed)** designations.

Role	Responsibility	R A C I
CISO	Owns IR policy and reporting	A
SOC Analyst	Detects, investigates, escalates	R
IT Manager	Containment and recovery	R
Legal Counsel	Privacy breach evaluation, regulatory reporting	C
Communications Lead	Drafts and approves public/internal messages	R/C
HR	Handles insider threats or personnel issues	C/I
Department Heads	Informed of incidents affecting operations	I

COMMUNICATION TEMPLATES

Clear, fast communication during a crisis is essential. This pack includes:

📩 **Internal Notification Sample (Email)**

Subject: URGENT: Cybersecurity Incident – Immediate Attention Required
Dear Team,
We are currently investigating a potential security incident affecting [department/system]. Please do not take any action unless directed. A follow-up update will be sent within 30 minutes.

📣 **External Notification Sample (Client/Partner)**

Subject: Security Incident Notification
We have identified and contained a security incident involving [general system type, e.g., user login portal]. At this time, no data loss has been confirmed. We are taking all steps to ensure transparency and will follow up with more details shortly.

PHISHING INCIDENT SIMULATION (SAMPLE SCENARIO)

You'll receive a **pre-built tabletop simulation** for phishing attacks:

Simulation Element	Description
Attack Description	Employee received a fake HR email and clicked a malicious link
Discovery Point	Alert from SIEM flagged unusual outbound traffic
Incident Impact	Access token stolen, privilege escalation attempt
IR Actions	Account disabled, logs reviewed, phishing alert sent to staff
Lessons Learned	Need MFA for internal tools and phishing awareness refresh

Also includes:

- ✅ Timeline for facilitator
- ✅ Staff response cards
- ✅ Incident logging sheet

🎯 *Use this in training or tabletop exercises to test team readiness.*

> *"A good plan is a competitive advantage. A great response is a reputational lifesaver."*

BEST PRACTICE TIPS

- Update contact info quarterly
- Conduct IR tabletop exercises twice a year
- Ensure all team members understand the escalation path
- Link your IR Plan to your BCP/DR Plan for full resilience

AUDIT READINESS GUIDE

"Be Prepared. Stay Compliant. Pass With Confidence."

OVERVIEW

Whether you're facing an internal audit, external certification (e.g., ISO 27001, SOC 2), or regulatory review (HIPAA, PCI-DSS), being **audit-ready** means your documentation, processes, and controls are **consistent, verifiable, and defensible**.

This guide includes:

- ✅ Step-by-step GRC audit prep checklist
- ✅ Clear distinction between internal vs external audit roles
- ✅ Editable **Evidence Collection Templates** for controls and domains

"You don't prepare for an audit the week it starts—you prepare year-round."

STEP-BY-STEP GRC AUDIT PREPARATION

Step	Action
1	Review the scope of the audit (framework, systems, timeframe)
2	Identify applicable controls (based on NIST, ISO, SOC 2, etc.)
3	Assign owners for each control area (see Roles chart)
4	Collect and validate evidence (use provided templates)
5	Conduct a mock internal audit or walkthrough
6	Review prior audit findings and remediation status
7	Organize and label documents for easy access
8	Prepare your team with a pre-audit briefing
9	Maintain a central audit folder (digital + secure backup)

INTERNAL VS EXTERNAL AUDIT ROLES

Role	Internal Audit	External Audit
CISO	Approves policies, aligns strategy	Primary executive point of contact
Compliance Officer	Ensures control implementation	Provides evidence and answers questions
Control Owner	Executes daily/weekly control activities	Shares logs, policies, reports
Audit Lead/PM	Coordinates tasks and timelines	Supports external auditor with responses
IT/Admin Teams	Provide technical evidence	Demonstrate tool configurations or logs
Auditor	Internal: evaluates gaps	External: validates control effectiveness

Use this table to prepare roles and responsibilities before audit kickoff.

EVIDENCE COLLECTION TEMPLATE (SAMPLE STRUCTURE)

Domain	Control ID	Description	Evidence Required	Owner	Status	Last Updated
Access Control	AC-01	Enforce least privilege	User access review logs, role documentation	IT Manager	In Progress	08/01/2025
Incident Response	IR-02	IR Plan implemented	IR plan doc, tabletop summary, alert logs	CISO	Complete	07/22/2025
Vendor Risk	VR-04	Vendor due diligence	Questionnaire, risk scorecard, DPA	Procurement	Complete	07/15/2025

TIPS FOR A SUCCESSFUL AUDIT

- Keep policies version-controlled and accessible
- Store logs and system evidence with retention in mind (90–365 days+)
- Schedule internal control reviews **before** external audits
- Maintain an **Audit Readiness Binder** (digital + physical)
- Learn from each audit and update your **Audit Playbook**

COMMON EVIDENCE REQUESTS BY FRAMEWORK

Framework	Common Requests
ISO 27001	Risk treatment plan, ISMS scope, control mapping
SOC 2	Change management logs, onboarding/offboarding process
HIPAA	Risk analysis, BAAs, training records
PCI-DSS	Network segmentation diagram, quarterly scans
NIST 800-171	SSP, POAM, multi-factor access records

Use this reference to prepare your documents by compliance type.

CYBER GRC CAREER PREP PACK

"From Zero to Hired: Land Your Dream GRC Role with Confidence"

OVERVIEW

Cyber Governance, Risk, and Compliance (GRC) roles are in high demand, but **breaking in and standing out** requires more than just certifications.

This Career Prep Pack equips you with:

- ✅ A **Sample GRC Resume** that gets noticed
- ✅ Top **15 Interview Questions with Model Answers**
- ✅ A **LinkedIn Optimization Checklist** to position yourself as a GRC expert
- ✅ A curated list of **must-have GRC Certifications** to accelerate your career

> *"It's not just about being qualified—it's about being visible, credible, and ready."*

SAMPLE GRC RESUME TEMPLATE

Section	Key Elements
Professional Summary	2–3 lines highlighting GRC expertise and value proposition
Core Competencies	Bullet points for Risk Assessment, Compliance Audits, Control Mapping, TPRM, Policy Development
Professional Experience	STAR-format bullets showing achievements (e.g., "Reduced vendor onboarding time by 30% through streamlined due diligence process")
Certifications	CISA, ISO 27001 Lead Implementer, Security+
Tools & Frameworks	RiskRhino, Archer, ISO 27001, NIST CSF, SOC 2
Education	Degree + ongoing training/courses

☑ *Includes resume keywords to beat ATS filters for GRC roles.*

TOP 15 CYBER GRC INTERVIEW QUESTIONS & MODEL ANSWERS

Question	Sample Answer Snippet
1. Can you explain what GRC means to you?	GRC is about aligning governance frameworks, managing risk proactively, and ensuring compliance to protect business value.
2. How do you conduct a risk assessment?	I identify assets, assess threats/vulnerabilities, score risk (impact × likelihood), and propose mitigations.
3. What's your experience with NIST CSF or ISO 27001?	I've performed gap assessments, mapped controls, and developed POAMs for ISO 27001 readiness.
4. How would you handle a failed audit finding?	Conduct root cause analysis, update the risk register, and develop a CAPA (Corrective Action Plan).
5. How do you manage third-party vendor risks?	Through vendor questionnaires, tiering models, and periodic reassessments linked to SLAs.
6. What GRC tools are you familiar with?	I've used RiskRhino for risk registers and control tracking, as well as GRC modules in Archer.
7. How do you ensure policies stay aligned with regulations?	Quarterly policy reviews against updated frameworks and cross-team collaboration.
8. Describe a time you built a compliance program from scratch.	[STAR example included in full guide]
9. How would you explain SOC 2 to a non-technical audience?	SOC 2 is like a health check for a company's data security and privacy practices.
10. How do you prioritize remediation efforts?	Based on risk scoring, business impact, and regulatory requirements.
11-15	[Additional behavioral and scenario-based questions in the downloadable pack]

CYBER GRC LINKEDIN OPTIMIZATION CHECKLIST

Optimization Area	Action Step
Headline	Include GRC keywords (e.g., "GRC Analyst
About Section	Write a story-driven summary focusing on your GRC journey and value to employers
Experience	Use bullet points with quantifiable results (e.g., "Led ISO 27001 internal audit, reducing gaps by 40%")
Skills & Endorsements	Add Risk Assessment, Compliance Management, Vendor Risk, Policy Development
Certifications Section	Display your CISA, CRISC, ISO Lead Implementer prominently
Featured Section	Upload your GRC resume, audit reports, articles, or LinkedIn posts
Engagement Strategy	Join 3–5 GRC groups, comment on posts, and share insights weekly

🚀 *Includes a LinkedIn headline formula to instantly increase profile visibility.*

TOP CYBER GRC CERTIFICATIONS LIST (WITH CAREER PATH)

Certification	Best For	Level
CISA (Certified Information Systems Auditor)	IT Auditors, Compliance Professionals	Intermediate
CRISC (Certified in Risk and Information Systems Control)	Risk Managers, GRC Analysts	Intermediate to Advanced
ISO 27001 Lead Implementer	Consultants, ISMS Managers	Intermediate
CGEIT (Certified in the Governance of Enterprise IT)	IT Governance Professionals	Advanced
CIPM (Certified Information Privacy Manager)	Privacy Program Leaders	Intermediate
Security+ (CompTIA)	Beginners transitioning to GRC	Entry
Certified in Cybersecurity (ISC2 CC)	Beginners in cybersecurity fundamentals	Entry

The guide also includes a "Certification Roadmap" to help you progress from entry to expert.


SkillWeed