Aims
This module analyses the role of security from the perspective of business application design. The aim is to learn the fundamental processes that need to be incorporated into the application development lifecycle, and thus how to integrate security as a core component within an application architecture. This module uses case studies to support the learning of these fundamental application security design skills, to understand what decisions need to be made to both meet business requirements and to mitigate information security risks.

Pre-requisites
IYM001 Security Management, IYM002 Introduction to Cryptography and IYM003 Network Security

Essential Reading
- Principles of Information Security (Whitman and Mattord)

Learning Outcomes
On completion of the module the students should be able to:
- Recognise a variety of security issues that arise in applications
- Review how the various security issues in a particular application relate to one another
- Understand how and why businesses address specific security concerns in their applications
- Appreciate various aspects of integrating security into the application development lifecycle
- Analyse how security aims are met in a particular application
- Evaluate the effectiveness of security mechanisms in the technical and business context of the case studies

Assessment
This module is assessed by a two hour unseen written examination.
This module is split into four parts. The first half of the course covers general application security theory, processes and issues. In the second half of this module, we use payment applications as case studies of the theory learned in the first two parts.

**Part 1 – Application development**
To begin the course, we need to consider security management processes in the context of the application lifecycle. This draws upon some of the principles expounded in the ‘Security Management’ module (IYM001) such as audit and incident handling. From this, we focus on how risk assessment is implemented at the level of application security. We learn how to model an application to assess its vulnerabilities, and how these might be exploited by well-known threats to application security. We also consider how the results of a threat analysis are communicated to the business as part of a risk assessment process.

**Part 2 – Application security technology**
In this part we explore essential application security technologies. We begin with an introduction to information security standards and key management. We review relevant material from the ‘Introduction to Cryptography’ module (IYM002), but in the context of how standards can be used to meet business requirements. We focus on key management frameworks, for both symmetric and public key cryptography, as they are essential for any cryptographic based application security.

Next we explore identity management and how it relates to application security. This starts by discussing what identity means from the various perspectives of business, user and government and why it is important to certain types of application and business process. We extend the discussion to single-sign-on schemes and look at various identity management initiatives.

Finally, this part looks at web application security, an area to which identity management systems are well suited. We look at the security issues that impact web applications, revisit some of the security techniques that we learned in the core modules, and then extend them by examining security initiatives which include XML security, SAML and WS-Security.

**Part 3 – Payment security**
The second half of the course is a case study of payment applications, which draws upon the topics studied in parts 1 and 2. In order to understand and analyse current payment security, we cover the background of several related areas, beginning with general payment models. The previous material in this module means we are in a position to study and understand the threats and risks in such models, before examining how the financial industry has proceeded to combat the security issues with the use of smart card technology and the EMV payment application.

**Part 4 – Secure electronic commerce**
In this final part we extend the case study to secure electronic commerce schemes for Internet applications. We will evaluate the effectiveness of two proposals, investigating both technical security properties and the arising business issues. This part, and the module, finishes with an insight into the current security landscape, looking at for example: current attack methods, the importance of trust and identity, and the role of information security in business.