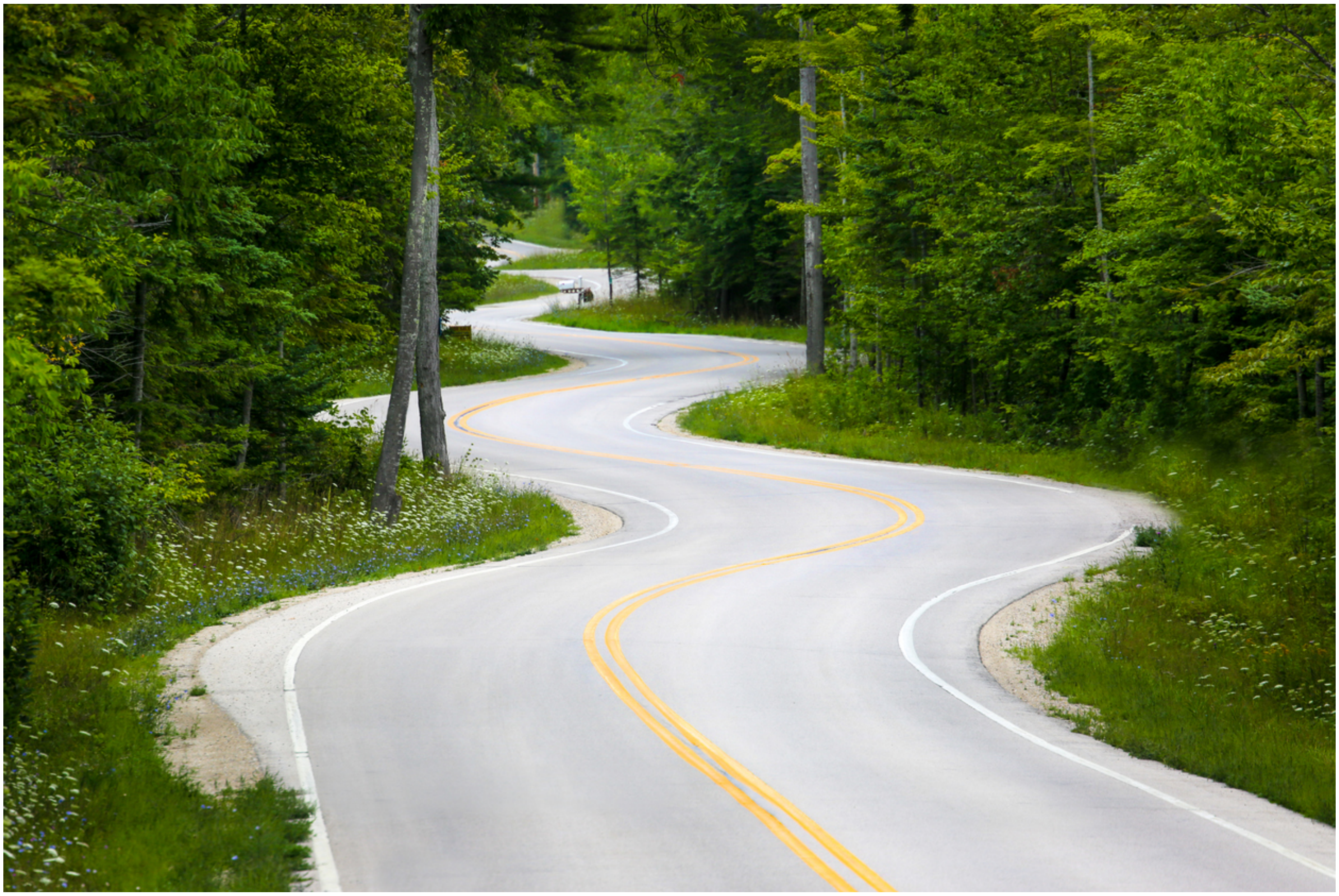


Maturity Assessment, Profile, and Plan

A MAPP to Clearer Information Security

by Christophe Veltsos, Ph.D.

While the information security industry has undergone convulsive change, it is coalescing around maturity-based management of key business processes. The MAPP approach provides practical implementation of the maturity model.

TrustMAPP®
Measure. Improve. Manage.

What You’ll Learn

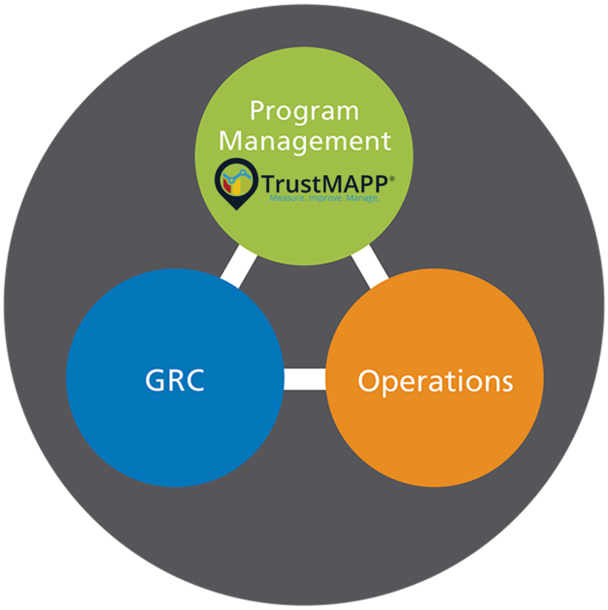
Four emerging and positive industry factors bode well for information security officers and corporate executives responsible for information security. These factors finally enable an information security roadmap that can unite organizations around a sound strategy.

Emerging Security Factors

1. Board directors and the C-suite are now engaged in security, but demand **metrics** and investments in **capacity-building** rather than fleeting point-in-time compliance.
2. The security industry is quickly coalescing around **maturity** as the standard by which security program capacity is measured and improved.
3. Maturity at the **business process level** (vs. audit compliance) is becoming the focus of the industry’s best practice maturity-based assessments.
4. Automation **platforms** have come a great distance to assist the CISO in evaluating, tracking, and reporting an organization's security maturity.

This paper describes a three-step maturity-centric approach—**M**aturity **A**ssessment, a **P**rofile, and a **P**lan (MAPP). An information security MAPP empowers the CISO to evaluate, track, report, and strategize the organization’s security priorities.

Information Security Program



Factor #1
Executives and Boards Are a Captive Audience Demanding Metrics

Board directors and the C-suite are now engaged in security, but demand metrics and investments in capacity-building rather than fleeting point-in-time compliance.

Chief Information Security Officers (CISOs) are under increasing pressure to effectively report on the organization's ability to secure its data. A 2015 survey by Deloitte reported that many CISOs share the following problems: limited resources, inadequate strategy, a lack of trust from executives, and ineffective communication about the organization's security. As boards and executives expand the frequency and depth of interactions regarding cyber security, CISOs must be able to translate the value and effectiveness of upwards of 100 controls to people with little or no information security expertise.

For many CISOs, answering even simple questions from management, such as "How capable are we?" and "How do we know if this is enough?" can be challenging and time-consuming. According to an article by the CEB, an executive advisory firm, CISOs can spend three to four weeks to prepare for their next presentation to executives and boards.

How can CISOs improve their ability to report to board directors and executive stakeholders in a meaningful and consistent manner, instead of getting lost in the proverbial weeds of security controls? How can CISOs elevate the discussion to communicate the organization's security posture clearly and accurately? How can CISOs engage with management on how to best prioritize security improvements to achieve appropriate risk levels?

According to a 2015 NYSE/Veracode report entitled Cybersecurity in the Boardroom, nearly two-thirds of board directors prefer to be presented cyber security information either via "high-level security strategy descriptions" or via risk metrics. By contrast, only 9% chose "audit and compliance status" as their preferred briefing method.

WANTED

A methodology to assess the maturity of security processes that is understandable, logical, repeatable, reliable, and robust.

Factor #2
The Emerging Industry Standard is Maturity

The security industry is quickly coalescing around maturity as defined by COBIT as the standard by which security program capacity is measured and improved.

One way to focus the discussion on security strategy is to look at the maturity of the organization's security activities. Unlike audits, which provide only a snapshot-in-time of the effectiveness of controls, a maturity assessment helps determine an organization's ability to cope with constantly evolving risks. A maturity assessment determines the extent to which the security activities are effective and responsive.

In 2011, ISACA introduced a maturity assessment-based approach called the Process Assessment Model (PAM), based on COBIT 4.1. According to COBIT's FAQ, PAM provides management with "a robust, reliable, repeatable approach and supporting tools to better understand the current capability of their governance and management processes, and to help management do benchmarking, gap analysis, and process improvement planning." The value of the PAM approach is to "understand the level of capability that is present, and the level that is appropriate for a given process, based on business requirements, and to understand the nature of any gaps so that any significant weaknesses in the process can be identified and improved."

In other words, PAM was conceived as a methodology to better communicate an organization's security posture — "How are we doing?" — and explain to management how the various projects undertaken are part of a larger information security program — "Why are we doing this?"

The value of a maturity-based assessment approach is also shared by other key auditing and advisory entities:

- The Institute of Internal Auditors recommends using an approach such as the Process Assessment Model "to communicate to the board and senior management the current status of the IT governance environment" in its Auditing IT Governance guide.
- Deloitte writes that a maturity assessment can help an organization "understand its capabilities for managing and mitigating the ever-present risk posed by cyber threats."
- KPMG advocates reporting on the maturity of control structures when communicating with the board.
- In July 2015, The Conference Board, an organization providing leadership advice, issued A Cyber Security Guide for Directors in which it advocates the use of a maturity dashboard to represent and communicate the maturity of the components (i.e. processes) of its cyber security program.

In June 2015, the Federal Financial Institutions Examination Council (FFIEC) released its Cybersecurity Assessment Tool (CAT), as well as a five-page summary for board directors. The CAT "provides a repeatable and measurable process for institutions to measure their cybersecurity preparedness over time.“ Figure 1 shows the five activities described by the CAT, starting with a maturity assessment.

The FFIEC identified the following benefits from using CAT:

- Identifying factors contributing to and determining the institution's overall cyber risk.
- Assessing the institution's cyber security preparedness.
- Evaluating whether the institution's cyber security preparedness is aligned with its risks.
- Determining risk management practices and controls that are needed or need enhancement and actions to be taken to achieve the desired state.
- Informing risk management strategies.

Maturity assessments are a proven way to assess, communicate, and even manage information security programs. In short, such an approach can lead to more effective IT governance.

Factor #3
Assessments Are Focused on Actionable Processes

Maturity at the business process level (vs. audit compliance) is becoming the focus of the industry's best practice maturity-based assessments.

While it might be tempting to try to assess the maturity of all of the security controls in the organization, a better approach is to first group controls into business-focused security processes. The exact groupings might depend on a particular security framework (e.g. NIST 800-53 or NIST CSF) or regulation (e.g. HIPAA or FFIEC).

Instead of tracking and measuring each control individually, a process- centric approach to performing maturity assessments, such as COBIT PAM, first combines controls into (business) processes, according to business needs/industry/regulation.

Assessing Maturity of the “Access Control” Process

To illustrate how maturity assessments work, consider the business process of Access Control, which is found in every security/regulatory framework. Instead of tracking each control separately, we can focus on the maturity of the organization’s security practices across its environment using the 1-5 maturity scale:
Six COBIT dimensions are analyzed and scored using CMMI maturity levels:

1. What is our level of maturity of Awareness for Access Control Management?
2. What is our level of maturity for Policy & Procedures for Access Control Management?
3. What is our level of maturity of Automation for Access Control Management?
4. What is our level of maturity of Expertise for Access Control Management?
5. What is our level of maturity of Accountability for Access Control Management?
6. What is our level of maturity of Measurability for Access Control Management?

The maturity assessment approach provides a holistic method to understand dimensions of a control process. It applies to internal policies and external regulations, focuses on areas of greatest impact, and aligns with business goals. For example, if the business process is performing well in the Awareness domain, Policy and Procedure domain, and Accountability domain (relative to our process in question), then improving the Automation (tools) domain and the Measurability domain can be the organization’s focus.

The organization can then evaluate the maturity of each process across each of the six dimensions defined in COBIT 4.1.

- Awareness and communication
- Policies, processes and procedures
- Tools and automation
- Skills and expertise
- Responsibility and accountability
- Goals and metrics

The measurement of maturity for each process-dimension pair is taken using a predefined maturity scale, such as the CMMI, which ranges from a maturity level of one to five. The CMMI maturity levels are:

1. Initial (also sometimes termed ad-hoc)
2. Repeatable
3. Defined
4. Managed
5. Optimizing

The maturity scale is uniformly applied to all of the measurements: for each process, for each dimension, determine a maturity level using the maturity scale. This approach is logical, repeatable, and reliable.

Factor #4
Automation Is Making Maturity Management Feasible

Automation platforms have come a great distance to assist the CISO in evaluating, tracking, and reporting an organization's security maturity.

One way to focus the discussion on security strategy is to look at the maturity of the organization's security activities. Unlike audits, which provide only a snapshot-in-time of the effectiveness of controls, a maturity assessment helps determine an organization's ability to cope with constantly evolving risks. A maturity assessment determines the extent to which the security activities are effective and responsive.

Maturity assessments form the basis by which the CISO can measure the effectiveness of the organization's cyber security capability. When aggregated across all of the organization's security processes, the maturity measures provide a unique security profile of the organization.

Presented with clear information about the maturity of the various security processes, the CISO and management can now perform a gap-analysis between the current maturity level and the desired maturity level and determine if the organization is performing at the level that it should be. When that is not the case, appropriate remediation efforts can be **planned**, and appropriately funded now that management better understands the maturity gap as well as where and why those resources will be spent.

The methodology described can be summarized via the **MAPP** acronym, a **M**aturity **A**ssessment, **P**rofile, and **P**lan. With this methodology, a CISO measures the maturity of key business processes in a robust, reliable, repeatable approach to communicate the organization's security posture, and to engage with management in benchmarking, gap analysis and process improvement planning. MAPP isn't about conducting an audit but about measuring performance of required security processes based upon the business needs / industry / regulation.

TrustMAPP – Getting Maximum Value From Maturity Assessments

How can CISOs get maximum benefit out of the MAPP approach just described? Is there a tool that can track these maturity measurements for each process-dimension pair along with desired maturity goals, generate various profile views, and provide cost estimates for closing the maturity gaps? Can such a tool provide a configurable dashboard, enabling CISOs to generate reports for various audiences including boards, management, peers, or internal audit?

TrustMAPP is an automated platform that allows taking stock of security gaps and translating findings (maturity profiles) into communication with boards, and action plans with budgets.

Assessments with TrustMAPP are rapid and repeatable using survey templates configured to the NIST Cyber Security Framework as well as industry-specific regulations, such as GLBA, HIPAA, PCI DSS, GLBA, FFIEC, FISMA, and SOX.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

GDPR

HIPAA
Health Insurance Portability and Accountability Act

PCi

ISO
International Organization for Standardization

TrustMAPP®
Measure. Improve. Manage.

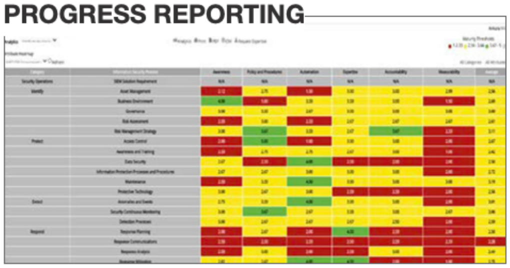
TrustMAPP enables meaningful business discussions about resource allocation and CapEX requirements for security improvements. Calculators in TrustMAPP support estimation and planning, with built-in financial planning intelligence, which covers:

- One-Time Capital Cost (if applicable)
- One-Time Labor (effort in hours)
- Ongoing Labor (hours/month)

TrustMAPP also provides multiple security dashboards, including trending diagrams, historical reports, and what-if analyses. TrustMAPP's reports can be exported as data tables or can be visualized with its built-in analytics engine.

With TrustMAPP, CISOs can conduct continuous risk management, unite stakeholders around a clear Maturity Assessment, Profile and Plan (MAPP), and align information security with corporate business objectives. From a governance perspective, TrustMAPP enables the CISO to have effective presentations and interactions with boards.

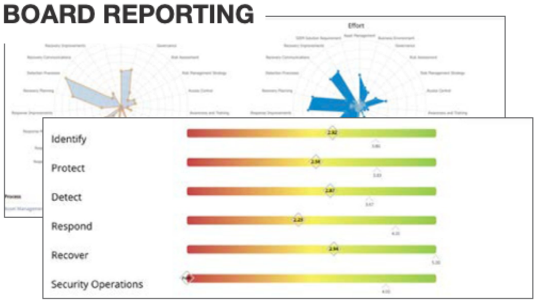
PROGRESS REPORTING



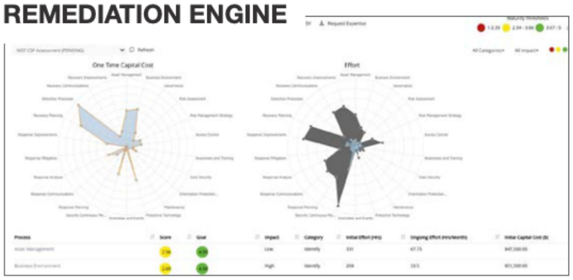
WORKFLOW MANAGEMENT

TRACKING COMPLIANCE & POSTURE IMPROVEMENT

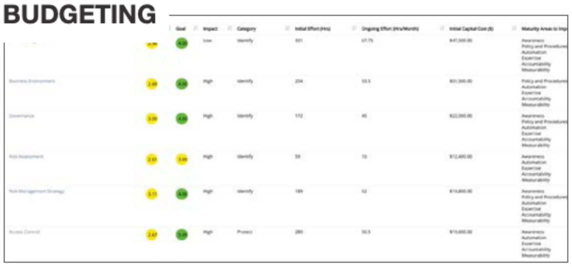
BOARD REPORTING



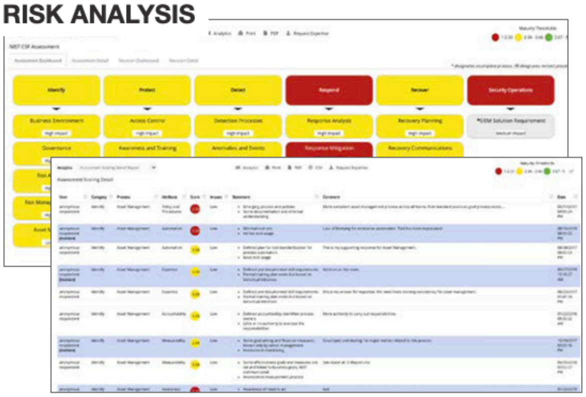
REMEDIATION ENGINE



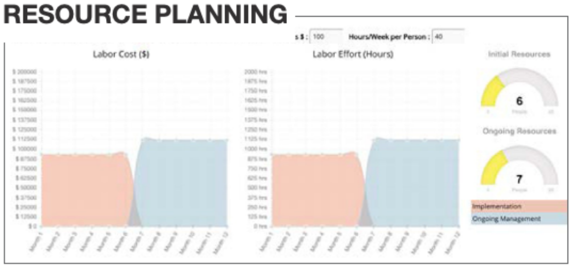
BUDGETING



RISK ANALYSIS



RESOURCE PLANNING



TrustMAPP®
Measure. Improve. Manage.

Conclusion: Clarity and Speed Are Welcome New Advantages in Security Management

With TrustMAPP, you can

- Determine the strength of your security processes
- Track maturity trends across processes and time
- Estimate cost and effort levels to achieve desired maturity levels,
- Plan and implement remediation
- Update senior executives on progress

In its 2013 Information Security Maturity Assessment Study, the information security consulting firm Secure Digital Solutions (SDS) reported that regardless of size, “the maturity of the information security program tends to be a challenge for both large and small firms.“ SDS set about developing TrustMAPP to help answer this industry need.

TrustMAPP empowers the CISO with a clear picture of the organization’s security posture, including trending analysis, planning and budgeting, and built-in support for multiple frameworks. With the cloud-based platform, the scoring, tracking, and reporting of the maturity of security processes can happen in weeks, instead of months, using the tool’s built- in dashboards. TrustMAPP helps CISOs create and communicate an information security roadmap to guide the organization’s security activities.

Despite the outward appearance of chaos and convulsive change in the information security industry, behind the scenes quiet progress has been occurring over the last several years. Taken together, these factors are positive. They’re uniting boards and CISOs (many new to their posts) around common business values, making measurement more standard worldwide, and equipping security leaders with superior platforms that maximize their time and resources.

By leveraging the best-practice **MAPP** model of Maturity Assessment, Profile, and Plan, using an automated tool like TrustMAPP, CISOs can focus more of their time and interactions towards security strategy.

About The Author

Christophe Veltsos, Ph.D. is an associate professor in the Department of Computer Information Science at Minnesota State University, Mankato where he regularly teaches Information Security and Information Warfare classes. Beyond the classroom, Chris is also very active in the security community, engaging with community groups and advising business leaders on how to best manage information security risks. Follow Dr. Veltsos on Twitter at @DrInfoSec.