1. **Course number and name**: CSCI 5531 Systems and Software Assurance

2. **Credits and contact hours**: 3 credit, 3 contact

3. **Instructor’s or course coordinator’s name**: Vladan Jovanovic, PhD

4. **Textbook, title, author and year**: IAM/IEM
   a. **Other supplemental materials**: None

5. **Specific course information**
   a. **Brief description of the content of the course (Catalog Description)**
      This course presents a body of knowledge in systems and software assurance and evaluation including security, safety, and integrity analysis. The core part of the course is software assurance where students are exposed to code and architectural analysis, secure coding practices, standards, and tools. The course also explores standards in modeling internal security at the organizational level and will involve students in risk assessments, comprehensive assurance planning, as well as an array of countermeasure considerations.
   b. **Prerequisites**: A minimum grade of “C” in CSCI 1302 and CSCI 3432
   c. **Indicate whether a required, elective, or selected elective course in the program**
      Elective course for BS-CS.

6. **Specific goals for the course**
   a. **Specific outcomes of instruction, ex. The student will be able to explain the significance of current research about a particular topic.**

<table>
<thead>
<tr>
<th>Course Learning Outcomes</th>
<th>Student Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand international and national standards (including ISO 17799) as frameworks in modeling internal security standards, policies and procedures.</td>
<td>1a, 1e, 1g</td>
</tr>
<tr>
<td>Describe the course topics in the explicit context of technologically rich environments of modern software and data intensive systems and networks.</td>
<td>1a, 1b, 1f</td>
</tr>
<tr>
<td>Understand the most relevant systems assurance issues in situations characterized by complex interdependencies, for example associated with multiple locations, substantial software development, large data center responsibilities and multilayered networks.</td>
<td>1e, 1g</td>
</tr>
<tr>
<td>Complement technical issues underlining non-electronic security with leadership ones in all areas of security including those for large and medium-sized organizations.</td>
<td>1e, 1f, 1g</td>
</tr>
</tbody>
</table>
Perform risk assessments, comprehensive assurance planning, improvement of policies and procedures as well as budget preparations, an array of risk assessments and countermeasure planning  

| Perform relevant calculations in capacity planning, storage virtualization (using RAID for fault tolerance and backups) and similar. | 1b, 1c, 1i |

b. Student Outcomes

- 1a: An ability to apply knowledge of computing and mathematics appropriate to the discipline
- 1b: An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution
- 1c: An ability to design, implement and evaluate a computer-based system, process, component, or program to meet desired needs
- 1e: An understanding of professional, ethical, legal, security, and social issues and responsibilities
- 1f: An ability to communicate effectively with a range of audiences
- 1g: An ability to analyze the local and global impact of computing on individuals, organizations and society, including ethical, legal, security and global policy issues
- 1i: An ability to use current techniques, skills, and tools necessary for computing practice

7. Brief list of topics to be covered

- ISMS, plans, and policies
- Drawing Networks
- Oracle DB Hardening
- XP event log
- DMZ/Firewall
- Data Backup
- SAINT/NESUS
- Countermeasures
- ISSO duties
- Risks, Assets, Policies
- IA framework, ISMS, IAM
- IAM, Sec. Plan-ISMS
- NIST guidelines, Security Ops
- Access control, Incident response
- Personal Sec, Intrusion Detection
- Secure Software Development
- Security Metrics and Reporting