Information Security Forum

Time to Grow

Using maturity models to create and protect value

A maturity model is a business planning tool that helps organisations target the right amount of maturity at areas that create or protect value. The ISF's report ***Time to Grow: Using maturity models to create and protect value*** helps organisations to assess their current information security maturity, translate business objectives into a target maturity, and develop actionable plans to achieve it.

We identified three key benefits that using a maturity model provides. It enables organisations to:

Build consensus

- by communicating and engaging with the organisation to agree a shared vision of how information security can support strategic goals.
- by facilitating business-based discussions with decision-makers.

Prioritise investment

- by using the maturity model for planning and prioritising specific actions to achieve strategic goals.
- by supporting normal business planning and focusing on areas of value to the organisation.

Demonstrate progress

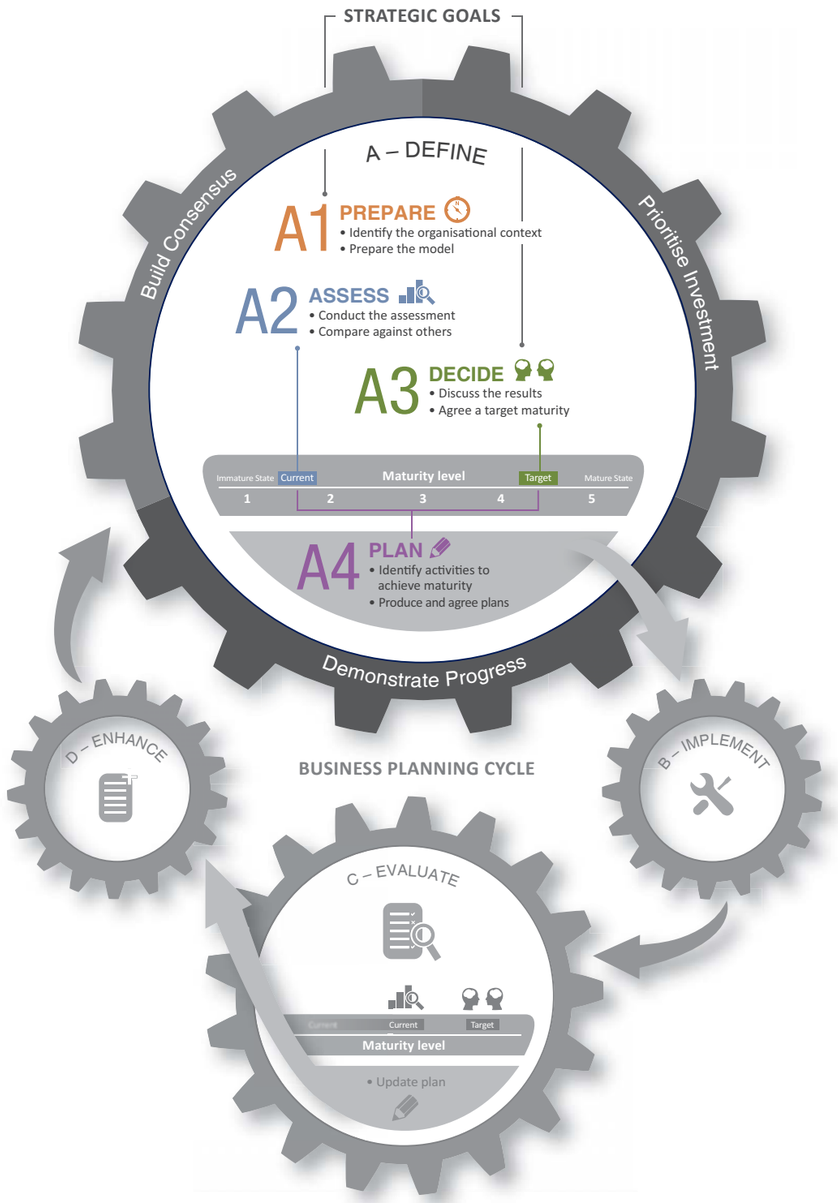
- by using maturity as an informative and consistent metric to measure and compare progress across different areas of information security or business units.
- by allowing the CISO to answer senior management questions about how the organisation compares to its peers and competitors.

Using a maturity model also acts as a catalyst for engagement with the wider business through the process of deciding where to target maturity and agreeing the appropriate maturity level. It provides a framework and common language for discussion and debate on how information security can enable the organisation to achieve its goals.

The ISF's ***Time to Grow: Using maturity models to create and protect value*** contains a four-phase process to make effective and efficient use of any maturity model. The report is accompanied by the ***ISF Maturity Model Accelerator Tool***, a high-level maturity model based on the ***ISF's Standard of Good Practice for Information Security***.

Using a maturity model for business planning

The ***ISF's four-phase process*** for using a maturity model (A1 – A4) is highlighted below. This process sits within the first step of a regular business planning cycle (A – D), enabling CISOs to integrate the use of a maturity model into 'business as usual'.



The report shares lessons learnt and practical examples from ISF Members who have successfully used maturity models for business planning. As a result, an organisation can spend the minimum necessary time on the assessment and more time implementing improvements. The four Phases of the process are:

PREPARE

THE ORGANISATION AND THE MATURITY MODEL

Step: Identify the organisational context: The assessment needs the right focus. From the start, this process is focussed on organisational value.

Step: Prepare the model: The report explains the three types of model (activity, capability and hybrid) their uses and limitations in information security and gives simple guidelines on how to choose the right one.

Tasks: understand strategic goals; scope the assessment; identify and engage stakeholders; sell the idea

Tasks: select the model; adapt the model

I want to...	Use...
know what other organisations are doing in one discipline of information security (e.g. vulnerability management)	an activity maturity model
compare our capability across several different disciplines of information security	a capability maturity model
compare high-level activities and our capability in those activities across several disciplines of information security	a hybrid maturity model

ASSESS

CURRENT MATURITY AND, IF NECESSARY, THE MATURITY OF OTHER ORGANISATIONS

Step: Conduct the assessment: There are four major factors to consider for a maturity assessment: independence, interaction, evidence and validation. This Phase details these factors and the issues that will affect your decisions.

Step: Compare against others: There is often executive interest in how an organisation compares against their peers and competitors. The report describes five potential sources of data to enable comparison.

Tasks: tailor the assessment; execute the assessment

5 sources of data: Regulator required, trade body, third-party data, ask, guess

DECIDE

AN APPROPRIATE TARGET MATURITY FOR THE ORGANISATION

Step: Discuss the results: The report presents a number of insights into maturity and its costs to inform the discussion and enable business and information security leaders to understand their current maturity and how it could be improved.

Step: Agree a target maturity: Choosing the target maturity is fundamental to using a maturity model and our research has identified three different approaches. The approach an organisation takes will depend on its experience of information security.

Tasks: group the results; prepare audience-specific visual aids

Tasks: identify ideal maturity; set a target maturity

LIMITED EXPERIENCE: set a small increase in a few areas

MODERATE EXPERIENCE: compare against others

HIGHLY EXPERIENCED: focus on value, compliance and risk

PLAN

TO ACHIEVE TARGET MATURITY

Step: Identify activities to achieve maturity: To achieve the target maturity, a list of activities needs to be developed.

Step: Produce and agree plans: This process explains how to turn your decisions into prioritised plans for action.

Outcome: Following this process will assist the security function to produce a prioritised plan to develop maturity in areas that support the organisation's strategic goals.

The ISF Maturity Model Accelerator Tool

The ***ISF Maturity Model Accelerator Tool*** combines tried and tested concepts of maturity with the structure and language used in the ***ISF's Standard of Good Practice for Information Security***. This allows users to assess and plan their information security maturity in line with ***the Standard***. The tool can be used as is, or tailored to concentrate on the areas of most value within your organisation.

Where next?

The ISF's ***Time to Grow: Using maturity models to create and protect value*** report helps organisations to assess their current information security maturity, translate business objectives into a target maturity, and develop actionable plans to achieve it. The report contains a four-phase process to make effective and efficient use of any maturity model. The report is accompanied by the ***ISF Maturity Model Accelerator Tool***, a high-level maturity model aligned with the ***ISF's Standard of Good Practice for Information Security***.

This report helps organisations:

- get the greatest return on investment possible from using a maturity model.
- identify a target maturity that will help achieve strategic goals.
- make an informed decision about maturity, accounting for hidden costs and considerations.

The report is supported by an implementation space on the ISF Member website, ***ISF Live***, which contains a facilitated forum for Members to discuss related issues and solutions.

Time to Grow: Using maturity models to create and protect value is available free of charge to ISF Members, and can be downloaded from the ISF Member website www.isflive.org. Non-Members can purchase the report by contacting Steve Durbin at steve.durbin@securityforum.org.

Contact

For more information, please contact:
Steve Durbin, Managing Director
US Tel: +1 (347) 767 6772
UK Tel: +44 (0)20 3289 5884
UK Mobile: +44 (0)7785 953 800
Email: steve.durbin@securityforum.org
Web: www.securityforum.org

About the ISF

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management by developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work programme. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. And by working together, Members avoid the major expenditure required to reach the same goals on their own.

Disclaimer