Modern computer applications are typically exposed to the Internet via the host machine or a networked system, thus making them vulnerable to attack from many different entities on a global scale. Developing secure applications means designing, implementing and testing code that can withstand attacks by malicious entities. Additional challenges are posed by the trend towards DevOps, i.e. merged development and operations phases, as well as the increased use and combination of technologies such as Cloud, IoT, ICS, mobile applications, and hybrid and converged deployments. These trends enable rapid applications development, but also increase the potential for security vulnerabilities. The core cybersecurity principles of confidentiality, availability and integrity can be disrupted by attacks on insecure systems and applications, leading to financial and reputational loss, and possibly legal prosecution. This module covers fundamental issues that need to be understood when designing and building secure systems and applications. It aims to provide students with an overview of the common technical security controls available to prevent security incidents and to mitigate risk, as well as an understanding of the importance of secure development processes, security policies, and appropriate project management.