In an age of outsourcing tasks that are not considered to be a core competency of the business, organisations have often relied on external consultants for matters pertaining to security. In actual fact, most companies could have utilized existing skill-sets in-house to produce a security risk management program, if only they knew what steps to take, and how to go about it all. Evan Wheeler in his book on information security risk management does just that— he equips professionals tasked with security, with the thinking required to create a program that is more preoccupied with the complex strategic-level questions than the technical or operational level skills required to execute particular tools and applications. Wheeler, a practicing security consultant himself, asks the big questions which technicians usually cannot answer beginning with the “why” question. From Wheeler’s perspective it is important that those who have been given the role to manage security, have the upper management support to act as “internal” consultants with clear roles and responsibilities defined from the outset, given resource allocation limitations. Wheeler’s book offers a simple to understand risk management lifecycle where the business owners are empowered to manage their own risks with the security team playing a supporting role as policymaker and overseer. Security thus becomes everyone’s problem.

Wheeler organizes his book in three very accessible parts. The first part provides an introduction to risk management which positions security within an organizational context as well as introduces the risk management lifecycle. The second part which is on risk assessment and analysis techniques, includes chapters on risk profiling, formulating a risk, risk exposure, security control, risk evaluation and reporting. And the final third part is on building and running a risk management program, with a focus on generating a blueprint for security. What is practical about this book is that there are quick guides to follow with detailed descriptions for each part, sub-part, and individual steps in the stages of the risk management workflow. The numerous template pro-formas included in the book also presents another tangible way for practitioners to get involved in risk management, providing an approach towards identifying and mapping an organisation’s risks and mitigating them. The book also contains generic case studies wherever appropriate. The appendices which include example profiles and questionnaires are additionally supported by partly-filled out tabular forms in the main body of the text. Sample worksheets, workflow diagrams, tips and tricks, and associated warning signals along the way are also illustrative, helping the information security professional to get started straight away without falling into recognized pitfalls. One thing that makes this
book so useful is the style that it has been written in, a credit to Wheeler that it allows for
direct engagement and is easily digestible by any one at any level in the organisation.

A distinct omission in Wheeler’s book is an acknowledgment of the importance of the
existence of international standards, such as the International Standards Organisation’s
(ISO) 27000 series of standards on information security matters, and also other IT
governance related frameworks, such as CoBIT. While the claim is made that Wheeler
offers a new approach in his book, shaking up old paradigms, it is probably more correct
to say that Wheeler has taken tried and tested elements in security management, and has
presented them in a more accessible way to the professional who might not necessarily
have a security background. The success of the book is in its presentation of the security
risk management lifecycle.

With the admission that the qualitative versus quantitative approach to risk assessment
continues to be debated by the industry, Wheeler spends some time describing the
implementation of each approach, tending towards a little bit of this, and a little bit of that,
in his self-professed cookbook of risk management. But for the greater part, Wheeler is
obviously encouraging of the qualitative assessment given the length of space attributed
to this approach in the book. One criticism of solely using either a qualitative approach or
a quantitative approach to risk assessment has very much to do with how to interpret the
meaning behind the results. Take for example a quantitative assessment based on
annualized loss expectancy (ALE). It is very likely to have two risks end up with exactly
the same dollar figure. The fallback position in this situation is to a qualitative assessment
result to weigh up which is more significant to the given organizational context when
addressing the risk concerns. Innovative modeling approaches which utilize a hybrid
approach are now being implemented in many organisations. The absence of this
discussion from the book is noted, Wheeler taking the perspective that most organisations
use a qualitative approach alone because the quantitative assessment approach relies on
too many historical facts which are usually unknown, and upon complex equations.

Another detail that seems to have not been addressed is that security risk requires
business owners to consider interdependencies at a variety of layers. These layers can be
considered as categories of resources, i.e., applications, infrastructure, environment,
facility, business unit and vendor, each of which have impacts at the financial, legal,
reputational or regulatory levels. The failure to recognize interdependencies as being an
integral dimension of risk assessments can lead to detrimental effects in any risk
management program. Scenario analyses conducted to gauge the consequences of
negative effects on a crucial element in the security value chain might mean that controls
and mechanisms to protect that element are of greater significance than another element
that might have a bigger risk exposure but is not underlying most other processes. Much
of this work on interdependencies was begun in the critical infrastructure protection (CIP)
domain but has been applied in many other areas, including in the banking sector which
has been preoccupied with risk appetite since consumers have begun to use emerging
technologies do conduct their transactions.
Wheeler’s book is predominantly a practitioner’s guide to security risk management but can also be used as a teaching text to help engineers, students of security, information assurance, or information systems more broadly. The key message that Wheeler is emphasizing is that risk is at the core of security, and at the heart of every business. Despite that the book lacks key referencing from academic literature, it can still be used as the basis for setting a large-scale team assignment on devising a risk management program from the ground up for a real organisation. Security professionals in banks will particularly find the book relevant, with examples from this sector discussed or alluded to.