**Common Rubric Criteria for ITCO 361**

**Expectations:** Student work at the undergraduate level is expected to focus on a broad overview of an academic discipline, along with—where appropriate— basic theoretical frameworks of professional practices and familiarity with discipline‐specific tools and their application. Blooms taxonomy levels only apply for IT content criteria.

*Version 5.0 – October 2017*

*DNS = Did Not Submit N/A = Not Applicable to Assignment*

**IT Content Criteria**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IT Content Criteria** | **Exemplary (5)** | **Accomplished (4)** | **Proficient (3)** | **Partially Proficient (2)** | **Unacceptable (1)** |
| **Blooms Taxonomy Level** | **Analysis** | **Application** | **Comprehension** | **Knowledge** | **Knowledge** |
| **Information** **Security**  **Attacks, Defense, and Investigation**  *[ATTACK/DEFENS/INVEST]* | Demonstrates full understanding of hardware and software vulnerability as well as hardware and software tools that can be used to secure organizations’ information systems. Describes the attacks, countermeasures, security mechanisms, information states,  and digital forensics. Demonstrates complete understanding of how various security tools including encryption tools, packet filters, content filters, hash algorithms, can be used to design secure infrastructure. | Demonstrates sound understanding of hardware and software vulnerability as well as hardware and software tools that can be used to secure organizations’ information systems. Describes the attacks, countermeasures, security mechanisms, information states, and digital forensics. Demonstrates sound understanding of secure information architecture. | Demonstrates the ability to explain various security vulnerabilities as well as how software and hardware security can be compromised by hackers. Demonstrate good understanding of security hardware and software as well as the ability to explain how security hardware can be used to provide physical and logical security. | Demonstrates ability to list and describe security vulnerabilities. Demonstrate basic understanding of software and hardware security can be compromised by hackers. Demonstrate basic understanding of security hardware and software but cannot fully explain how security hardware can be used to provide physical and logical security. | Does not demonstrate an acceptable understanding of security vulnerabilities and how and hardware security can be compromised by hackers as well as mechanisms that can be used to provide security for hardware and software. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IT Content Criteria** | **Exemplary (5)** | **Accomplished (4)** | **Proficient (3)** | **Partially Proficient (2)** | **Unacceptable (1)** |
| **Blooms Taxonomy Level** | **Analysis** | **Application** | **Comprehension** | **Knowledge** | **Knowledge** |
| **Information** **Security**  **Policy and Operational Issues**  *[POLICY/OPS ISSUES]* | Demonstrates full understanding of how technical and administrative controls can be used to secure information systems. If given a design scenario, describes the security controls that can be used to protect and organization and compare various tools that can be used for logical and physical controls. | Demonstrates sound understanding of how technical and administrative controls can be used to secure information systems as well as the ability to recommends various documents that can be used for administrative control of physical and data security. | Demonstrates the ability to explain logical and physical security as well as security management processes such as information security policies, standards, baselines, guidelines, and procedures as well as  the purpose of technical and administrative controls. | Demonstrates ability to list and define logical and physical security mechanisms as well as security management processes such as information security policies, standards, baselines, guidelines, and procedures. | Demonstrates a lack of understanding of logical and physical security as well as security management processes such as information security policies, standards, baselines, guidelines, and procedures. |
| **Information Security**  **Services and Threat Analysis**  *[SRVS/THREAT ANALYSIS]* | Demonstrate full understanding of security requirements analysis, risk analysis, analysis, cost‐benefits, analysis, risk identification, and risk mitigation. Demonstrates full understanding of the various methodologies used to conduct risk analysis and perform systems certification and accreditation in organizations. | Demonstrate sound understanding of security risk identification and risk mitigation processes. Demonstrates sound understanding security certification and accreditation process as well as various documents that are produced when conducting system certification and accreditation tasks. | Demonstrate the ability to explain IT risk assessment and audit processes as well as an understanding of security risk identification and risk mitigation processes. Explains information security certification and accreditation process. | Demonstrates the ability to describe the processes that are used to conduct IT risk assessment and security audits as well as the issues that are involved in information security management in organizations. | Demonstrate a lack understanding of risk assessment and IT security audits basics as well as failure to demonstrate basic steps used to manage information security in organizations. |
| **IT Content Criteria** | **Exemplary (5)** | **Accomplished (4)** | **Proficient (3)** | **Partially Proficient (2)** | **Unacceptable (1)** |
| **Blooms Taxonomy Level** | **Analysis** | **Application** | **Comprehension** | **Knowledge** | **Knowledge** |
| **Teamwork**  **Basic Team Skills**  *[TEAMWORK]* | Demonstrates advanced capabilities in developing and implementing strategies surrounding all areas: group conflict resolution, team building, ensuring team integrity, and team management objective identification. | Demonstrates capabilities in developing and implementing strategies surrounding two or more areas: group conflict resolution, team building, ensuring team integrity, and team management objective identification. | Demonstrates capabilities in developing and implementing strategies surrounding at least one area: group conflict resolution, team building, ensuring team integrity, and team management objective identification. | Demonstrates evolving capabilities in developing and implementing strategies surrounding one area: group conflict resolution, team building, ensuring team integrity, and team management objective identification. | Demonstrates inability in developing and implementing strategies such as: group conflict resolution, team building, ensuring team integrity, and team management objective identification. |

**General Education Criteria**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **General Education Criteria** | **Exemplary (5)** | **Accomplished (4)** | **Proficient (3)** | **Partially Proficient (2)** | **Unacceptable (1)** |
| **CRITICAL THINKING** Synthesize different ideas, beliefs, perspectives, and approaches in the process of arriving at conclusions or solutions (includes ethical reasoning and awareness of cultural diversity)**.** | Demonstrates outstanding or exemplary ability to integrate different ideas, beliefs, perspectives and approaches in the process of arriving at conclusions or solutions as required by the assignment (includes issues related to ethical questions)  Demonstrates outstanding or exemplary ability to proactively seek and incorporate multiple and diverse perspectives when working with one’s own and other cultures (as applicable). | Demonstrates clear ability to integrate different ideas, beliefs, perspectives and approaches in the process of arriving at conclusions or solutions as required by the assignment (includes issues related to ethical questions).  Demonstrates clear ability to seek and incorporate multiple and diverse perspectives when working with one’s own and other cultures (as applicable). | Demonstrates adequate or proficient ability to integrate, different ideas, beliefs, perspectives and approaches in the process of arriving at conclusions or solutions as required by the assignment (includes issues related to ethical questions).  Demonstrates adequate ability to seek (when instructed), and incorporate multiple and diverse perspectives when working with one’s own and other cultures (as applicable). | Demonstrates inadequate or partially proficient ability to integrate, different ideas, thoughts, perspectives and approaches in the process of arriving at conclusions or solutions as required by the assignment (includes issues related to ethical questions).  Demonstrates partially proficient ability to incorporate multiple and diverse perspectives when working with one’s own and other cultures (as applicable). | Demonstrates limited ability to integrate different ideas, thoughts, perspectives and approaches in the process of arriving at conclusions or solutions as required by the assignment (includes issues related to ethical questions).  Demonstrates limited ability to incorporate multiple and diverse perspectives when working with one’s own and other cultures (as applicable). |