



## OUTLINE OF MAJOR COMPONENTS OF ANNUAL PLAN

**CYBER-THREAT IS  
MAINLY A  
REFLECTION OF  
OUR WEAKNESSES.**  
- Stephane Nappo

The most important aspect of the plan is to deliver the promised benefits to key business stakeholders, executives and decision makers and protect the organization.

### **Benefits and Milestones – Timeline (Metrics and KPIs)**

- ❖ Regular engagement with key stakeholders – transparency and visibility.
- ❖ Business engagement framework / model.
- ❖ Regular (monthly?) Cyber Security Forums.

### **Optimum Efficiency Security Operating Centre**

- ❖ This is the basic foundation of a cybersecurity function. Adopt a model. Refine. Finetune.

### **Incident Response Management**

- ❖ Practice as you would a fire drill. Simulations. Test. Learn. Improve.

### **Projects Portfolio**

- ❖ Collaboration with IT. Standards and tools. Cloud. Identity and Access Management. Apps. Mobility.
- ❖ Safety a critical aspect of Digital and Customer Experience (CX).

### **Culture and Change**

- ❖ This is what the business sees. It is a mistake to ignore this part. Cyber Awareness training is essential. ISMS<sup>(1)</sup> too.
- ❖ Innovate. Use gamification. Who wouldn't want to play a video game and become cyber certified.

### **Audit and Risk**

- ❖ Risk management. Reporting. This is how it can be proven that progress has been made. Compare the risk profile of cyber security in the beginning and at the end of the year.

### **Legal and Commercial - Procurement**

- ❖ It is amazing how often cybersecurity is forgotten in procurement. Big mistake.

### **Regulatory Compliance**

- ❖ Define in advance. Monitor legislative developments. Legal is a great help here if they are your friends.

### **Critical Systems and Data**

- ❖ Controls. Registers. Governance. Policies and procedures.

Please contact us for more information.