Law Lab: From crisis to consequences. The legal lessons you'll want to know for when that unthinkable cyberattack happens

WHAT IS A CYBERSECURITY PLAN?

Joaquín Muñoz – Partner Bird&Bird

What are we talking about?

WHAT IS A CYBERSECURITY PLAN?

What are the links between all this?

CYBERSECURITY PLAN

GDPR

ISO 27001

IT SECURITY

What is a Cybersecurity Plan?

1. It consists of organising **cyber-security work**
2. In an **orderly and prioritised** manner
3. As an **iterative and incremental process**
4. To be able to **focus where it hurts.**

What is a Cybersecurity Plan?

1. Strategy
2. Policy
3. Procedures
4. Technologies

What can we use as a reference?

- NIST Cybersecurity Framework
- ISO27001
- GDPR - LOPDGDD
- Private Schemes and Frameworks
- Sector Focus regulation
- Local Schemes and Frameworks
  - National Security Scheme (Spain)
  - Security Master Plan by INCIBE (Spain)

What do they have in common?

ALL FRAMEWORKS

- Inventory of assets
- Focus on risk analysis and risk management
- Knowledge of the context
- Alignment with the business
- Involve the whole organisation

ISO27001

- Define Management Systems
- They are compliance-oriented
- They are **certifiable** frameworks
- These are well-recognised standards

Then...

ISO27001 leads to a Cybersecurity Plan,

but ...

We can also have a Cybersecurity Plan without following such a rigid framework, so that it better suits our needs.

What about GDPR?

HOW TO INTEGRATE PRIVACY
AND INFORMATION SECURITY

Comparison ISO27001/ENS vs GDPR

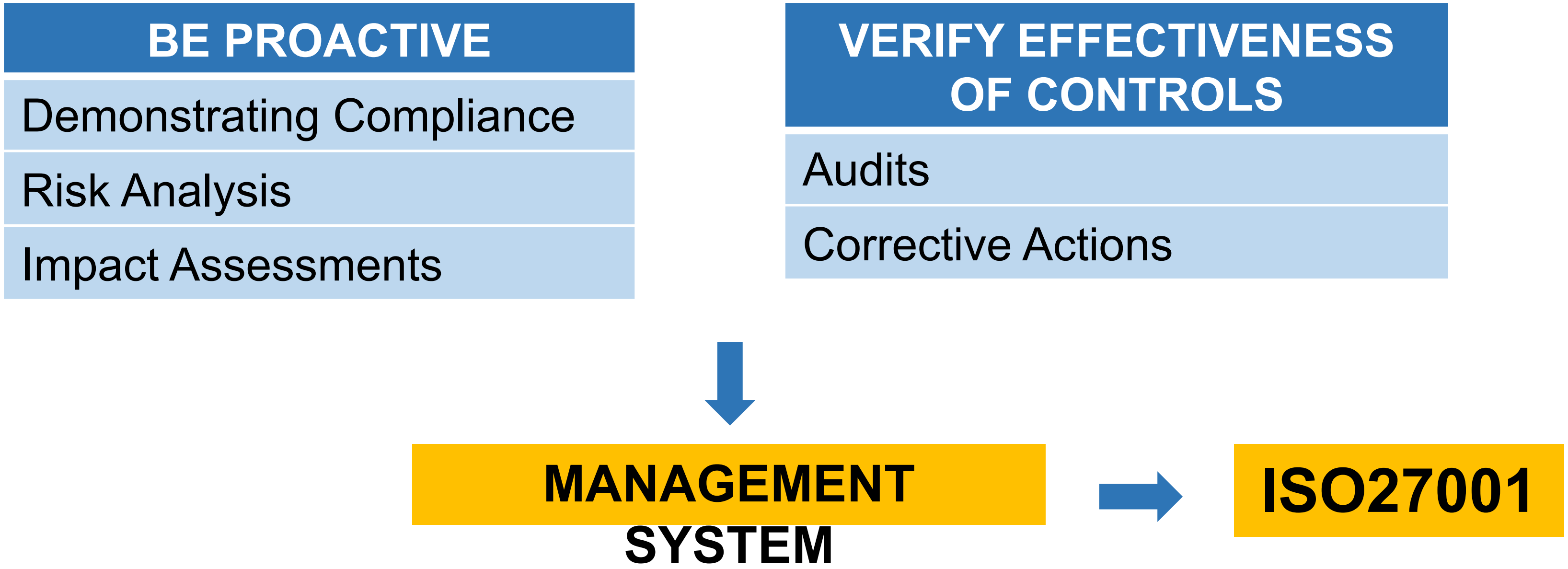
	ISO27001 / ENS / ...	GDPR
What does it protect?	Information and systems security	Human rights and freedoms
How does it protect?	Elements of legal (ENS) and organisational compliance	Elements of legal and organisational compliance
	Security measures	Security measures
	RISK ANALYSIS	**RISK ANALYSIS**

Comparison ISO27001/ENS vs GDPR

	ISO27001 / ENS / ...	GDPR	
What does it protect?	Information and systems security	Human rights and freedoms	
How does it protect?	Legal (ENS) and Organisational Compliance	Legal and organisational compliance	
	Security measures		Common elements
	RISK ANALYSIS		

More synergies …

- GDPR requires:



BE PROACTIVE

Demonstrating Compliance

Risk Analysis

Impact Assessments

VERIFY EFFECTIVENESS OF CONTROLS

Audits

Corrective Actions

MANAGEMENT SYSTEM

ISO27001

Integration of risk analysis

- **Personal data** are part of the information assets.
- Risk analysis on the **processing activities.**
- The new special categories of data implies **new risks** to add to the analysis and new controls.

How is it done?

STEPS TO A CYBERSECURITY PLAN

Key steps

1. Asset (not only data) identification and valuation;
2. Risk análisis;
3. Identification and evaluation of controls in place;
4. Selection of new controls to reduce risk;
5. Establish a prioritised list of controls to be implemented;
6. Implementation in as smooth a procedure as possible.

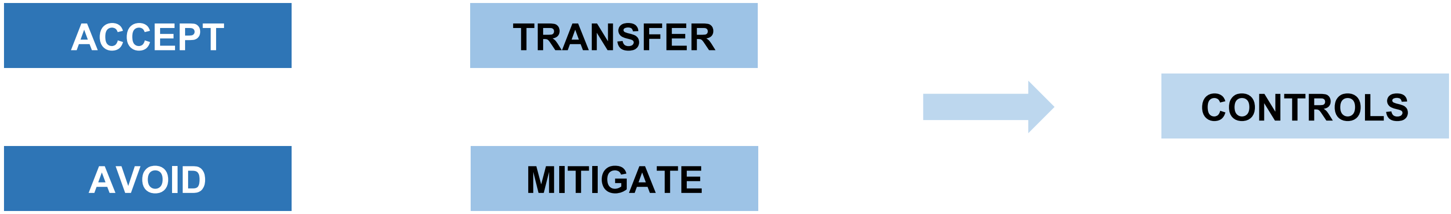
Asset mapping and valuation

- Identification of assets, mainly at 3 levels

ASSET CLASSES	ASSETS	EXAMPLES
Information assets	Information, data	Project information, Customer information, ...
Information systems	Applications	CRM, Project Management Software, ...
Assets of the organisation	Systems	Virtualised server, CRM service in the cloud, Database server,...

Risk analysis and management

1. Identification of threats and risks
2. Risk assessment
3. Risk appetite
4. Risk management


ACCEPT

TRANSFER

AVOID

MITIGATE

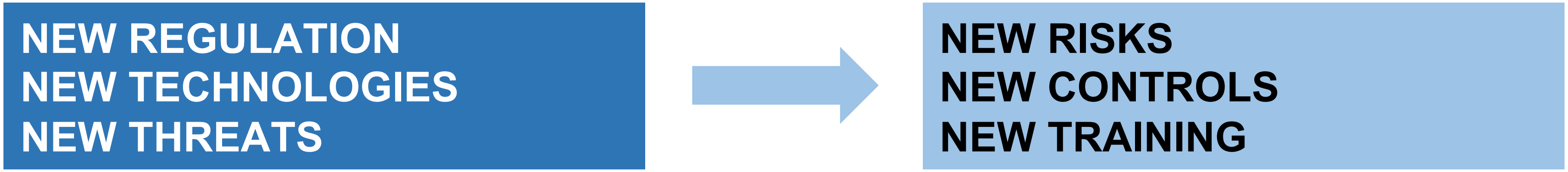
CONTROLS

Smooth management of implementation plans

- Initial list prioritised according to criticality
- Time-slots
- Re-prioritisation and re-definition
- Iterative and incremental process
  - Increasing the type of risks dealt with => doing new things
  - Improve maturity of controls => improve existing ones

A Cybersecurity Plan is a living thing

- It is a process, not a Project
- The risks are constantly evolving (and evolving faster and faster).
- Employee's training is key (culture)



NEW REGULATION
NEW TECHNOLOGIES
NEW THREATS

NEW RISKS
NEW CONTROLS
NEW TRAINING

Back to the beginning

RELATIONS BETWEEN THE
DIFFERENT FIELDS

Conclusion …

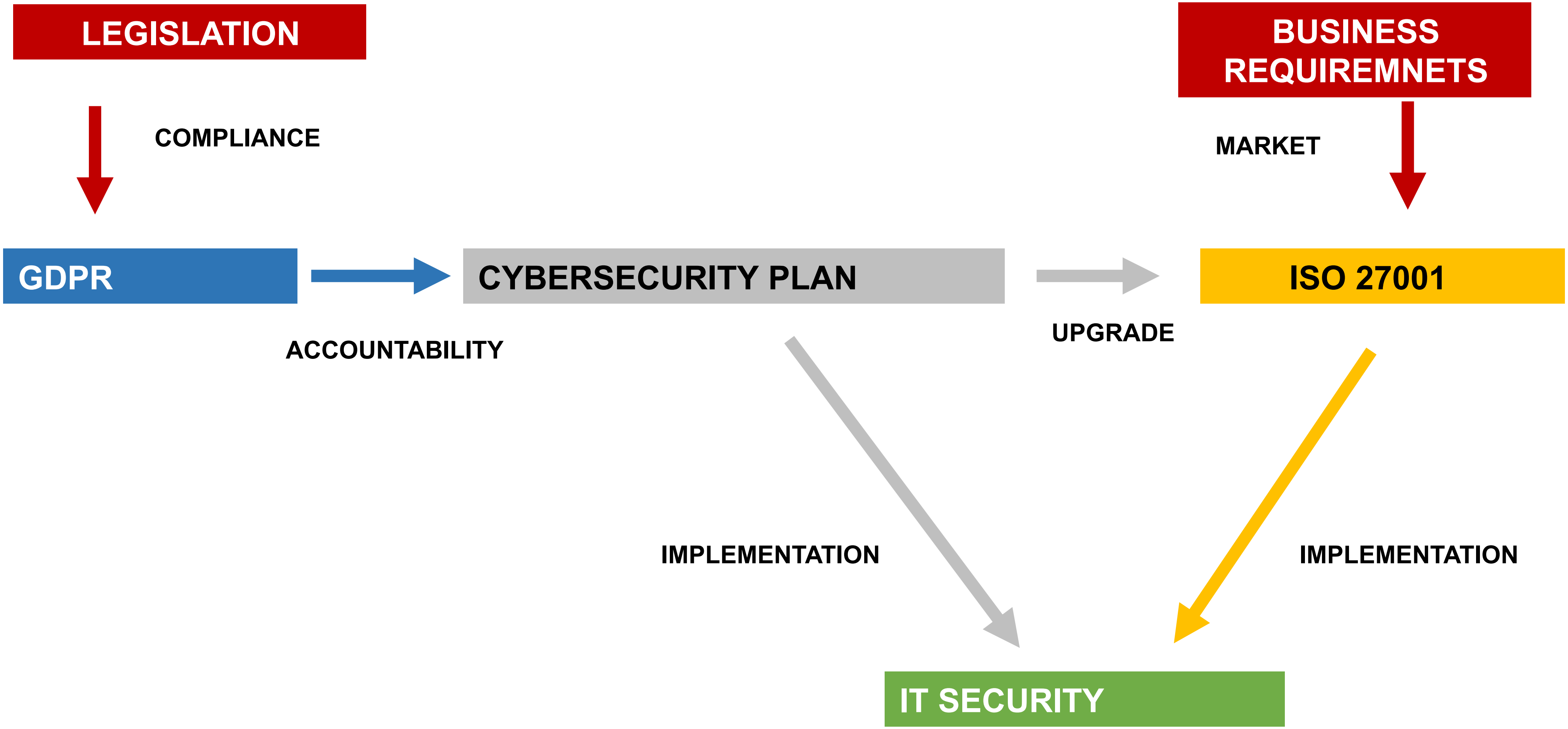
FURTHER INTEGRATION

GREATER EFFECTIVENESS

COMPLIANCE
SECURITY GOVERNANCE
SECURITY OPERATIONS

→

LEGAL COMPLIANCE
MARKET ADAPTATION



LEGISLATION

COMPLIANCE

BUSINESS REQUIREMNETS

MARKET

GDPR

CYBERSECURITY PLAN

ISO 27001

ACCOUNTABILITY

UPGRADE

IMPLEMENTATION

IMPLEMENTATION

IT SECURITY

Data Breach Management

I. Phases

1. Identification/Detection
2. Evaluation
3. Containment
4. Investigation
5. Execution and communication
6. Recovery
7. Follow up

II. Risk classification

III. Communications/Notices

1. GDPR
2. Law enforcement and Courts
3. Notification
   - Clients
   - Employees
   - Third parties
4. Other type of notifications

Final remarks

1. Cooperation with the relevant authorities and regulators
2. Fast decision-making
3. Responsibility / Competence
4. Traceability of decisions
5. Collection of relevant information
6. Compliance with local regulations
7. Coordination approach
8. Justification and motivation
9. Confidentiality

THANK YOU!

Joaquín Muñoz
joaquin.munoz@twobirds.com
https://www.linkedin.com/in/joaquinmunoz/