COMPASS

Responsible Innovation Roadmap

Cyber Security

Step 1: Embed vital and review desirable aspects for company management.

Step 2: Reflect on integration of responsible innovation practices throughout the entire innovation process of your company.

COMPANY MANAGEMENT

Vital

□ Developing, reviewing or re-affirming a company mission statement to set the context for responsible innovation. Demonstrating therein a commitment to the care and protection of employees, clients and other stakeholders.

□ Ensuring commitment to ethical and secure modes of operation for products and services at stages of (a) research; (b) design and service development; (c) marketing and sales; (d) service operation.

□ Ensuring impact assessments are undertaken at all stages (taking account of the range of stakeholders and wider environmental issues). Linking these to procedures (with clear lines of responsibility) that facilitate the making of key decisions to move forward or halt the innovation process.

□ Having emergency and contingency plans in place for breaches that could compromise confidential and/ or private data.

□ Demonstrating readiness to engage with and respond to feedback from clients and ensuring that protocols are in place for dealing with feedback (openness to information sharing) and involving them in decision-making processes where appropriate.

□ Adhering to codes of practice and applicable standards. Obtaining certification after compliance established via an accredited external agency, where appropriate.

□ Maintaining an Ethics Board or similar to help 'cement' ethical culture within the company.

□ Developing and/or maintaining a code of conduct that is transparent and publicly available.

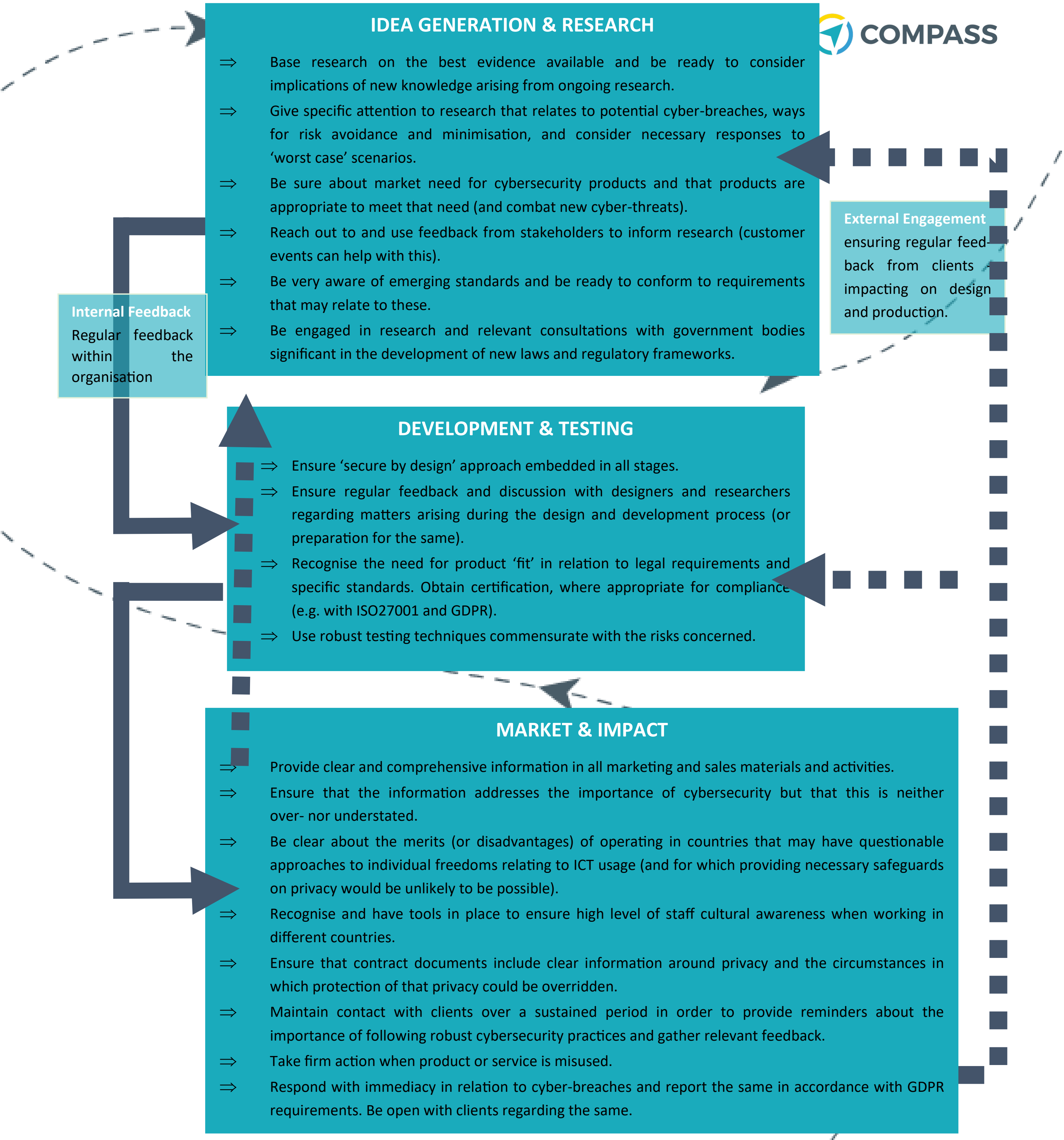
□ Working and collaborating with a relevant industry association body with a shared ethos and, with or independently of it, to contribute to standards development in the field.

Desirable

□ Being forward in raising public awareness of cybersecurity issues; and providing support for science education (with a gender-balanced approach).

□ Leaving room for fundamental research (where appropriate in collaboration with centres of expertise) applicable to the sector.

COMPASS



IDEA GENERATION & RESEARCH

⇒ Base research on the best evidence available and be ready to consider implications of new knowledge arising from ongoing research.

⇒ Give specific attention to research that relates to potential cyber-breaches, ways for risk avoidance and minimisation, and consider necessary responses to ‘worst case’ scenarios.

⇒ Be sure about market need for cybersecurity products and that products are appropriate to meet that need (and combat new cyber-threats).

⇒ Reach out to and use feedback from stakeholders to inform research (customer events can help with this).

⇒ Be very aware of emerging standards and be ready to conform to requirements that may relate to these.

⇒ Be engaged in research and relevant consultations with government bodies significant in the development of new laws and regulatory frameworks.

External Engagement
ensuring regular feed-back from clients impacting on design and production.

Internal Feedback
Regular feedback within the organisation

DEVELOPMENT & TESTING

⇒ Ensure ‘secure by design’ approach embedded in all stages.

⇒ Ensure regular feedback and discussion with designers and researchers regarding matters arising during the design and development process (or preparation for the same).

⇒ Recognise the need for product ‘fit’ in relation to legal requirements and specific standards. Obtain certification, where appropriate for compliance (e.g. with ISO27001 and GDPR).

⇒ Use robust testing techniques commensurate with the risks concerned.

MARKET & IMPACT

⇒ Provide clear and comprehensive information in all marketing and sales materials and activities.

⇒ Ensure that the information addresses the importance of cybersecurity but that this is neither over- nor understated.

⇒ Be clear about the merits (or disadvantages) of operating in countries that may have questionable approaches to individual freedoms relating to ICT usage (and for which providing necessary safeguards on privacy would be unlikely to be possible).

⇒ Recognise and have tools in place to ensure high level of staff cultural awareness when working in different countries.

⇒ Ensure that contract documents include clear information around privacy and the circumstances in which protection of that privacy could be overridden.

⇒ Maintain contact with clients over a sustained period in order to provide reminders about the importance of following robust cybersecurity practices and gather relevant feedback.

⇒ Take firm action when product or service is misused.

⇒ Respond with immediacy in relation to cyber-breaches and report the same in accordance with GDPR requirements. Be open with clients regarding the same.

How to read this roadmap:

❑ Solid lines represent transitions between stages.

❑ Dotted lines represent feedback.

By Malcolm Fisk & Catherine Flick, De Montfort University

https://www.innovation-compass.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 710543