

An ILLUMANT White Paper



A Standards-based Maturity Model for Unit-by-Unit Risk Assessment

WRITTEN BY

MATIJA SILJAK

DATE

OCTOBER 2008

A Standards-based Maturity Model for Unit-by-Unit Risk Assessment

One of the challenges resulting from the openness of the university environment is deciding how to secure sensitive electronic information flowing through decentralized and distributed business processes.

To overcome this challenge, universities need a mechanism for comparing and contrasting the degree of exposure and risk posed by each individual academic and administrative unit. This requires answering the following questions university wide, as well as on a unit-by-unit level:

- What constitutes sensitive information?
- Where is it?
- How much of it exists?
- How effectively is it protected?
- What vulnerabilities could lead to compromise?
- What is the likelihood of compromise?
- What are the tangible and intangible costs of compromise?
- What is the best strategy for improvement from a cost-benefit perspective?

These questions are the foundation of a risk assessment. The answers to these questions are essential to establishing and maintaining a formidable and efficient security program, and the questions should be asked regularly.

Illumant has developed a standards-based approach tailored to university environments to address these questions in a cost-effective way. This process allows universities to make relevant unit-by-unit comparisons of risk and exposure and to help focus security efforts in areas where they are needed most.

Case study: Risk Assessment of an “Ivy Plus” University Client

Illumant was engaged to perform a unit-by-unit risk assessment to evaluate the effectiveness of security measures in mitigating risk exposure. Step one was to perform a preliminary analysis of the units to determine their criticality. Step two was to evaluate security controls using a standard risk maturity model. At the conclusion of the assessment, Illumant was able to identify areas where the security measures implemented were not appropriate based on the corresponding level of risk. Illumant made numerous recommendations to realign protection measures with exposure levels.

Components of Illumant’s Risk Assessment Program

Illumant’s risk assessment methodology is comprised of the following components:

- **Unit risk classification** to evaluate objective and subjective factors such as the size and complexity of the unit and the amount of sensitive data stored or handled by the unit, in order to “right-size” the overall assessment.
- **Assessment scoping** to identify targets of the examination, including critical business processes and locations, personnel, documentation, subcontractors, systems, applications, and data that should be considered when evaluating the effectiveness of a unit’s security measures.
- **Data collection** to gather the appropriate types and quantities of data necessary from key IT staff members, unit leaders, administrators and other relevant users (e.g., faculty, students, and administrative staff), to evaluate the effectiveness and maturity of security measures, primarily consisting of carefully designed questionnaires and document

request lists, but also including high level review of evidence to confirm the accuracy and completeness of responses.

- **Technical vulnerability assessment** to reviewing existing assessments to determine whether the department or unit is effectively mitigating the risks identified at a technical level. Upon request, Illumant can provide a complete vulnerability assessment of each unit although we may also rely on existing information if feasible.
- **Evaluation criteria** to provide a consistent, standards-based approach to measure the effectiveness and maturity of specific security policies, procedures, practices and controls in mitigating risk. In addition, the criteria are designed to establish the quantity and sensitivity of information at each site. This information is used to compare the levels of risk and exposure of sensitive data between departmental and administrative units as well as to identify systemic risks across all units.

Evaluation Criteria

Illumant utilizes a standards-based controls maturity model to rate the appropriateness and effectiveness of each of the in-scope procedures, processes, practices, or controls. Illumant uses as its rating system the controls maturity model defined by the Information Technology Governance Institute (ITGI):

Control Quality	
Rating	Characteristics
Stage 0: Nonexistent	At this level, there is a complete lack of any recognizable control process or the existence of any related procedures. The organization has not even acknowledged there is an issue to be addressed; therefore, no communication about the issue is generated.
Stage 1: Initial/Ad Hoc	There is some evidence the organization recognizes that controls and related procedures are important and need to be addressed. However, controls and related policies and procedures are not in place and documented. An event and disclosure process does not exist. Employees are not aware of their responsibility for control activities. The operating effectiveness of control activities is not evaluated on a regular basis. Control deficiencies are not identified.
Stage 2: Repeatable but Intuitive	Controls and related policies and procedures are in place but not always fully documented. An event and disclosure process is in place but not documented. Employees may not be aware of their responsibility for control activities. The operating effectiveness of control activities is not adequately evaluated on a regular basis and the process is not documented. Control deficiencies may be identified but are not remedied in a timely manner.
Stage 3: Defined Process	Controls and related policies and procedures are in place and adequately documented. An event and disclosure process is in place and adequately documented. Employees are aware of their responsibility for control activities. The operating effectiveness of control activities is evaluated on a periodic basis (e.g., quarterly); however, the process is not fully documented. Control deficiencies are identified and remedied in a timely manner.

<p>Stage 4: Managed and Measurable</p>	<p>Controls and related policies and procedures are in place and adequately documented, and employees are aware of their responsibility for control activities.</p> <p>An event and disclosure process is in place, adequately documented and monitored, but not always reevaluated to reflect major process or organizational changes.</p> <p>The operating effectiveness of control activities is evaluated on a periodic basis (e.g., weekly), and the process is adequately documented.</p> <p>There is limited, primarily tactical, use of technology to document processes, control objectives and activities.</p>
<p>Stage 5: Optimized</p>	<p>Stage 5 meets all of the characteristics of stage 4.</p> <p>An enterprise-wide control and risk management program exists such that controls and procedures are well documented and continuously reevaluated to reflect major process or organizational changes.</p> <p>A self-assessment process is used to evaluate the design and effectiveness of controls.</p> <p>Technology is leveraged to its fullest extent to document processes, control objectives and activities, identify gaps, and evaluate the effectiveness of controls.</p>

These evaluation criteria are used to identify systemic issues and opportunities for improvement. Furthermore, an assessment using these criteria enables stakeholders to more objectively evaluate findings and recommendations for each unit.

Results

For each department or administrative area, the following information is presented:

- Type, quantity and sensitivity of different data within the unit
- Threats to the exposure of sensitive data (e.g., joy-riders, hackers, viruses, malware, accidental disclosure, inadequately trained staff, etc.) with categorization (e.g., human, environmental, accidental or malicious)
- The likelihood of each threat being realized, taking into account vulnerabilities as well as strengths and weaknesses in security processes and countermeasures
- The potential consequences and impact of threats
- Estimated cost and complexity for effective risk mitigation

About the Author



Mat Siljak is Director, Advisory Services, at Illumant, where he drives compliance and enterprise security services at Illumant. Leveraging deep technology, regulatory, and risk management expertise, he has managed over 100 consulting engagements for firms ranging from Fortune 500 to pre-public companies along with numerous University clients. Mat has participated in many high profile conferences, including "Sarbanes-Oxley: Lessons from the Trenches" and "Sarbanes-Oxley and the CIO." He is CISA certified and is a member of ISACA, and the San Francisco Bay Area Chapter of InfraGard

which provides channels for the exchange of information about infrastructure threats and vulnerabilities

Prior to joining Illumant, Mat co-founded OLOSEC Network Security Solutions, an information security consulting firm based in Menlo Park, California. He previously held the position of Chief Technology Officer for Bullhound, Ltd., a global technology hedge fund based in London. Mat holds a B.S. and an M.S. in Electrical Engineering, both from Stanford University.



ILLUMANT

2672 Bayshore Parkway
Suite 505
Mountain View, CA 94043
Phone: +1 650.961.5911
Fax: +1 650.961.5912

www.illumant.com

ABOUT ILLUMANT

Illumant is a trusted strategic and tactical risk management advisor to Fortune 500 companies, higher education institutions, and other public and pre-public enterprises.

Leveraging best practices and deep knowledge of governance, risk management, compliance, and information technology, we partner with our clients to assess and solve critical business problems. Whether the focus is on initiatives driven by regulatory compliance, corporate mergers and acquisitions, or operational pain points, Illumant plays a major role in helping clients consistently meet their objectives.