GapSolutions

Project Model Information Security

Project Model

1

What is the GapSolutions Project Model?

The Project Model is a format used by the GapSolutions Information Security department, providing a clear set of targets for each project stage, to ensure a smooth process throughout. The project model comprises 3 stages:

1. Mapping
2. Risk Management
3. Audit

Mapping

2

Mapping

Phase 1 – Mapping: Understanding and Documenting Your Organization

The first phase of our process is all about gaining a deep understanding of your organization. Through interviews, inspections, and the materials you provide, we create a holistic picture of your company's structure and operations. This ensures everything is fully documented and accessible via our secure portal, keeping the entire project transparent and traceable.

Key Activities in Phase 1:

1) Threat Profiling: We work closely with you to create a customized threat profile, considering factors like:

- **Public Exposure:** Are you a high-profile organization that might attract diverse cyber threats?
- **Financial Standing:** Organizations with strong financial backing may be more attractive to criminal characters.
- **Activism Risk:** Does your organization deal with sensitive issues like human rights or environmental concerns?
- **Political Exposure:** If you're involved in political matters, you could face more advanced threats.
- **Infrastructure Impact:** Does your organization play a vital role in local, regional, or national infrastructure?
- **Attack Surface:** We'll evaluate your potential vulnerabilities, including networks, devices, servers, and more.

2) Mapping Key Areas: We collect vital information from interviews and materials to understand your:

- **Processes:** Documenting your core business operations and supporting processes.
- **Assets:** Identifying valuable assets like hardware, software, intellectual property, and reputation.
- **Suppliers:** Understanding your critical third-party relationships and how they tie into your business.
- **Security Measures:** Reviewing your current security policies, procedures, and technologies.

3) **Portal Documentation:** All collected data is entered into our secure portal, ensuring all relevant information is available for future steps and detailed documentation.

Risk Management 3

Risk Management

Phase 2 - Risk Management: Safeguarding Your Organization

Our Risk Management Model follows best practices from ISO 27005:2022 and the NIST RMF (800-30 series). The process is divided into key stages to ensure a thorough and effective evaluation of your organization's risks, helping you prioritize what matters most.

Key Activities in the Risk Management Phase:

1) Establishment of a Risk Model: We begin with a collaborative workshop to align our approach with your specific risk management preferences. During this session we define:

- **Risk Assessment Methodology:** Whether you prefer a qualitative, quantitative, or hybrid approach.
- **Risk Scale:** Deciding how risks will be rated, either using a 1-5 scale (from low to high), financial metrics, or another system.
- **Risk Appetite:** We'll discuss which extent of risk your leadership finds acceptable.
- **Risk/Threat Catalog:** We'll define a list of main threats to your business.

All of this will be consolidated into a comprehensive Risk Management Policy, tailored to your needs.

2) Risk Evaluation: Once the Risk Model has been established, we assess your IT assets and systems—starting with the critical ones identified during Phase 1 (Mapping). We evaluate each asset based on:

- **Likelihood and Impact:** For every identified threat, we measure how likely it is to occur and what the potential damage could be.
- **Asset Categorization:** We classify your assets, with a system to identify critical systems and the least important in terms of maintaining business operations.

We then examine the identified assets, mapping out existing threats and compiling detailed risk assessments in the GapPortal. Once all assets are evaluated, we build a complete, holistic risk based mapping of your organization.

Risk Management 4

3) Risk Mitigation & Handover: After evaluating risks, we identify mitigation strategies to reduce them. Each mitigation is linked to a **Residual Risk Level**, reflecting the risk that remains after these measures are applied.

We'll review this with you in a final workshop, where we:

- Discuss the findings, particularly any **High-Criticality** risks.
- Ensure your leadership is ready to take on responsibility of managing these risks.
- Plan any additional actions before moving to the next phase of the project.

This phase ensures that all risks are thoroughly assessed, and effective mitigations are put in place, providing your leadership with the insight needed to safeguard the organization.

Audit

5

Audit

Phase 3 - Audit: Ensuring Compliance and Strengthening Security

The Audit stage of the Project Model is the third phase of our Information Security Project Plan, following the completion of the Risk Management phase. This stage focuses on internally auditing your organization's compliance with key legislation, standards, and existing policies, ensuring that your security measures are effective and meet the necessary requirements.

Key Activities in the Audit Phase:

1) Audits in the GapPortal: Using our GapPortal, we compare the data collected during Phases 1 and 2 with key security requirements from frameworks and directives like:

- **ISO 27001**
- **NIS2 Directive**
- **CIS Critical Security Controls v8 (CIS18)**
- **CER**

Each audit links to specific documentation and evidence, such as:

- **Control series**
- **Files**
- **Risk assessments**
- **Information assets**
- **Audit goals**

This ensures full traceability and documentation to document compliance with each requirement.

Audit

2) Management Training: We provide management training, summarizing key security findings, risks, and information regarding incident handling, thus helping leadership make informed decisions. This includes:

- **Risk Analysis:** Highlighting threats and vulnerabilities through risk assessments.
- **Compliance Reporting:** Demonstrating adherence to regulatory requirements through specific audits.
- **Disaster Recovery and Incident Handling Guidance:** Providing training to the leadership on how to prepare effectively for a potential disaster recovery or emergency scenario in the organization.

This ensures transparency, accountability, and informed decision-making at all levels of the organization.

3) Policies and Procedures: During this phase we review and ensure your organization has the necessary policies and procedures in place to meet both legal and standards-based requirements. These policies form the foundation of your information security framework and include:

- **Information Security Policy**
- **Risk Management Policy**
- **Disaster Recovery and Incident Handling Policy**

These documents guide your organization’s approach to security and ensure compliance with applicable standards such as **ISO 27001** and **NIS2.**

We cooperate with your organization to ensure that the GapPortal is set up in a way that supports the existing security and compliance activities and helps streamline the reoccurring work using our annual wheel tool. This tool provides reporting, notification and documentation on what tasks to perform, helping your employees best stay on track with your governance and compliance activities.

Contact us to ensure your organization’s security is robust, compliant, and resilient. Our tailored risk management, audit, and incident handling solutions help you navigate complex security standards, minimize risks, and strengthen your overall security posture. Let our experts guide your organization to enhanced protection and compliance.

GapSolutions

Contact:

GapSolutions A/S
Uraniavej 6
8700 Horsens

Telefon: 8844 0808
Hjemmeside: www.gapsolutions.dk