

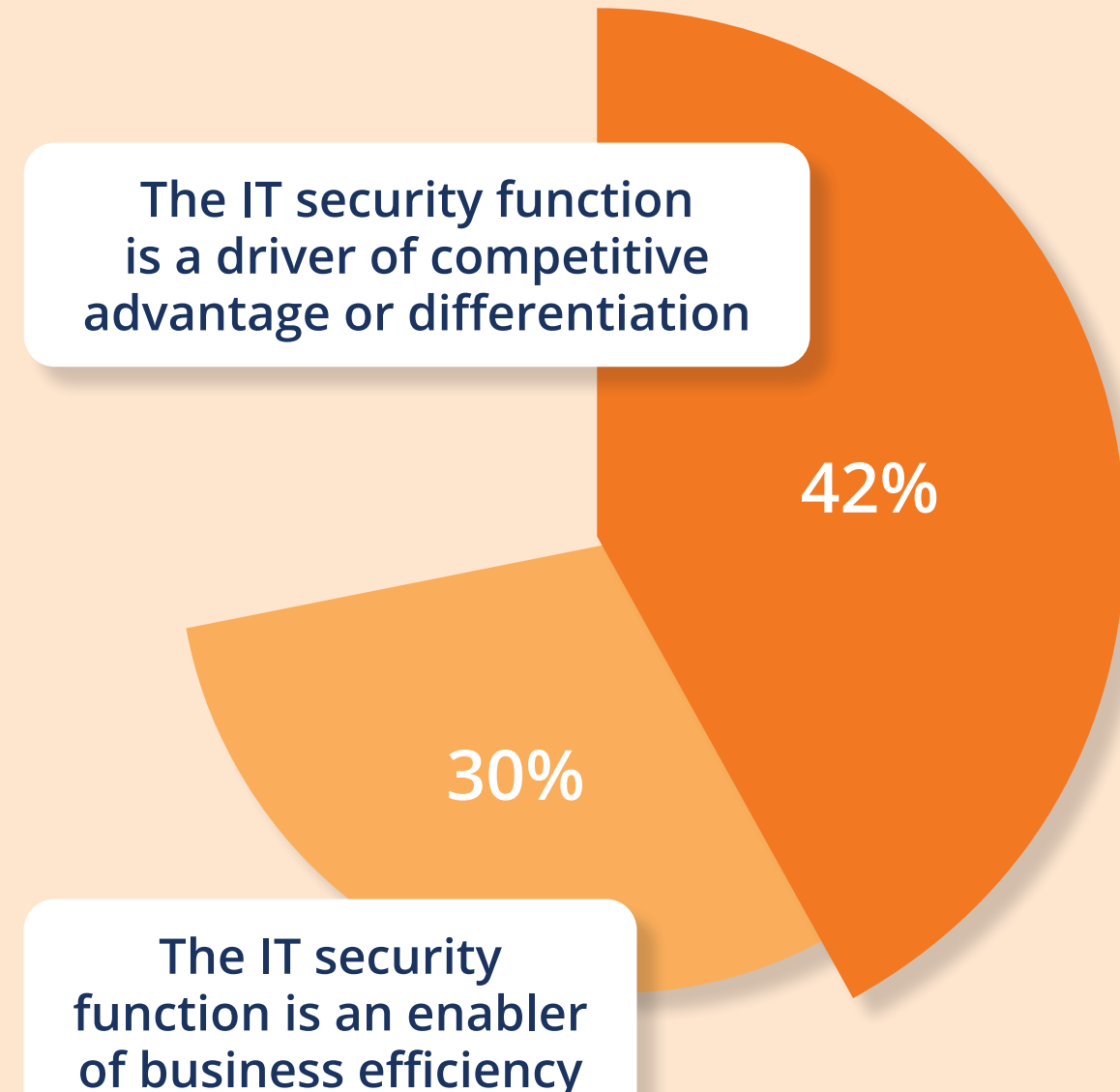
LEVERAGE NEW TECHNOLOGIES TO BUILD DIGITAL TRUST

Digital trust is built on an IT security paradigm incomparable with a traditional “moat and castle” perimeter protection. New approaches and new technologies must be embraced to safeguard the digital business of tomorrow.

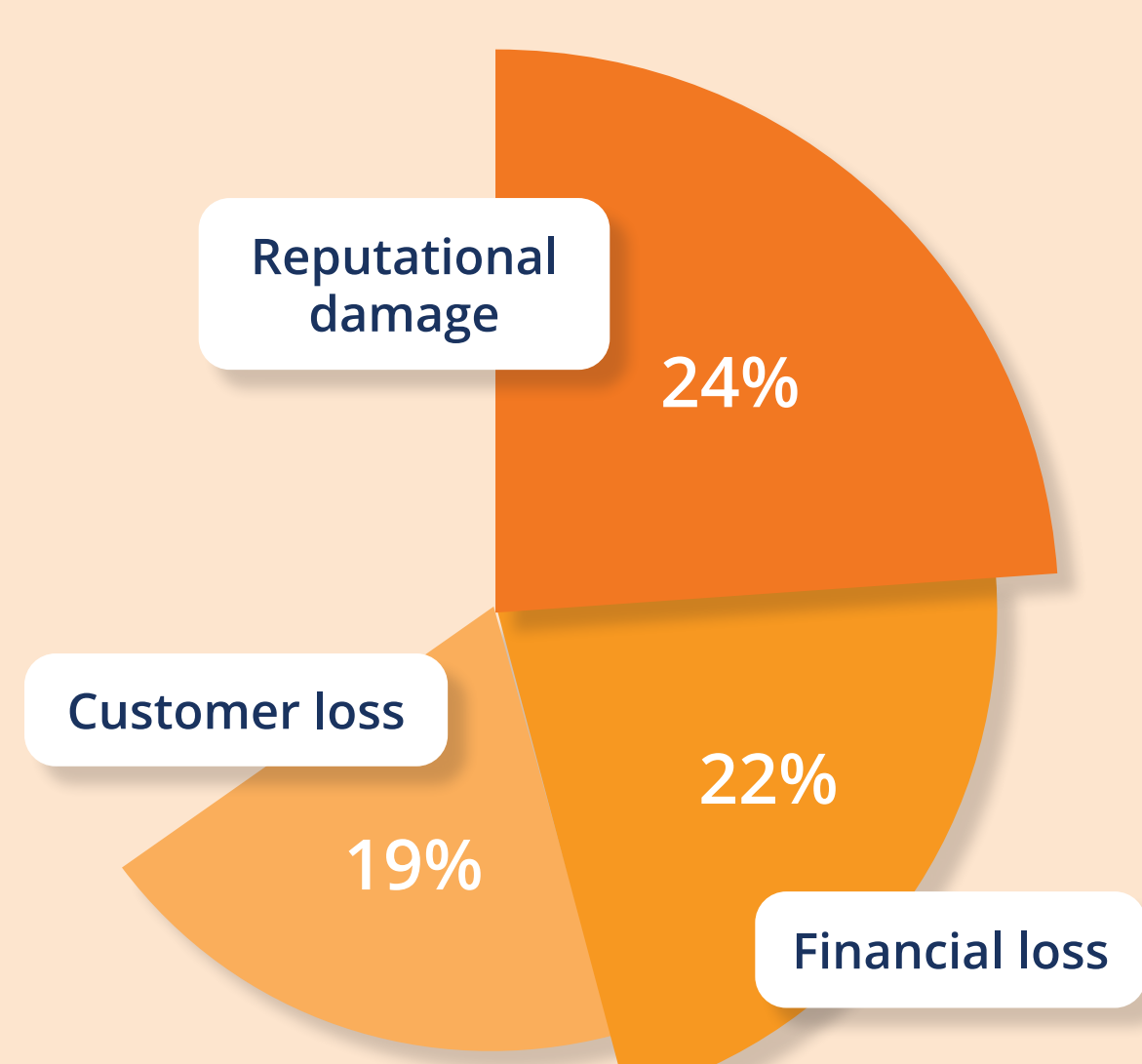


IT SECURITY IS ALL ABOUT BUSINESS

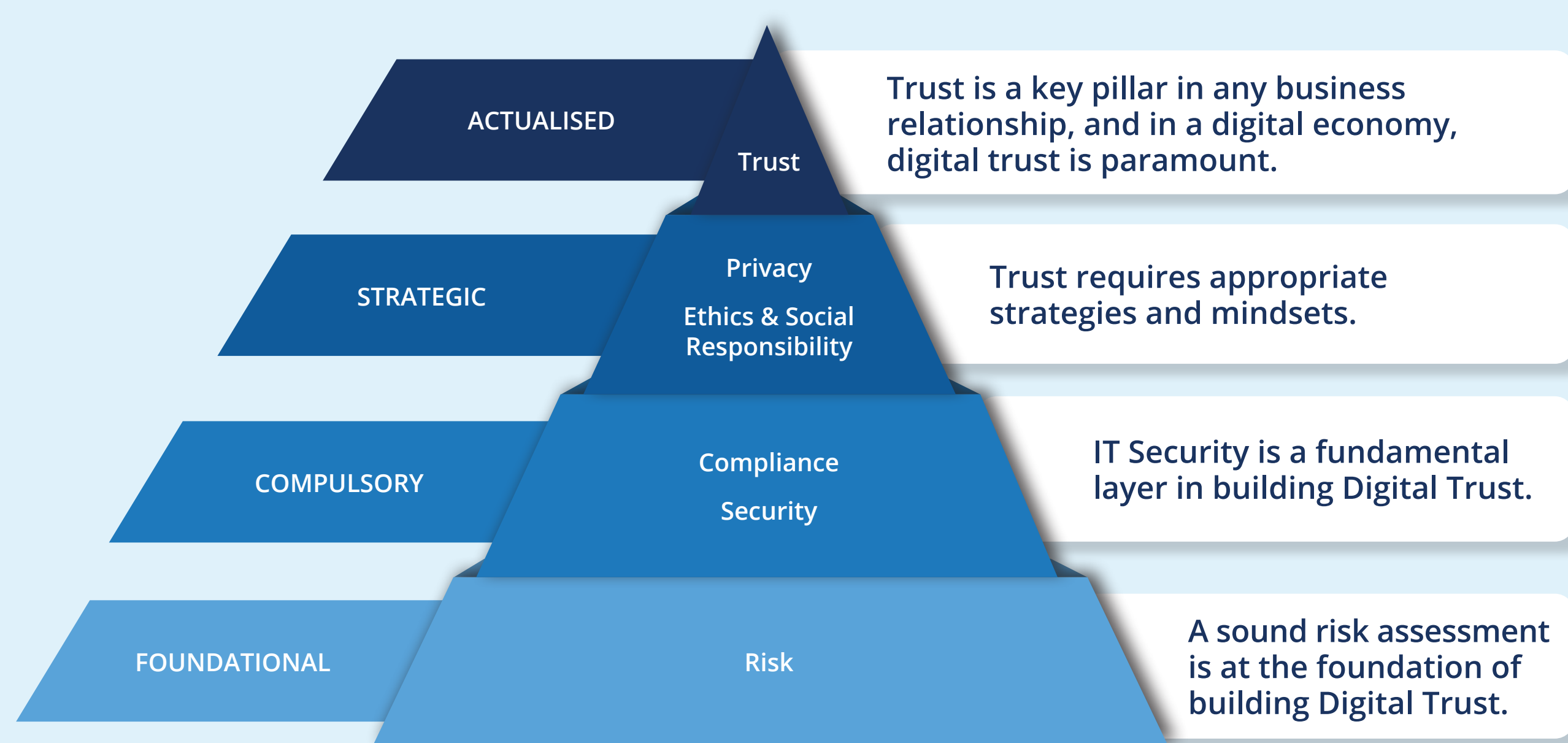
Business managers in the Nordic and Benelux countries see IT security as **more than a necessary cost**:



IT security executives in the Nordic and Benelux countries are mostly concerned about the **external impact of security incidents**:



DIGITAL TRUST IS NEEDED IN A DIGITISED ECONOMY



A NEW APPROACH TO SECURITY IS NEEDED

Security executives struggle to improve IT security capabilities due to:



The amount of time it takes to maintain and manage security tools



Users adopting cloud resources and “shadow IT”



The difficulties in balancing security with business/productivity priorities



There being too many legacy systems



A lack of understanding by management of IT security



A MODERN IT SECURITY ENVIRONMENT NEEDS TO SUPPORT THE REQUIREMENTS SET BY THE BUSINESS

According to Nordic and Benelux IT security executives the top 3 requirements are:



44%
Flexibility

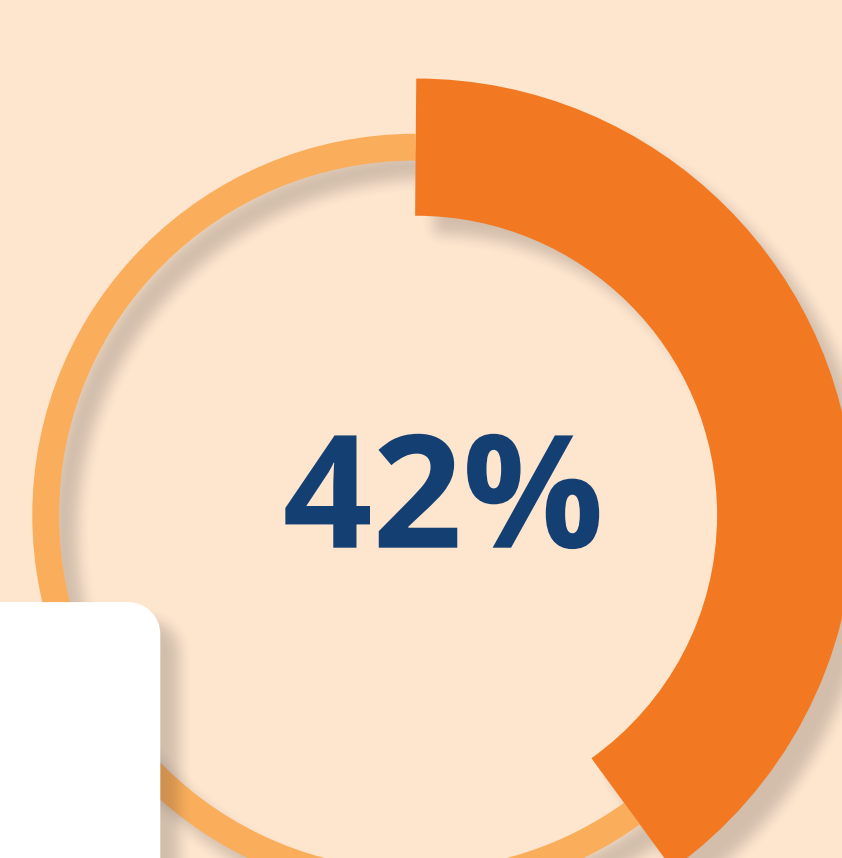


30%
Rapid development of new features



22%
Full integration with other technologies

ZERO TRUST MUST REPLACE “MOAT AND CASTLE” TO DEAL WITH INTERNAL THREATS



Managing internal security risk is the most widespread security operations priority in organisations in the Nordics and Benelux regions



MANAGING PRIVILEGES IS ESSENTIAL FOR ZERO TRUST

1.

Establishing zero trust requires new technologies.

2.

New technologies must manage – not only user and device access – but users’ privileges.

3.

The hybrid environment requires organisations to securely leverage public cloud, on-premise resource and edge components.

4.

User privileges must be dynamically managed to build digital trust.