GRC Practical Lab Series: Introduction & Overview

To: All GRC Students
From: Instructor
Subject: Integration of Hands-On GRC Lab Series with Curriculum

1. Welcome Message

Welcome to the Hands-On GRC Lab Series! This practical component is designed to complement and enhance the theoretical knowledge you have gained in **GRC101**, **GRC102**, and **GRC103**. Over the next 10 labs, you will bridge the gap between governance, risk, and compliance frameworks and their real-world implementation. These labs will empower you to apply your learning in a controlled environment, ensuring you are prepared to address modern cybersecurity challenges with confidence.

2. Lab Series Overview

The labs are structured to align with the concepts covered in your coursework. Below is a table summarizing the labs and their alignment with the curriculum:

Lab #	Lab Title	Primary Focus Area	Alignment with Curriculum
1	Vulnerability Assessment	Technical Fundamentals	GRC101 (Weeks 2-5): Risk Management Fundamentals GRC103 (Week 11): Risk Identification Techniques
2	OWASP Top 10 Web App Testing	Application Security	GRC102 (Week 6): Principles of Information Security Governance GRC103 (Week 12): Risk Analysis and Evaluation
3	Social Engineering & Phishing Simulation	Human Risk	GRC101 (Week 4): Risk Management Fundamentals GRC102 (Week 7): Developing Security Policies and Procedures
4	Digital Forensics & Incident Response	Reactive Security	GRC102 (Week 9): Monitoring and Auditing Security Controls GRC103 (Week 14): Risk Monitoring and Reporting
5	Security Control Auditing	Proactive Assurance	GRC101 (Week 5): Compliance Management and Reporting GRC102 (Week 9): Monitoring and Auditing Security Controls
6	Cloud & IaC Security Auditing	Modern Infrastructure	GRC102 (Week 6): Principles of Information Security Governance GRC103 (Week 13): Risk Treatment Strategies

7	Security Monitoring & SIEM	Detective Controls	GRC102 (Week 9): Monitoring and Auditing Security Controls GRC103 (Week 14): Risk Monitoring and Reporting
8	Data Protection & Privacy	Privacy Compliance	GRC101 (Week 3): GRC Regulatory Environment and Standards GRC102 (Week 7): Developing Security Policies and Procedures
9	Third-Party Risk Management	Extended Enterprise	GRC101 (Week 4): Risk Management Fundamentals GRC103 (Week 12): Risk Analysis and Evaluation
10	**Capstone:** GRC Program Synthesis	Strategic GRC	GRC101 (Week 5): Compliance Management and Reporting GRC103 (Week 15): Practical Risk Assessment Workshop

3. Overarching Learning Outcomes

By the end of this lab series, you will be able to:

- **Apply** GRC frameworks (e.g., NIST, CIS, ISO27001) to real-world scenarios.
- **Conduct** technical assessments to identify and evaluate risks.
- **Develop** policies and procedures based on regulatory requirements.
- **Create** comprehensive reports for technical and executive audiences.
- **Design** risk treatment and mitigation strategies aligned with business objectives.

4. Lab Environment & Prerequisites

A. Required Software (Pre-Installed)

- **Virtualization Software:** VMware Workstation Player or VirtualBox.
- **PDF Reader:** For reviewing lab guides and drafting reports.

B. Virtual Machines (Download and Import Before Lab Sessions)

1. **Kali Linux (Attacker Machine):**

- **Download:** Kali Linux Official Site
- **Credentials:** kali:kali

2. **Metasploitable 2 (Victim Machine for Labs 1, 4, 5, 7, 8):**
   - **Download:** Metasploitable 2 on SourceForge
   - **Credentials:** msfadmin:msfadmin
3. **OWASP Broken Web Applications (BWA) (Victim Machine for Lab 2):**
   - **Download:** OWASP BWA on SourceForge

5. Lab Schedule and Integration with Curriculum

The labs are scheduled to align with your coursework as follows:

Lab #	Lab Title	Scheduled Week	Aligned Course Week(s)	Curriculum Topics Covered
1	Vulnerability Assessment	Week 11	GRC103 (Week 11)	Risk Identification Techniques
2	OWASP Top 10 Web App Testing	Week 11	GRC103 (Week 12)	Risk Analysis and Evaluation
3	Social Engineering & Phishing Simulation	Week 12	GRC103 (Week 13)	Risk Treatment Strategies
4	Digital Forensics & Incident Response	Week 12	GRC103 (Week 14)	Risk Monitoring and Reporting
5	Security Control Auditing	Week 13	GRC103 (Week 15)	Practical Risk Assessment Workshop
6	Cloud & IaC Security Auditing	Week 13	GRC102 (Week 9)	Monitoring and Auditing Security Controls
7	Security Monitoring & SIEM	Week 14	GRC102 (Week 9)	Monitoring and Auditing Security Controls
8	Data Protection & Privacy	Week 14	GRC101 (Week 3)	GRC Regulatory Environment and Standards
9	Third-Party Risk Management	Week 15	GRC101 (Week 4)	Risk Management Fundamentals
10	Capstone: GRC Program Synthesis	Week 15	GRC101 (Week 5)	Compliance Management and Reporting

6. Conduct & Best Practices

- **Ethics:** These labs are for educational purposes only. Use the tools and techniques only in the isolated lab environment.
- **Documentation:** Maintain detailed notes and evidence for each lab. This mimics real-world GRC documentation requirements.
- **Collaboration:** Discuss findings with peers, but submit individual reports.
- **Ask Questions:** Engage with instructors to clarify concepts and techniques.

7. What to Bring to Each Lab

- **Notebook and Pen:** For note-taking and drafting reports.
- **USB Drive/Cloud Storage:** To save lab reports and evidence.
- **Lab Guide:** Provided at the start of each session.
- **Virtual Machines:** Pre-loaded and ready to use.

8. Conclusion

This lab series is designed to transform theoretical knowledge into practical expertise. By aligning with your coursework, these labs will help you build a holistic understanding of GRC in action. Let's embark on this journey to become proficient GRC professionals!

See you in the lab!