Now that cyber security has the attention of the board and information risk is on the agenda, Chief Information Security Officers (CISOs) are being asked increasingly tough questions about security investment and risk.

It’s never been more important for CISOs to be ready to answer these questions and articulate how the information security function is contributing to strategic priorities while helping to balance information risk.

Yet many are struggling to do so.

ISF research has found that many CISOs are reporting the wrong key performance indicators (KPIs) and key risk indicators (KRIs). In addition, they have little or no interaction with the audiences to whom they are reporting.

They are guessing at what their audiences need and are missing the mark when attempting to provide ongoing management reporting on topics including:

- information security effectiveness
- organisational risk
- information security arrangements.

Engaged Reporting provides a way for CISOs to succeed by engaging with audiences to identify common interests, determine relevant data, generate reliable insights and create impact supported by the right KPIs and KRIs. This supports informed decision-making.

Are you ready to answer these questions?

- Can we reduce security costs without exposing the business to significant risks?
- How secure are our critical information assets? How secure do they need to be?
- What implications could a breach or an incident have on the business?
- What is the information security function doing to support new initiatives?
- Is the business sufficiently securing its core products and services?

This report provides guidance and mechanisms that will help CISOs and their teams turn technical security metrics into reporting that is aligned to the strategic aims and goals of the organisation by virtue of meaningful conversations.
The ISF Approach for Engaged Reporting (ISF Approach), shown below, provides a four-phase, practical approach for creating key performance indicators (KPIs) and key risk indicators (KRIs) that support informed decision-making. The ISF Approach encourages CISOs to forge a path to having the right conversations with the right people. It is designed to be applied up, down and across at all levels of an organisation.

**THE ISF APPROACH FOR ENGAGED REPORTING**

**PHASE A: ESTABLISH RELEVANCE**

Step 1. Understand the business context
Step 2. Identify audiences and collaborators
Step 3. Determine common interests
Step 4. Identify the key information security priorities
Step 5. Design KPI/KRI combinations
Step 6. Test and confirm KPI/KRI combinations

**PHASE B: GENERATE INSIGHTS**

Step 1. Gather data
Step 2. Produce and calibrate KPI/KRI combinations
Step 3. Interpret KPI/KRI combinations to develop insights

**PHASE C: CREATE IMPACT**

Step 1. Agree conclusions, proposals and recommendations
Step 2. Produce reports and presentations
Step 3. Prepare to present and distribute reports
Step 4. Present and agree on next steps

**PHASE D: LEARN AND IMPROVE**

Step 1. Develop learning and improvement plans

---

**ENGAGING TO REPORT**

This builds an essential understanding of the needs and reporting preferences of the audiences. In particular, it identifies reporting requirements that are in line with strategic aims and business goals. It also improves the CISO’s understanding of business drivers and priorities in order to identify common interests and KPI/KRI combinations.

**ENGAGING TO COLLABORATE**

This enables the CISO to gather, calibrate and interpret information. It also identifies existing reports that can be used to enrich reporting.
The fundamental concepts of Engaged Reporting can be represented by an equation, as follows:

Engaged Reporting ties performance and risk management together – through KPI/KRI combinations.

**KPI**

An expression of progress towards strategic aims and business goals. Predominantly backward looking.

Reports on:

- Actual progress against plans and targets

Also provides a basis for:

- Identifying trends for future resource availability and performance

**KRI**

A predictor of events that can affect the achievement of strategic aims and business goals. Predominantly forward looking.

Reports on:

- New and previously identified uncertainties, expressed in terms of their likelihood and impact

Also provides a basis for:

- Assessing whether previous predictions on risk (as a function of likelihood and impact) were sound, thus identifying trends on quality of foresight

**Top tips**

- Align information security priorities with the strategic priorities of the organisation
- Take the time to engage with the right audiences and build a coalition
- Use the language and terminology of the audience
- Always ask for feedback to keep reporting relevant and meaningful
- Treat reporting as an opportunity to develop trust and influence beyond reporting

**Fictional case study**

A fictional case study accompanies each phase of the ISF Approach, describing how a CISO uses the approach to align the information security function’s priorities with the strategic priorities of the business and answering some of the questions being asked by the board.
Engaged Reporting describes the fundamental components of successful reporting and provides a practical approach for CISOs to engage up, down and across at all levels of their organisations – to identify and use relevant KPIs and KRIs necessary for fact-based decision-making. We recommend that the CISO in each ISF Member organisation:

‒ consider their specific goals for reporting and plan a way forward to achieve Engaged Reporting
‒ understand the fundamental concepts underlying the approach
‒ apply the approach: bearing in mind that this is a flexible and iterative process that will evolve in line with changes in their organisation and resulting reporting requirements
‒ benefit from the reporting indicators and example reporting formats in this report
‒ give careful consideration to the concepts in this report and consult other related ISF materials including IRAMs: The Next Generation of Assessing Information Risk, From Promoting Awareness to Embedding Behaviours: Secure by choice, not by chance, Information Security Strategy: Transitioning from alignment to integration, Engaging With The Board: Balancing cyber risk and reward and Information Security Governance: Raising the game
‒ use ISF Live to share their thoughts, information, articles and other relevant materials, and to debate the ISF’s findings in this report.

Consultancy Services from the ISF provide Members with the opportunity to purchase professional support to supplement the implementation of ISF products.

Engaged Reporting is available free of charge to ISF Members, and can be downloaded from the ISF Member website www.isflive.org. Non-Members interested in purchasing the report should contact Steve Durbin at steve.durbin@securityforum.org.