# CS 405 Project Two Script Template

Complete this template by replacing the bracketed text with the relevant information.

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | Andres Cruz |
| **2** | Defense in depth discusses the idea of security being an overarching implementation that starts at the inception of development. |
| **3** | There are 10 security principles to discuss and identify |
| **4** | Along with the principles, they also have coding standards that apply to them. These coding standards attempt to mitigate risk and errors. |
| **5** | Encryption policies discuss handling of data during its different phases. The phases include data at rest, data at flight and data in use. Each phase provides an avenue for attackers to intercept data and should be mitigated with encryption. |
| **6** | Triple A policies provide a method of safe guarding data by forcing users to authenticate, authorize and account. All three assist in ensuring that data is not misused or stolen. |
| **7** | Unit testing gave us a chance to utilize software tools that could be written to test for errors. The tests could be customized to fit the needs of the software being developed |
| **8** | The automation summary maps out the whole process and acts a visual guide throughout the defense in depth process. The automation summary can also be edited and improved upon at an point in the process. |
| **9** | Tools assist in detecting and identifying risks and errors before they are too large and remediation bevomes costly. |
| **10** | Risks and benefits put in place the effects can be very different. All risks should be reasonably mitigated although there will always be a level of risk that you accept. The risks you accept, typically have a low severity, probability, or a low remediation cost. It isn’t possible to mitigate all risks as the cost to do so would outweigh the benefit of the mitigation. |
| **11** | My recommendation is to stay current with patches and updates. Always monitor the security measures put in place for new and improved methods of implementation and to be aware of dated or exploited tools that would need to be replaced |