

Data Security final

by Nikhitha Akula

Submission date: 09-Jan-2025 03:47PM (UTC+0000)

Submission ID: 247815660

File name: 58973_Nikhitha_Akula_Data_Security_final_634839_153673547.docx (41.87K)

Word count: 3965

Character count: 25719

NATURE GARDEN

Submitted by:

Ms. AKULA NIKHITHA

STUDENT ID : 2406304

Module name:

MSc/PgDip/PgCert Cybersecurity and Digital Forensics- ACCA7028

DATA SECURITY, GOVERNANCE AND COMPLIANCE

Submission Date:

9th January 2025

University of Wales Trinity Saint David

Abstract: [Abstract](#)

As businesses grow their digital operations internationally, information security and compliance become increasingly important. As an online and cloud-based service provider, NatureGarden (NG) has difficulties safeguarding confidential information, maintaining intellectual property, and guaranteeing the security of its customers and staff. In order to create a solid plan for NG's data security and governance, this study looks at standards such as ITIL, ISO 27001, and the NIST Cybersecurity Framework. It emphasizes how crucial it is to have thorough rules, manage risks, and follow laws like the CCPA and GDPR. In order to ensure regulatory compliance and asset protection, NG can reduce risks, improve security, and foster stakeholder confidence by putting systematic processes into place and upgrading standards.

[New page](#) Table of Contents:

1. Introduction
2. Framework Analysis
3. Scenario Analysis
4. Implementation Strategies
5. Further Insights and Improvements
6. Conclusion
7. References
8. Appendices

1. Introduction:

Because of its reliance on cloud services, wireless networks, and BYOD policies, NatureGarden (NG) is exposed to serious security concerns. In order to improve data security, guarantee CCPA and GDPR compliance, and reduce risks, this paper suggests a strategic framework utilizing ITIL, ISO 27001, and NIST. By using this strategy, NG's resources and reputation are safeguarded.

Purpose:

The purpose of this article is to develop a strong security architecture for NatureGarden (NG) in order to improve data security, guarantee compliance, reduce wireless and BYOD threats, and efficiently protect operations and intellectual property.

Frameworks considered:

The relevance and applicability of the following frameworks to NG were examined and evaluated:

1. ISO/IEC 27001: In order to preserve sensitive data, privacy, and integrity, organizations must match their processes with legislation and ethical standards such as the CCPA and GDPR. This increases stakeholder trust while lowering the risk of penalties, legal issues, and reputational harm. To adjust to changing regulatory demands, thorough procedures, frequent audits, and ongoing monitoring are necessary.

2. NIST Cybersecurity Framework: With its five main functions—identifying systems and risks, protecting with safeguards, detecting threats through monitoring, responding with incident protocols, and quickly recovering services

after an incident—the NIST Cybersecurity Framework offers a flexible, proactive approach to cybersecurity. It successfully lowers risks while adjusting to organizational needs.

3. COBIT: By emphasizing resource optimization, risk management, and regulatory compliance, COBIT synchronizes IT governance with business goals. In order to give value while keeping strong control and performance metrics, it creates responsibility and combines IT procedures with business strategy.

4. ITIL: By improving day-to-day operations and service delivery, ITIL focuses on efficient IT service management. Through organized procedures and ongoing development, it promotes governance by guaranteeing that IT services meet business objectives and adjust to shifting organizational requirements.

Key Challenges Addressed:

1. Security of Wireless Networks: WPA3 encryption, RBAC, and MFA are necessary for wireless security in order to guard against unwanted access and safeguard data. By putting these security measures in place, NatureGarden can fortify its wireless network and lower the possibility of security breaches.

2. BYOD Policies: By implementing MDM, limiting access to critical systems, and guaranteeing secure setups, BYOD policies mitigate the risks associated with personal devices and shield sensitive data from malware, unauthorized access, and other dangers.

3. Data Protection and Compliance: Under regulations such as GDPR, data protection and compliance guarantee the secure management of sensitive data. Policies protect privacy, stop illegal access, and help prevent fines, legal problems, and damage to one's reputation.

4. Safeguarding Intellectual Property: Under regulations such as GDPR, data protection and compliance guarantee the secure management of sensitive data. Policies protect privacy, stop illegal access, and help prevent fines, legal problems, and damage to one's reputation.

5. Lack of Security Policies: Under regulations such as GDPR, data protection and compliance guarantee the secure management of sensitive data. Policies protect privacy, stop illegal access, and help prevent fines, legal problems, and damage to one's reputation.

6. Insider Threat Management: Through access controls, behavioral analytics, and monitoring, insider threat management identifies and reduces the risks of purposeful or unintentional resource misuse, protecting sensitive data and maintaining operational integrity.

7. Cloud service Risk: Vulnerabilities in resources that are outsourced are the source of cloud service hazards. Secure configurations, encryption, threat detection, third-party audits, and unambiguous SLAs are necessary for their mitigation in order to guarantee data security, operational dependability, and accountability.

8. Compliance with Law and Ethics: Aligning with regulations like GDPR and CCPA secures data, fosters confidence, avoids penalties, and involves audits and continual monitoring.

2. Framework Analysis:

1. ITIL(INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY) :

Overview: ITIL aligns IT services with business objectives by offering best practices for IT service management. By integrating security across the service lifecycle, it guarantees dependable systems, proactive risk management, and continuous improvement, establishing security as a fundamental, continuous procedure.

Key Phases:

1.1: Service Strategy: In order to ensure effective IT expenditures that support long-term organizational growth, ITIL's Service Strategy phase focuses value-driven services, connects IT services with business goals, and develops a roadmap.

1.2: Service Design:

By emphasizing rules, risk management, and standards, the Service Design phase guarantees that security is incorporated into IT services from the outset and produces dependable, secure systems that are in line with business requirements.

1.3: Service Transition: According to ITIL, service transition minimizes interruptions and guarantees the seamless deployment of new or upgraded IT services. In order to satisfy business requirements and guarantee operational preparedness, it incorporates testing, change management, and knowledge transfer.

1.4: Service Operation: ITIL's Service Operation guarantees the dependable and effective administration of IT services. In order to preserve operational stability and customer pleasure, it focuses on managing occurrences, fixing issues, and completing service requests. This stage is essential to maintaining efficient daily IT operations.

1.5: Continual Service Improvement (CSI): ITIL's Continual Service Improvement (CSI) approach is centered on continuously improving IT services and procedures. In order to make sure that IT services adapt to changing business needs and provide increased efficiency and effectiveness, it makes use of performance measurements and feedback to pinpoint areas that require improvement.

2. ISO 27001:

Overview: A worldwide standard for creating an ISMS, ISO 27001 helps businesses identify risks and put controls in place to safeguard data availability, confidentiality, and integrity while guaranteeing an organized and ongoing approach to information security management.

Key Elements:

2.1: Information Security Policies: A worldwide standard for creating an ISMS, ISO 27001 helps businesses identify risks and put controls in place to safeguard data availability, confidentiality, and integrity while guaranteeing an organized and ongoing approach to information security management.

2.2: Risk Assessment and Treatment: Identifying, assessing, and reducing hazards are all part of risk assessment and treatment. Assuring compliance, asset protection, and adaptability through frequent reviews to handle new

threats and reduce disruptions, organizations implement controls, transfer, or accept risks.

2.3: Asset Management: Inventorying vital assets, classifying their significance, guaranteeing their safety, and facilitating efficient risk management, compliance, and resource utilization in organizational operations are all part of asset management.

2.4: Access Control: In order to safeguard resources, lower insider threats, and guarantee data integrity and confidentiality, access control employs policies, MFA, and RBAC to limit access to authorized users.

2.5: Incident Management: Predicting, recognizing, and responding to security occurrences are all part of incident management. In addition to improving response readiness, clearly defined roles, procedures, and testing guarantee prompt resolution, reduce interruptions, and safeguard critical data.

2.6: Compliance: Compliance protects data and reputation by guaranteeing respect to laws like GDPR. In addition to ensuring operations and fostering trust, policies, audits, and training also aid in adapting to changing regulatory requirements.

2.7: Internal Audits: Compliance protects data and reputation by guaranteeing respect to laws like GDPR. In addition to ensuring operations and fostering trust, policies, audits, and training also aid in adapting to changing regulatory requirements.

3. NIST (National Institute of Standards and Technology) Cybersecurity Framework:

Overview: Through its five functions—Identify, Protect, Detect, Respond, and Recover—the NIST Cybersecurity Framework provides a flexible method of

managing cyber risks that is in line with business requirements to improve proactive risk management and resilience.

3.1: Identify: Identifying entails being aware of assets, systems, and possible hazards. To guarantee efficient defense, organizations rank resources and evaluate vulnerabilities. Developing a defined security plan starts with this stage.

3.2: Protect: Puts an emphasis on deploying techniques like firewalls, multi-factor authentication (MFA), and encryption to protect systems and data. The goal is to erect obstacles that stop data breaches and illegal access.

3.3: Detect: This involves creating procedures and tools for real-time monitoring in order to spot odd activity or security breaches. It guarantees that dangers are identified early on before they become serious problems.

3.4: Respond: Creates precise guidelines for handling and containing cyberattacks. This feature ensures prompt and efficient action, reducing the consequences of breaches.

3.5: Recover: After an incident, this phase focuses on getting systems and operations back to normal. Recovery plans enable firms learn from catastrophes to improve defenses and guarantee continuation.

4. COBIT (Control Objectives for Information and Related Technologies):

Overview: A well-known IT governance framework that links IT strategy with business objectives is COBIT. In order to ensure accountability, performance evaluation, and efficient decision-making while providing organizational value, it places a strong emphasis on risk management, resource optimization, and compliance.

Key Areas:

4.1: Governance Framework: Creates a governance framework to match company objectives with IT goals. It improves organizational performance and compliance by outlining roles and responsibilities clearly to guarantee responsibility and consistency in decision-making.

4.2: Strategic alignment: Strategic alignment guarantees that IT investments and activities provide quantifiable value and directly support business priorities. Goal attainment is promoted by this alignment, which maximizes resource use and improves cooperation between IT and business groups.

4.3: Resource management: Resource management is concerned with making the most of IT resources, such as infrastructure, technology, and employees. Waste is decreased, operational effectiveness is increased, and scalability for future requirements is supported by efficient resource allocation and management.

4.4: Risk management: Risk management is the process of identifying, assessing, and reducing IT risks in order to preserve business continuity. To ensure a balanced approach to risk-taking and security, this entails putting controls in place, keeping an eye on threats, and determining risk tolerance levels.

4.5: Performance measurement: Monitors and assesses the efficiency of IT procedures and services using Key Performance Indicators (KPIs). Through the identification of areas for optimization and the guarantee of conformity with corporate objectives, performance measures facilitate continual improvement.

4.6: Audit and Assurance: Offers a methodical framework for confirming

compliance and preparing for an audit. Frequent audits promote transparency, guarantee compliance with legal requirements, and pinpoint areas where IT governance needs to be strengthened.

Benefits of COBIT:

- Strong IT connection with business plans.
- Efficient enforcement of compliance and risk management.
- Strong governance structure with quantifiable results.

Framework Comparison Table

Framework	Key Focus Areas	Advantages	Limitations
ISO/IEC 27001	ISMS, risk management, compliance	Comprehensive, globally recognized	Resource-intensive implementation
NIST Cybersecurity	Threat detection, response, recovery	Flexible, practical, widely used in the US	Less focused on governance
COBIT	IT governance, strategy alignment	Strong on governance and management	Limited focus on operational security

ITIL	IT service management, governance	Aligns IT services with business objectives	Focuses less on cybersecurity specifically
------	-----------------------------------	---	--

3. Scenario Analysis

Security Challenges Identified

Lack of Robust Security Policies: The company is vulnerable to compliance issues and vulnerabilities when there are unclear and inconsistent policies in place.

Exposure of Wireless Networks: Unauthorized intrusions are more likely when access restrictions and encryption are inadequate.

Unregulated BYOD Usage: Using personal devices to access company networks exposes users to hazards like viruses and data leaks.

Vulnerabilities in Intellectual Property Protection: Insufficient protections expose confidential data to loss or abuse.

Inadequate Compliance Mechanisms: Penalties and harm to one's reputation may result from noncompliance with regulations like the CCPA and GDPR.

Insider Threats: Data breaches and operational sabotage can result from insiders' malicious or inadvertent activities.

Cloud Misconfigurations: Inadequate security measures can leave private information vulnerable to outside attacks.

Lack of Contingency Planning: In the event of a crisis, a lack of disaster recovery plans may result in extended outages and business interruptions.

Threat and Risk Assessment

Threat	Risk Level	Potential Impact	Likelihood
Unauthorized Access	High	Data breaches	High
Attacks Phishing	Medium	Credential compromise	Medium
Data Theft	High	Loss of intellectual property	Medium
Compliance Violations	High	Fines, reputational damage	High
Insider Threats	Medium	Operational disruptions	Medium
Cloud Misconfigurations	Medium	Data exposure	Medium
Disaster Recovery Failure	High	Extended downtime	Medium

Proposed Framework:

1. Governance Mechanism:

A Data Governance Committee creates security rules, performs audits, and makes sure regulations are followed in order to guarantee thorough monitoring. It fosters accountability, efficiency, threat management, and operational integrity throughout the company by coordinating IT goals with business objectives.

Key Policies:**BYOD Policy:**

- Requires personal device security through the use of Mobile Device Management (MDM) technologies.
- Requires devices to be configured securely in order to minimize vulnerabilities.
- Limits access to critical systems according to responsibilities and need.

Acceptable Use Policy (AUP):

- Describes what can be done with both personal and business equipment.
- Lays out precise guidelines to stop the abuse of organizational resources.
- Makes certain that users understand their role in preserving security.

Data Retention Policy:

- Outlines precise rules for data deletion procedures, retention durations, and storage.
- Guarantees adherence to data privacy regulations such as GDPR.
- Reduces the amount of duplicated or out-of-date information stored in order to lower hazards.

2. Risk Management:**RiskAssessment:**

- Utilizing the FAIR paradigm, conduct risk assessments every six months to assess and measure the possible consequences of risks that have been identified.

- To prioritize mitigation efforts, identify high-risk areas such as malware, insider threats, and data breaches.

Strategies for Mitigation:

- Manage vulnerabilities, implement CIS Controls to secure configurations, and guarantee ongoing monitoring.
- Put in place endpoint security measures to identify and stop malware.

Risk Monitoring:

- To identify irregularities, implement automated techniques for real-time network traffic, device activity, and user behavior monitoring.

3. Security Measures

Access Control:

- For critical systems, enforce Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA).
- Make sure users have only the access required for their responsibilities by using the least-privilege concept.

Network Security:

- To protect wireless networks, use WPA3 encryption.
- To lessen attack surfaces, implement firewalls, intrusion detection/prevention systems (IDPS), and network segmentation.

Data Protection:

- Use AES-256 encryption standards to encrypt sensitive data while it's in transit and at rest.

- Use Data Loss Prevention (DLP) tools to keep an eye on and stop illegal data sharing.

4. Auditing and Compliance

ISO 27001 Alignment: To guarantee standard adherence, conduct frequent compliance audits and risk management evaluations.

Create a methodical approach to ensure GDPR adherence.

Automated Tools: To monitor compliance status and do gap analyses for ongoing development, use automated tools.

Audit Logs: Keep thorough and precise audit logs to prove compliance efforts and support regulatory inspections.

5. Continuity Planning and Incident Response

Incident Response Team (IRT):

- Establish a specialized team to identify, look into, and mitigate security incidents. This is known as the Incident Response Team (IRT).
- For prompt incident management, create an escalation procedure with roles and duties that are well-defined.

Business Continuity Plan (BCP):

- Establish offsite backups and redundancy mechanisms as part of your Business Continuity Plan (BCP) to guarantee data and operational availability.
- Every three months, test recovery procedures to reduce downtime and confirm their efficacy.

Disaster Recovery Plan (DRP):

- The creation of a thorough plan for resuming activities following interruptions is the third step in the Disaster Recovery Plan (DRP).
- To improve preparedness, train employees and hone recovery techniques through simulated exercises.

Threat Analysis:

1. Unauthorized Access: In wireless networks, inadequate authentication procedures permit unwanted access, putting private information at risk.

2. Phishing Attacks: Workers may be tricked by phony emails, which could result in compromised credentials and illegal access.

3. Data Theft: When encryption isn't used, intellectual property is susceptible to theft and illegal distribution.

4. Compliance Violations: Inadequate procedures for adhering to regulations, including GDPR, can lead to fines and harm to one's reputation.

5. Insider Threats: Data breaches and operational sabotage may result from insiders' malicious or unintentional misuse of resources.

6. Cloud Misconfigurations: Vulnerabilities are caused by inadequately secured cloud resources, which expose private data to outside threats.

7. Disaster Recovery Failure: Inadequate backup preparations may result in extended outages and interruptions during unanticipated events.

Gap Analysis – Current vs Desired State:

Aspect	Current State	Desired State
Security Policies	Non-existent or outdated	Comprehensive and updated regularly
BYOD Policy	Unregulated	Clear, enforced with monitoring
Network Security	Basic encryption	Advanced encryption and segmentation
Compliance Frameworks	Partial GDPR compliance	Full compliance with monitoring tools
Insider Threat Detection	Limited mechanisms	Behavioral analytics and monitoring
Cloud Security	Basic configurations	Advanced monitoring and secure setups
Contingency Planning	Lacking	Robust disaster recovery and continuity plans

Strategies for Mitigation:

1. Updated Security Policies: To handle changing security issues and guarantee organizational coherence, create and implement updated policies.
2. The implementation of multi-factor authentication (MFA) can enhance network access security and lower the risk of unlawful entry.
3. Data Encryption: To prevent theft and unwanted access, encrypt intellectual

property and sensitive data.

4. Compliance Audits and Training: Regularly audit and instruct employees on security best practices and compliance standards.

5. Insider Threat Detection: To identify and stop malevolent or unintentional insider threats, use behavioral analytics.

6. Secure Cloud Configurations: Make sure that cloud service configurations are secure and conduct regular audits to find weaknesses.

7. Contingency Planning - Develop thorough plans that include failover systems and backups to keep things running in the event of an interruption.

4. Implementation Strategies

Development of Policies:

Policy Development:

To create unambiguous security standards, draft and implement BYOD and network security rules.

Improvements in Technology:

To fortify security infrastructure, implement sophisticated encryption technologies, access control systems, and insider threat detection systems.

Programs for Training:

Inform staff members about cybersecurity best practices, regulatory standards, and the value of insider threat awareness.

Improvements to Cloud Security:

Cloud Security Enhancements:

To fix vulnerabilities, make sure cloud configurations are safe, monitor frequently, and use third-party audits.

Frequent Audits:

To find and fix vulnerabilities early on, conduct regular security assessments and risk analyses.

Behavioral Analytics Integration:

Lower the risk of insider threats by putting in place real-time tools that track and identify unusual user activity.

Contingency Planning:

To guarantee operational resilience in times of emergency, create business continuity procedures and disaster recovery plans.

Service Level Agreements (SLAs):

To preserve responsibility and guarantee dependable service delivery, establish and enforce SLAs with cloud service providers.

Cost-Benefit Analysis (CBA)

Action	Cost	Benefits
Implementing BYOD policies	Moderate	Reduces risks of unauthorized access
Deploying encryption tools	High	Protects sensitive data, ensures compliance
Conducting staff training	Low	Minimizes human error and phishing risks
Enhancing insider threat detection	Moderate	Prevents sabotage and data misuse
Regular audits	Moderate	Identifies gaps and maintains system integrity
Cloud security enhancements	High	Protects data and ensures resilience
Contingency planning	Moderate	Ensures continuity during unexpected failures

Defining SLAs	Low	Guarantees cloud service accountability
---------------	-----	---

Evaluation of Cost-Benefit Analysis (CBA)

1. Return on Investment: Investments in encryption, insider threat detection, cloud security, and contingency planning minimize costly breaches and operational disruptions, protecting both financial and reputational assets.

2. Impact of Training Programs: Low-cost training initiatives successfully lessen human-related weaknesses including social engineering and phishing attacks.

Value of Audits and SLAs: The value of regular audits and well-defined service level agreements (SLAs) is threefold: they promote continuous improvement, guarantee system dependability, and uphold service provider accountability.

Graphic Improvements for Display

Diagrams:

Policy Hierarchy Charts: Showcase the hierarchical structure and connections among different security policies.

Potential dangers, their likelihood, and their impact levels are highlighted in the Threat Assessment Matrices.

Incident Response Workflows: Outline in detail how you identify and handle security incidents.

Detection Flows for Behavioral Analytics: Showcase methods for tracking and detecting unusual user activity.

Cloud Security Monitoring Structures: Showcase the instruments and procedures for protecting cloud infrastructure. Outline business continuity and catastrophe recovery plans using the Contingency Planning Workflows.

2. Graphs: Present the results of cost-benefit analyses and show how successful risk reduction techniques are by using visual aids.

Main Analysis Recommendations:

1. Adopt ISO/IEC 27001: Create a robust Information Security Management System (ISMS) tailored to NG's unique needs by Adopting ISO/IEC 27001.
2. Increase Security Measures: To strengthen system defenses, use behavioral analytics, multi-factor authentication (MFA), and sophisticated encryption techniques.
3. Create a Governance Board: Assemble a specialized group to oversee security guidelines, keep an eye on insider dangers, and guarantee legal compliance.
4. Employee Training: To lessen susceptibilities to phishing and social engineering techniques, give staff members continual training.
5. Regular Audits and Updates: To counter new and emerging threats, do regular security assessments and upgrade frameworks.
6. Increase Cloud Security: To safeguard cloud-based resources, put in place secure configurations, real-time monitoring, and thorough SLAs.
7. Create Contingency Plans: Develop thorough business continuity and catastrophe recovery plans to ensure

Efficacy Assessment of the Framework:

1. An organized approach to risk mitigation and compliance management is

provided by ISO 27001. By guaranteeing regulatory alignment, it provides enormous long-term benefits despite the high initial expenses.

2. CIS Controls: Offers useful, doable instructions that enable prompt deployment of crucial security measures.

For complete security coverage, integration with other frameworks is necessary.

Using quantifiable analysis, the FAIR Model facilitates risk assessment and allows high-risk concerns to be prioritized.

It places less emphasis on particular technological measures and more on risk assessment.

5. Further Insights and Improvements:

Improved Integration of the Framework :

- To increase versatility, combine components from other frameworks. For example: o For compliance and the ISMS foundation, see ISO/IEC 27001. For proactive threat detection, incorporate NIST's real-time monitoring capabilities.
- Use COBIT to oversee governance.
- Use ITIL for recovery planning and incident response processes.

Prospects for the Future

- Put AI-powered tools for threat analysis and mitigation into practice.
- Create a specialized staff to examine and update policies on a regular basis.

- Test the robustness of the architecture by conducting threat simulation exercises every two years.
- To guarantee access security, apply the concepts of Zero Trust Architecture (ZTA).
- Use Secure Access Service Edge (SASE) to protect your network and cloud.

6. Conclusion

Conclusion

By improving data protection, governance, and compliance, the suggested security framework tackles NatureGarden's major issues. Important conclusions highlight how crucial it is to reinforce security defenses by putting policies like ISO/IEC 27001, multi-factor authentication, encryption, and behavioral analytics into place. By lowering vulnerabilities and mitigating risks, the framework promotes operational resilience and guarantees adherence to laws like the GDPR. The framework supports NatureGarden's goals of protecting intellectual property, guaranteeing regulatory compliance, and preserving continuous operations by coordinating IT strategies with business objectives. NatureGarden can achieve long-term sustainability and a strong security posture by using this strategy.

7. References

1. M. E. Whitman and H. J. Mattord, Management of Information Security, 6th ed. Cengage Learning, 2019.
2. NIST, "Cybersecurity Framework," [Online]. Available: <https://www.nist.gov>. [Accessed: Jan. 8, 2025].
3. ISO, ISO/IEC 27031:2011 - Guidelines for ICT Continuity, International Organization for Standardization, 2011.
4. ISACA, COBIT Framework for IT Governance and Management. ISACA, 2023.
5. NIST, "Contingency Planning Guide," [Online]. Available: <https://www.nist.gov>. [Accessed: Jan. 8, 2025].

8. Appendices

Additional resources that offer more in-depth analysis and bolster the report's core ideas are included in the appendices section. These resources could consist of:

Detailed Tables: In-depth explanations of risk analyses, mitigation techniques, and implementation procedures.

Risk Matrices: Tables that show the impact and probability of risks that have been detected in order to rank mitigation activities.

Implementation Plans: Detailed instructions detailing the timetable, materials, and steps necessary to carry out the suggested security measures.

Additional Information: Any audit findings, research findings, or supporting material for the conclusions and recommendations.

Data Security final

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

67 / 100

PAGE 1

PAGE 2

QM

Abstract

Abstract should be the last to be written to outline the key finding or contribution that would interest key players of what was done.

QM

New page

Start on new page

PAGE 3

QM

Conjunction

Do not start a sentence with a conjunction such as but, and, because, etc.

QM

Acronyms

Spell out all acronyms first time used.

PAGE 4

PAGE 5

PAGE 6

PAGE 7



Table

Number and name your table



Table

Number and name your table



Conclusion

Your conclusion can be improved; it should summarised your key areas of the report. Try to use paragraphs instead of one flow.

GRADING FORM: L7 DSGC (ACCA7028)

NIKHITHA AKULA

66.50

ENGAGEMENT WITH LITERATURE

Your work must include articles published by peer reviewed journals, conference proceedings, books, and related website (e.g. IEEE, ACM, Science direct). Information from website such as ehow, wiki, forums, etc. will not be accepted (15 marks)



While you have provided a reference list, the body of your report lacks referencing. Also you have not engaged peer reviewed articles, which are credible sources.

8

You are awarded marks based on:
awarded for:

- Diversity of sources and materials used
- Key concepts discussed
- Appropriate summaries of articles and level of critical appraisal of literature
- Application of appropriate referencing conventions

KNOWLEDGE AND UNDERSTANDING

Your work must demonstrate understanding of concepts and underlying principles. You should explain and analysis the chosen area

in a meaningful way. (15 marks)



Demonstrated specialised area of knowledge. Understanding of the concepts of the subject informed by current research. Critical awareness of current problems and insights.

11

You are awarded marks based on:

- Depth of the research
- Strength of the statements
- Structure of the paper
- Quality of the report

COGNITIVE AND INTELLECTUAL

Your work must demonstrate critical analysis and evaluation of your approach for security framework and model. Your work must also justify your findings and provide evidences. (40 marks)



Sound critical evaluation/ critique of current research and methodologies, Proposes new hypotheses, where appropriate.

30

Marks are awarded based on:

critical analysis and evaluation of your approach for security framework and model.

How you justify your findings and provide evidences.

PRACTICAL SKILLS

Marks will be awarded based on the quality of and level of detail provided for the design approach; diagrams, table, charts and any other design methods utilise will enhance marks. (20 marks)



You have provided relevant and appropriate tables. It would be good to use other form of diagrams could be used to aid your own approach and other areas within your report.

Marks are awarded based on the quality of and level of detail provided for the design approach; diagrams, table, charts and any other design methods utilise will enhance marks.

12

TRANSFERABLE SKILLS FOR LIFE

This should be presented in an academic way and therefore must include an abstract, an introduction, a conclusion and a list of references. (10 marks)



Please see comments within your report to improve this section. Your work could do with formatting.

5.5