GRC105 - Incident Management and Business Continuity

Week 20: Theory-Based Lab Assignment

Incident Response Planning and Documentation

Course: GRC105 - Incident Management and Business Continuity
Institution: International Cybersecurity and Digital Forensics Academy (ICDFA)
Week: 20 (December 1-7)
Topic: Incident Response Planning
Assignment Type: Theory-Based Lab
Total Points: 100
Due Date: End of Week 20

Assignment Overview

This theory-based lab assignment evaluates your understanding of incident response planning concepts, frameworks, and documentation requirements based on industry standards, including NIST SP 800-61 Revision 3 and CISA guidelines. You will develop comprehensive incident response documentation for a fictional organization, demonstrating mastery of the NIST Incident Response Lifecycle and associated best practices.

The assignment requires you to apply theoretical knowledge gained during Week 20 lectures to create practical incident response artifacts that would be used in a real-world organizational setting. Your deliverables will demonstrate understanding of preparation requirements, team structures, communication protocols, and continuous improvement processes.

Learning Objectives

Upon completion of this assignment, students will be able to:

1. **Apply the NIST Incident Response Lifecycle** to organizational security operations by developing comprehensive documentation for each phase
2. **Design incident response team structures** with clearly defined roles, responsibilities, and RACI matrices
3. **Develop incident classification and prioritization frameworks** aligned with business impact and regulatory requirements
4. **Create communication protocols** for internal and external stakeholders during security incidents
5. **Establish metrics and continuous improvement processes** for incident response program maturity

Scenario Background

You have been hired as the **Governance, Risk, and Compliance (GRC) Manager** for **TechMed Solutions**, a mid-sized healthcare technology company with the following characteristics:

Organizational Attribute	Details
Industry	Healthcare Technology (SaaS Platform)
Employee Count	850 employees across 3 locations
Annual Revenue	$120 million USD
Customer Base	200+ healthcare providers across North America
Data Handled	Protected Health Information (PHI), Payment Card Data (PCI), Proprietary Medical Algorithms
Regulatory Requirements	HIPAA, PCI DSS, SOC 2 Type II, GDPR (limited European customers)
Current Security Posture	Basic security controls in place, no formal incident response program
IT Infrastructure	Hybrid cloud environment (AWS primary, on-premises data center for legacy systems)

TechMed Solutions recently experienced a minor security incident involving unauthorized access to a development environment. While no customer data was compromised, the incident exposed significant gaps in the organization's ability to detect, respond to, and recover from security events. The Board of Directors has mandated the establishment of a formal incident response program, and you have been tasked with developing the foundational documentation.

Assignment Tasks

Task 1: Incident Response Policy Development (25 points)

Develop a comprehensive **Incident Response Policy** for TechMed Solutions that establishes the foundation for the organization's incident response program. Your policy document must address the following components:

Required Policy Elements:

6. **Purpose and Scope** - Define the policy's objectives and applicability across the organization, including all employees, contractors, and third-party service providers.
7. **Definitions** - Provide clear definitions for key terms including security incident, security event, incident response, Computer Security Incident Response Team (CSIRT), and incident severity levels.
8. **Roles and Responsibilities** - Establish high-level accountability for incident response activities across organizational functions including executive leadership, IT operations, legal, human resources, and communications.
9. **Incident Classification Framework** - Develop a classification system that categorizes incidents by type (malware, unauthorized access, data breach, denial of service, insider threat, physical security) and severity (Critical, High, Medium, Low) with clear criteria for each level.
10. **Reporting Requirements** - Specify mandatory reporting procedures for employees who discover or

suspect security incidents, including reporting channels, timeframes, and escalation paths.

11. **Regulatory and Legal Compliance** - Address compliance obligations under HIPAA, PCI DSS, and other applicable regulations, including breach notification requirements and timelines.
12. **Policy Review and Updates** - Establish a schedule for policy review and update procedures to ensure the policy remains current with evolving threats and regulatory requirements.

Deliverable Format: Professional policy document (3-5 pages) following standard organizational policy structure with version control, approval signatures, and effective date.

Task 2: Incident Response Plan (IRP) Development (30 points)

Create a detailed **Incident Response Plan** that operationalizes the policy established in Task 1. The IRP must provide tactical guidance for responding to security incidents across the NIST Incident Response Lifecycle.

Required IRP Components:

Phase 1: Preparation (8 points)

13. **CSIRT Structure and Composition** - Define the incident response team structure including core team members, extended team members, and external resources. Specify reporting relationships and authority levels.
14. **Tools and Resources** - Identify required incident response tools including forensic software, communication platforms, documentation systems, and technical resources needed for effective response.
15. **Training and Awareness Program** - Outline training requirements for CSIRT members and general employee security awareness programs to support incident detection and reporting.
16. **Communication Infrastructure** - Establish secure communication channels for incident response activities, including out-of-band communication methods for scenarios where primary systems are compromised.

Phase 2: Detection and Analysis (8 points)

17. **Detection Sources and Methods** - Document primary detection mechanisms including SIEM alerts, IDS/IPS notifications, antivirus alerts, user reports, and third-party notifications.
18. **Initial Triage Procedures** - Develop step-by-step procedures for validating suspected incidents and distinguishing true positives from false alarms.
19. **Incident Analysis Framework** - Create a structured approach for analyzing confirmed incidents including evidence collection, scope determination, and attack vector identification.
20. **Documentation Requirements** - Specify required documentation during detection and analysis including incident tickets, initial assessment reports, and evidence logs.

Phase 3: Containment, Eradication, and Recovery (8 points)

21. **Containment Strategies** - Develop both short-term containment strategies (immediate threat isolation) and long-term containment strategies (sustainable isolation while maintaining business operations).

22 **Eradication Procedures** - Document systematic procedures for removing threats from the environment including malware removal, account remediation, and vulnerability patching.

23 **Recovery Processes** - Establish phased recovery procedures including system restoration from backups, validation testing, and return to normal operations with enhanced monitoring.

24 **Business Continuity Integration** - Specify how incident response activities integrate with business continuity and disaster recovery plans for major incidents.

Phase 4: Post-Incident Activity (6 points)

25 **Lessons Learned Process** - Define structured review procedures including timing, participants, and documentation requirements for post-incident reviews.

26 **Root Cause Analysis** - Specify methodologies for identifying underlying causes of incidents and systemic vulnerabilities.

27 **Improvement Recommendations** - Establish processes for translating lessons learned into actionable improvements across people, processes, and technology.

28 **Metrics and Reporting** - Define key performance indicators (KPIs) and metrics for measuring incident response effectiveness and program maturity.

Deliverable Format: Comprehensive incident response plan document (8-12 pages) with clear section headings, procedures written in actionable language, and appendices for templates and checklists.

Task 3: CSIRT Structure and RACI Matrix (20 points)

Design the organizational structure for TechMed Solutions' Computer Security Incident Response Team (CSIRT) and develop a detailed RACI matrix defining accountability for incident response activities.

Required Components:

29 **CSIRT Organizational Chart** - Create a visual representation of the CSIRT structure showing reporting relationships, core team members, extended team members, and external stakeholders. Include specific job titles and functional areas.

30 **Role Definitions** - Provide detailed role descriptions for each CSIRT position including:

- ✓ **Incident Response Manager** - Leadership, coordination, and decision-making authority
- ✓ **Security Analysts** - Detection, triage, and initial investigation
- ✓ **Forensics Specialists** - Evidence collection, preservation, and deep technical analysis
- ✓ **Communications Coordinator** - Internal and external stakeholder communication
- ✓ **Legal Liaison** - Regulatory compliance and legal considerations
- ✓ **IT Operations Representative** - System access and technical support

31 **RACI Matrix** - Develop a comprehensive RACI (Responsible, Accountable, Consulted, Informed) matrix that clearly defines accountability for key incident response activities. Your matrix must include at minimum the following activities:

- ✓ Incident detection and initial reporting
- ✓ Incident validation and triage
- ✓ Incident classification and prioritization

- ✓ Evidence collection and preservation
- ✓ Containment decision-making
- ✓ Eradication execution
- ✓ System recovery and validation
- ✓ Stakeholder communication (internal)
- ✓ Stakeholder communication (external)
- ✓ Regulatory notification and reporting
- ✓ Post-incident review facilitation
- ✓ Lessons learned documentation
- ✓ IR plan updates and maintenance

32 **Escalation Procedures** - Define clear escalation criteria and paths for elevating incidents to executive leadership, legal counsel, and external parties based on severity and business impact.

Deliverable Format: CSIRT structure document (3-4 pages) including organizational chart diagram, role descriptions in table format, comprehensive RACI matrix, and escalation decision tree or flowchart.

Task 4: Incident Communication Plan (15 points)

Develop a comprehensive **Incident Communication Plan** that ensures timely, accurate, and appropriate communication with internal and external stakeholders during security incidents.

Required Components:

33 **Stakeholder Identification** - Identify all potential stakeholders requiring communication during incidents including:

- ✓ Internal stakeholders (executives, employees, IT staff, legal, HR, PR)
- ✓ External stakeholders (customers, regulators, law enforcement, media, partners, vendors)
- ✓ Specify communication requirements and expectations for each stakeholder group

34 **Communication Templates** - Create communication templates for common scenarios including:

- ✓ **Initial Incident Notification** (internal) - Alert to CSIRT and management
- ✓ **Executive Briefing** - Status updates for leadership
- ✓ **Customer Notification** - Breach notification for affected customers
- ✓ **Regulatory Notification** - Compliance reporting to HIPAA, PCI DSS authorities
- ✓ **Public Statement** - Media and public communication template

35 **Communication Protocols** - Establish protocols addressing:

- ✓ Approval workflows for external communications
- ✓ Secure communication channels for sensitive information
- ✓ Communication frequency and update schedules
- ✓ Spokesperson designation and media handling procedures
- ✓ Legal review requirements before external disclosures

36 **Regulatory Notification Requirements** - Document specific notification timelines and

requirements for applicable regulations:

- ✓ **HIPAA Breach Notification Rule** - 60-day notification requirement for breaches affecting 500+ individuals
- ✓ **PCI DSS** - Immediate notification to payment brands and acquiring bank
- ✓ **State Breach Notification Laws** - Varying requirements across jurisdictions

Deliverable Format: Communication plan document (4-6 pages) including stakeholder matrix, communication templates, protocol flowcharts, and regulatory compliance checklist.

Task 5: Incident Response Metrics and Continuous Improvement (10 points)

Establish a framework for measuring incident response effectiveness and driving continuous improvement of TechMed Solutions' incident response program.

Required Components:

37 **Key Performance Indicators (KPIs)** - Define measurable KPIs for incident response program performance including:

- ✓ **Mean Time to Detect (MTTD)** - Average time from incident occurrence to detection
- ✓ **Mean Time to Respond (MTTR)** - Average time from detection to initial response action
- ✓ **Mean Time to Contain (MTTC)** - Average time from detection to containment
- ✓ **Mean Time to Recover (MTTR)** - Average time from detection to full recovery
- ✓ **Incident Volume Trends** - Number and types of incidents over time
- ✓ **False Positive Rate** - Percentage of alerts that are not actual incidents

38 **Metrics Collection and Reporting** - Specify how metrics will be collected, analyzed, and reported to stakeholders including data sources, collection frequency, and reporting dashboards.

39 **Continuous Improvement Process** - Establish a structured process for translating metrics and lessons learned into program improvements including:

- ✓ Quarterly program reviews
- ✓ Annual tabletop exercises and simulations
- ✓ IR plan update procedures
- ✓ Training program enhancements based on identified gaps

40 **Program Maturity Assessment** - Develop criteria for assessing incident response program maturity using a capability maturity model framework (Initial, Developing, Defined, Managed, Optimizing).

Deliverable Format: Metrics and improvement framework document (2-3 pages) including KPI definitions table, metrics dashboard mockup or description, improvement process flowchart, and maturity assessment criteria.

Submission Requirements

Format and Structure

All deliverables must be submitted as professional business documents following these requirements:

41 **Document Format** - Microsoft Word (.docx) or PDF format

42 **Formatting Standards** - Professional business formatting with consistent fonts (Arial or Calibri 11-12pt), proper headings, page numbers, and table of contents for documents exceeding 5 pages

43 **Organization Branding** - Include TechMed Solutions branding elements (you may create a simple logo or header)

44 **Version Control** - All documents must include version number, author, and date in footer

45 **Citations and References** - Cite all external sources using APA format including NIST publications, CISA guidelines, and other industry frameworks referenced

Deliverable Checklist

Submit a single compressed file (ZIP) containing:

- Task 1: Incident Response Policy (PDF or DOCX)
- Task 2: Incident Response Plan (PDF or DOCX)
- Task 3: CSIRT Structure and RACI Matrix (PDF or DOCX)
- Task 4: Incident Communication Plan (PDF or DOCX)
- Task 5: Metrics and Continuous Improvement Framework (PDF or DOCX)
- References document listing all sources cited (PDF or DOCX)

File Naming Convention

Use the following naming convention for all files:

```
GRC105_Week20_Theory_[TaskNumber]_[LastName]_[FirstName].[extension]

Example: GRC105_Week20_Theory_Task1_Smith_John.pdf
```

Grading Rubric

Task 1: Incident Response Policy (25 points)

Criteria	**Excellent (23-25)**	**Good (20-22)**	**Satisfactory (17-19)**	**Needs Improvement (0-16)**
Completeness	All required policy elements comprehensively addressed	Most elements addressed with minor gaps	Some elements missing or superficial	Major elements missing
Alignment with Standards	Fully aligned with NIST and industry best practices	Generally aligned with minor deviations	Partial alignment with notable gaps	Limited alignment with standards
Regulatory Compliance	Thoroughly addresses all applicable regulations	Addresses most regulatory requirements	Some regulatory requirements addressed	Regulatory requirements inadequately addressed

Professional Quality	Exceptionally well-written, formatted, and organized	Well-written with minor formatting issues	Acceptable quality with some issues	Poor quality or unprofessional presentation

Task 2: Incident Response Plan (30 points)

Criteria	Excellent (27-30)	Good (24-26)	Satisfactory (20-23)	Needs Improvement (0-19)
NIST Lifecycle Coverage	All four phases comprehensively documented with actionable procedures	All phases addressed with minor gaps in detail	Some phases well-developed, others superficial	Incomplete or inadequate phase coverage
Practical Applicability	Procedures are clear, actionable, and immediately usable	Generally practical with minor ambiguities	Some procedures lack clarity or detail	Procedures are vague or impractical
Integration and Coherence	Excellent integration across phases and with organizational context	Good integration with minor disconnects	Adequate integration with some gaps	Poor integration or coherence
Technical Accuracy	Technically accurate and current with industry practices	Generally accurate with minor errors	Some technical inaccuracies present	Significant technical errors or outdated practices

Task 3: CSIRT Structure and RACI Matrix (20 points)

Criteria	Excellent (18-20)	Good (16-17)	Satisfactory (14-15)	Needs Improvement (0-13)
Organizational Design	CSIRT structure is well-designed, appropriate for organization size, with clear reporting relationships	Good structure with minor organizational issues	Basic structure with some unclear relationships	Poorly designed or inappropriate structure
Role Clarity	All roles clearly defined with specific responsibilities and qualifications	Most roles well-defined with minor gaps	Some role definitions lack clarity	Role definitions are vague or incomplete
RACI Matrix Completeness	Comprehensive RACI matrix covering all critical activities with clear accountability	Good coverage with minor gaps	Adequate coverage with some ambiguities	Incomplete or confusing RACI assignments
Escalation Procedures	Clear, well-defined escalation criteria and paths	Good escalation procedures with minor gaps	Basic escalation guidance provided	Unclear or missing escalation procedures

Task 4: Incident Communication Plan (15 points)

Criteria	Excellent (14-15)	Good (12-13)	Satisfactory (10-11)	Needs Improvement (0-9)
Stakeholder Coverage	All relevant stakeholders identified with tailored communication approaches	Most stakeholders identified with appropriate approaches	Basic stakeholder identification with generic approaches	Incomplete stakeholder identification
Template Quality	Communication templates are professional, comprehensive, and immediately usable	Good templates with minor improvements needed	Basic templates requiring customization	Templates are incomplete or unprofessional
Regulatory Compliance	Fully addresses all regulatory notification requirements with specific timelines	Addresses most requirements with minor gaps	Some regulatory requirements addressed	Inadequate regulatory compliance coverage
Practical Usability	Plan is clear, actionable, and ready for implementation	Generally usable with minor clarifications needed	Requires some refinement for practical use	Difficult to implement or unclear procedures

Task 5: Metrics and Continuous Improvement (10 points)

Criteria	Excellent (9-10)	Good (8)	Satisfactory (7)	Needs Improvement (0-6)
KPI Selection	KPIs are relevant, measurable, and aligned with program objectives	Good KPI selection with minor gaps	Basic KPIs identified with some relevance issues	KPIs are poorly selected or not measurable
Improvement Process	Well-defined continuous improvement process with clear procedures	Good process with minor procedural gaps	Basic improvement process outlined	Improvement process is vague or missing
Maturity Assessment	Comprehensive maturity framework with clear criteria	Good maturity framework with minor gaps	Basic maturity criteria provided	Maturity assessment inadequate or missing

Overall Presentation and Professionalism (Applies across all tasks)

Points may be deducted for:

- Poor grammar, spelling, or writing quality (-5 points)
- Inconsistent formatting or unprofessional presentation (-3 points)
- Missing citations or references (-3 points)
- Failure to follow submission requirements (-5 points)

Additional Resources

Students are encouraged to reference the following authoritative sources when completing this assignment:

46 **NIST Special Publication 800-61 Revision 3** - Computer Security Incident Handling Guide
47 **CISA Incident Response Plan Basics** - Foundational guidance for developing incident response capabilities
48 **SANS Incident Handler's Handbook** - Practical incident response procedures and checklists
49 **ISO/IEC 27035** - Information security incident management standard
50 **HIPAA Breach Notification Rule** - 45 CFR & 164.400-414
51 **PCI DSS Requirement 12.10** - Incident response plan requirements for payment card environments

All sources must be properly cited in your deliverables using APA format.

Academic Integrity

This is an individual assignment. While you may reference course materials, textbooks, and publicly available resources, all work submitted must be your own original creation. Collaboration with other students or submission of work created by others (including AI-generated content without proper attribution) constitutes academic dishonesty and will result in disciplinary action according to ICDFA policies.

You may use AI tools for research, brainstorming, or editing, but the final deliverables must reflect your own understanding and analysis. Any AI assistance must be disclosed in your submission.

Submission Instructions

52 Complete all five tasks according to the requirements specified

53 Organize all deliverables into a single folder named: GRC105_Week20_Theory_[LastName]_[FirstName]

54 Compress the folder into a ZIP file

55 Submit via the course learning management system before the deadline

56 Late submissions will be penalized 10% per day up to 3 days; submissions more than 3 days late will not be accepted

Questions and Support

If you have questions about this assignment, please:

- Post questions in the course discussion forum for general clarification
- Attend office hours for individual guidance
- Email the instructor at least 48 hours before the deadline for time-sensitive questions

This assignment is designed to prepare you for real-world incident response planning responsibilities in governance, risk, and compliance roles. Approach it with the professionalism and thoroughness you would apply in an actual organizational setting.

Good luck!