50 AI PROMPTS

IN CYBERSECURITY GRC

SkillWeed

CONTENTS

I. GOVERNANCE

1

Prompt: "Explain the purpose of a cybersecurity governance framework in simple terms."

Expected Outcome: A clear explanation highlighting how governance aligns security with business objectives.

2

Prompt: "List three examples of cybersecurity governance frameworks."

Expected Outcome: Examples like NIST CSF, ISO 27001, and COBIT.

3

Prompt: "Draft a cybersecurity governance policy outline for a small business."

Expected Outcome: An outline with sections for roles, responsibilities, risk management, and compliance.

4

Prompt: "What are the key responsibilities of a Chief Information Security Officer (CISO)?"

Expected Outcome: A detailed list, including strategy development, compliance, and team leadership.

5

Prompt: "Generate a risk-based decision-making process for IT governance."

Expected Outcome: Steps involving identifying, assessing, and mitigating risks.

II. RISK MANAGEMENT

6

Prompt: "What are the core components of a risk management framework?"

Expected Outcome: Components like risk identification, assessment, mitigation, and monitoring.

7

Prompt: "Describe the difference between inherent risk and residual risk."

Expected Outcome: A clear comparison showing inherent risk as the baseline risk before controls and residual risk as the remaining risk after controls.

8

Prompt: "Write a sample risk assessment for a medium-sized e-commerce company."

Expected Outcome: Identification of risks like DDoS attacks and data breaches, with mitigation strategies.

9

Prompt: "Explain how to calculate risk using the formula: Risk = Threat x Vulnerability x Impact."

Expected Outcome: A breakdown of each factor with examples.

10

Prompt: "Suggest five tools for effective cybersecurity risk assessment."

Expected Outcome: Tools like FAIR, RiskLens, and OpenRisk.

III. COMPLIANCE

11

Prompt: "Summarize the key requirements of GDPR for organizations handling EU data."

Expected Outcome: A list including data subject rights, data breach reporting, and lawful processing.

12

Prompt: "Draft a compliance checklist for HIPAA in a healthcare organization."

Expected Outcome: A checklist with items like secure patient data storage and regular audits.

13

Prompt: "What are the main differences between PCI DSS and SOC 2 compliance?"

Expected Outcome: A comparison of focus areas like payment card data vs. trust principles.

14

Prompt: "Explain the significance of Section 500.9 of the NYDFS Cybersecurity Regulation."

Expected Outcome: Insights into the requirement for periodic risk assessments.

15

Prompt: "Generate a compliance report template for ISO 27001 certification."

Expected Outcome: A template with sections for policies, risk assessment, and control implementation.

IV. POLICIES AND PROCEDURES

16

Prompt: "Create a password management policy for a small business."

Expected Outcome: A policy mandating complex passwords, rotation, and MFA.

17

Prompt: "What are the essential components of an incident response plan?"

Expected Outcome: Components like preparation, detection, containment, eradication, recovery, and lessons learned.

18

Prompt: "Write a template for a vendor security assessment policy."

Expected Outcome: A policy including vendor categorization, assessment criteria, and periodic reviews.

19

Prompt: "Explain the difference between policies, standards, and guidelines."

Expected Outcome: Definitions showing policies as high-level principles, standards as mandatory rules, and guidelines as recommendations.

20

Prompt: "Draft an acceptable use policy for an organization."

Expected Outcome: A policy outlining acceptable behaviors for using company IT assets.

V. AUDITS AND ASSESSMENTS

21

Prompt: "Explain the purpose of a cybersecurity audit."

Expected Outcome: An explanation showing audits ensure compliance and identify gaps in controls.

22

Prompt: "Create a checklist for a SOC 2 readiness assessment."

Expected Outcome: A checklist with items like access controls and data protection measures.

23

Prompt: "What are the steps to conduct a vulnerability assessment?"

Expected Outcome: Steps including asset discovery, scanning, analysis, and reporting.

24

Prompt: "Generate questions for a third-party cybersecurity risk assessment questionnaire."

Expected Outcome: Questions about data handling, incident response, and encryption practices.

25

Prompt: "Describe the difference between an internal audit and an external audit."

Expected Outcome: A comparison of focus areas, methodologies, and reporting.

VI. THIRD-PARTY RISK MANAGEMENT (TPRM)

26

Prompt: "Write a vendor risk management checklist."

Expected Outcome: A list covering vendor security policies, certifications, and access control mechanisms.

27

Prompt: "Explain the significance of due diligence in TPRM."

Expected Outcome: Insights into how due diligence reduces the risk of vendor-related breaches.

28

Prompt: "List five key elements of a vendor contract from a cybersecurity perspective."

Expected Outcome: Elements like SLAs, incident reporting, and data protection clauses.

29

Prompt: "Draft a sample vendor onboarding policy for a fintech company."

Expected Outcome: A policy covering security reviews, documentation, and training.

30

Prompt: "How can AI tools assist in automating vendor risk assessments?"

Expected Outcome: Examples like automated questionnaires and continuous monitoring.

VII. SECURITY CONTROLS

31

Prompt: "Explain the purpose of access control in cybersecurity."

Expected Outcome: An explanation focusing on preventing unauthorized access.

32

Prompt: "What are the key differences between physical and logical security controls?"

Expected Outcome: A comparison of physical controls like locks vs. logical controls like encryption.

33

Prompt: "Write a step-by-step guide to implementing MFA in a small organization."

Expected Outcome: Steps including tool selection, configuration, and user onboarding.

34

Prompt: "List five essential security controls for protecting cloud environments."

Expected Outcome: Controls like identity management, encryption, and monitoring.

35

Prompt: "Describe the role of firewalls in network security."

Expected Outcome: An explanation showing firewalls as barriers against unauthorized traffic.

VIII. INCIDENT RESPONSE

36

Prompt: "What are the phases of an incident response lifecycle?"

Expected Outcome: Phases like preparation, detection, containment, and recovery.

37

Prompt: "Draft a phishing response procedure for employees."

Expected Outcome: Steps for reporting, quarantining, and investigating phishing emails.

38

Prompt: "Explain the importance of a post-incident review."

Expected Outcome: Insights into improving future responses and closing gaps.

39

Prompt: "What is the difference between a data breach and a security incident?"

Expected Outcome: Definitions showing data breaches involve loss of data, while incidents may not.

40

Prompt: "Write a ransomware response playbook for a healthcare organization."

Expected Outcome: Playbook steps from identifying ransomware to isolating systems and recovery.

IX. CYBERSECURITY FRAMEWORKS

41

Prompt: "What are the five functions of the NIST Cybersecurity Framework?"

Expected Outcome: Functions like Identify, Protect, Detect, Respond, and Recover.

42

Prompt: "Compare ISO 27001 and NIST CSF."

Expected Outcome: A comparison table of scope, implementation, and certification.

43

Prompt: "Draft a mapping of NIST CSF to CIS Controls."

Expected Outcome: A table linking NIST functions to CIS Control categories.

44

Prompt: "Explain how CMMI can be used in a cybersecurity maturity assessment."

Expected Outcome: A guide to evaluating process maturity using CMMI.

45

Prompt: "What are the key focus areas of COBIT in IT governance?"

Expected Outcome: Areas like value delivery, resource optimization, and risk management.

X. CYBERSECURITY AWARENESS AND TRAINING

46

Prompt: "Write a cybersecurity awareness tip for employees."

Expected Outcome: A tip on recognizing phishing emails or using strong passwords.

47

Prompt: "What are the key elements of a successful cybersecurity training program?"

Expected Outcome: Elements like engaging content, real-life examples, and assessments.

48

Prompt: "List five creative ways to improve employee engagement in security training."

Expected Outcome: Ideas like gamification, quizzes, and rewards.

49

Prompt: "Draft a monthly cybersecurity awareness newsletter outline."

Expected Outcome: Sections for news, tips, and employee spotlights.

50

Prompt: "Explain the importance of ongoing training in reducing insider threats."

Expected Outcome: A detailed explanation showing training enhances vigilance and compliance.

SkillWeed