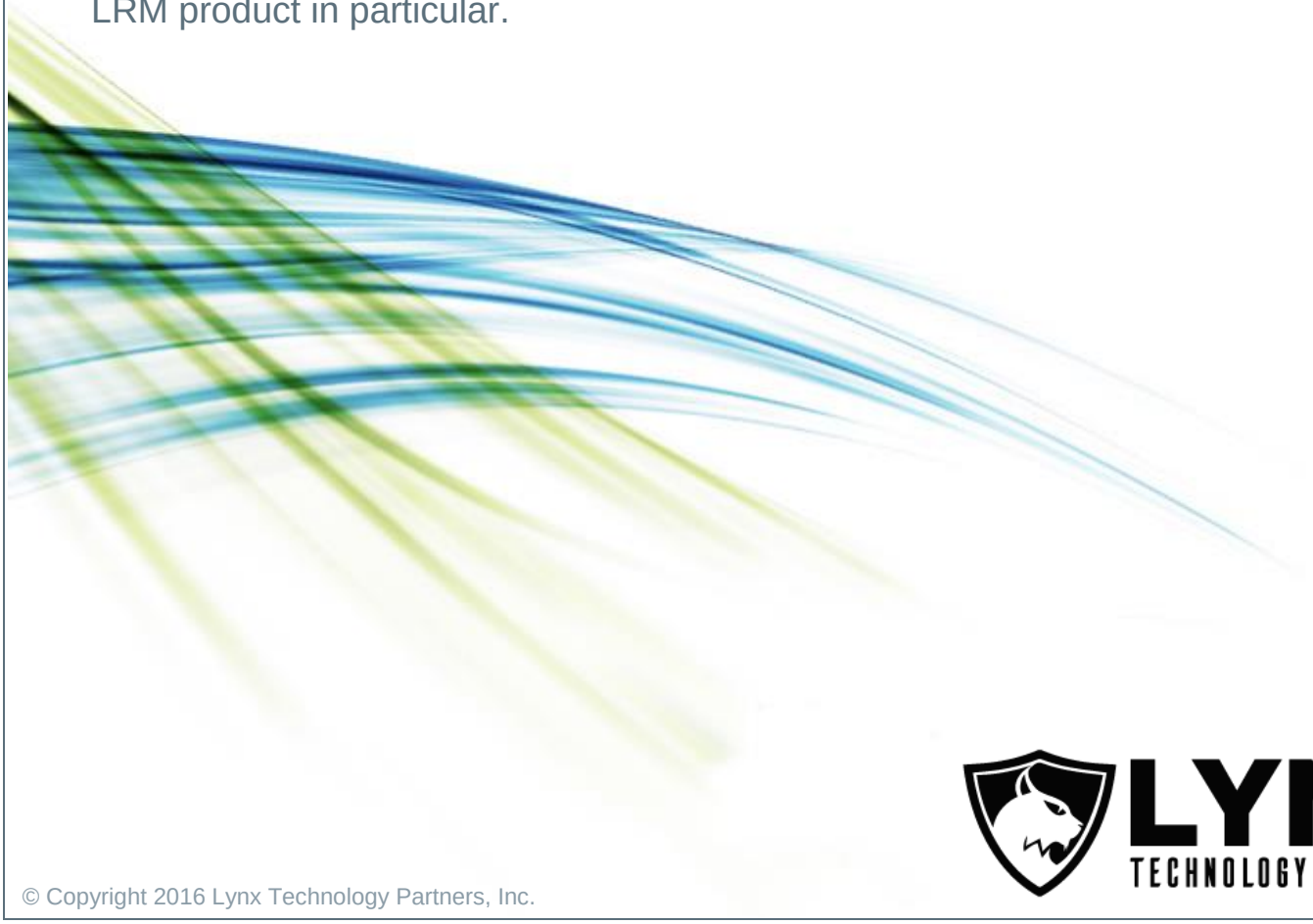
Lynx Risk Manager®

IT-GRC and Product Glossary

Overview

This document defines key terms from the IT-GRC industry in general and the LRM product in particular.



LYNX TECHNOLOGY PARTNERS

Product-Specific Terms

Term	Definition
Subject	Subjects are an abstraction of IT assets, expanded to include anything that needs to be tested during an assessment. A subjects can be an application, database, server (or group of similar servers), workstation (or group of similar workstations), network, facility, data center, group of people, or even the IT department or Security Team.
Asset	A specific tangible asset. One or more assets can be included as children to a subject. This allows a subject to represent a broad array of things, including single assets, a group of similar assets, or things that aren't assets at all.
Risk Profile	A collection of attributes on a subject which provide the information needed to determine what high-level threats the subject is exposed to, and what compliance mandates the subject is beholden to. Risk profile attributes are also used to automatically map controls to subjects. The customer can extend the attributes and groups available in the risk profile can be extended by customer
Risk Profile Assessment	A workflow tool that simplifies the process of collecting and asserting risk profile attributes. The workflow tool includes a survey feature that can be used to collect information from other participants.
Subject Criteria	A Boolean expression that operates on subject properties and risk profile attributes. For example, a subject criteria statement could be built as follows: All Subjects with Resource Type Application and Application Architecture Web Application and Exposure Externally-Facing This criteria statement would match all subjects that have those three attributes. Criteria Statements are used in several key places, including Dynamic Groups, Automatic Control Mapping, and Reference Scope Rules.
Subject Group	The static group that a subject lives in.

Term	Definition
Dynamic Group	Dynamic Groups contain subjects, but differ from static subject groups in that membership in a dynamic group is determined dynamically based on subject criteria statements that match subject properties. For example, a dynamic group with the following subject criteria statement: All Subjects with Resource Type Application and Application Architecture Web Application and Exposure Externally-Facing would include all subjects that matched those three attributes. Membership in a dynamic group is calculated dynamically, effectively updating dynamic group membership anytime a subject's risk profile attributes change.
Business Interest	The processes and information that matter to the business. These are the things that could have a business impact if they were compromised. Subjects support business interests. Customer information is a good example of a business interests. Subjects (the apps, databases, and servers that support customer information) would be mapped to it.
Business Impact Analysis (BIA)	A process for rating the expected business impact of a security breach affecting a business interest. Asks the simple question "what would happen to our business if customer information were disclosed to an unauthorized third party?" and uses that information to rate the criticality of the business interest.
BIA Survey	A survey-based process in LRM that asks business owners BIA questions and compiles responses into a rating.
Control	A technical, physical, or procedural activity designed to mitigate risk or satisfy compliance mandates.
Score	An assertion of whether a single control has been implemented appropriately on a subject. A Score is asserted as Pass, Fail, or Partial.
Observation	A detailed explanation of why a particular score was asserted on a control. For survey and manual controls, observations are entered by the person doing the scoring. For connector-driven score updates, the connector programmatically populates the observation.
Attachment	A document of any type can be attached to an object in LRM. The most common use of this is to attach a document to a score to serve as evidence that supports the pass / fail score that was asserted. Attachments can be attached to subjects, controls, and assessments as well. An attachment can be an actual document (any file), or a URL, which can be used to link to an external document repository such as Sharepoint.
Recency	Recency compares the time that has passed since a specific score was updated to the audit frequency defined for the corresponding control.

Term	Definition
Assessment	An Assessment captures workflow around the process of collecting manual assessment data. Assessments contain scope, which defines the specific subject and controls for which scores will be updated. Multiple Assessments can be performed at one time, allowing the total work for manual assessments to be divided into smaller pieces.
Survey (Control Survey)	A series of multiple-choice questions designed to collect information from system owners on whether key controls have been implemented on their systems. For example, a survey regarding user account request & approval procedures could be sent to an Application administrator to determine whether their procedures are in compliance with company policy. Although LRM has surveys for Controls, Risk Profiles, and Business Impact Analysis, when used on its own, the term "Survey" refers to a Control Survey.
Connector	A plug-in to LRM that allows the product to automatically collect scoring information from other products and 3rd party solutions.
Security Posture Index (SPI)	Scoring algorithm used in LRM. It is essentially a weighted average that produces a score between 0 and 100 for a given subject, business interest, or control. The algorithm is based on several factors including subject criticality rating, control importance level, and the control score (pass/fail/partial).
Key Performance Indicator (KPI)	A KPI is a metric tool available in LRM. A KPI consists of a Dynamic Group of Subjects, and one or more controls. The actual score of those subjects on those controls is compared to a threshold defined within the KPI.
Control Reference	Any authoritative reference source for controls information. Control References include Regulations, Standards, Best Practice Guides, and the Customer's Own Security Policy.
Threat	A high-level threat that identifies a risk scenario that should be considered for a subject.
Remediation Project	A collection of failing and partial control scores that will be remediated with a given project. LRM uses this construct to project the impact a project will have on risk & compliance metrics.

Industry Terms

Term	Definition	Source
Basel III	The Basel Capital Accord (Basel III) is an effort by international banking supervisors to provide large, internationally active banking organizations a uniform approach to risk-management practices. The applicable framework for information security in order to meet Basel III in the U.S. is the "FFIEC Information Security Booklet."	http://www.rsa.com/glossary http://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Compliance	Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.	www.theiia.org
Control	Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.	www.theiia.org
Control Environment	The attitude and actions of the board and management regarding the significance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements: • Integrity and ethical values • Management's philosophy and operating style • Organizational structure • Assignment of authority and responsibility • Human resource policies and practices • Competence of personnel	www.theiia.org

Term	Definition	Source
Control Processes	The policies, procedures, and activities that are part of a control framework, designed to ensure that risks are contained within the risk tolerances established by the risk management process.	www.theiia.org
Governance	The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.	www.theiia.org
Information Technology Controls	Controls that support business management and governance as well as provide general and technical controls over information technology infrastructures such as applications, information, infrastructure, and people.	www.theiia.org
Information Technology Governance	Consists of the leadership, organizational structures, and processes that ensure that the enterprise's information technology sustains and supports the organization's strategies and objectives.	www.theiia.org
Internal Audit	A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes.	www.theiia.org
Risk	The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.	www.theiia.org
Risk Appetite	The level of risk that an organization is willing to accept.	www.theiia.org
Risk Management	A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.	www.theiia.org

Term	Definition	Source
COBIT	Control Objectives for Information and related Technologies (COBIT) is a comprehensive approach to good IT practices. It is an important work for auditors, offered by the IT Governance Institute (ITGI) in close association with Information systems Audit and Control Association (ISACA). COBIT is consistent with ISO 27001 and other standards and frameworks.	www.rsa.com\glossary
HIPAA	Two parts of a comprehensive law for the medical industry, Health Insurance Portability and Accountability Act (HIPAA), are especially important for their security implications. As one of the first laws that applied to both privacy rights and information security in the United States, it has wide reaching implications.	www.rsa.com/glossary
GLBA	The Gramm-Leach-Bliley Financial Services Modernization Act of 1999 applies to all financial institutions in the U.S. regulated by the Office of the Comptroller of the Currency (OCC). GLBA requires that financial institutions ensure the security and confidentiality of customer personal information against "reasonably foreseeable" internal or external threats. From an information security perspective, organizations must implement a process that assesses and monitors the threat environment, as well as the tools and policies to counter threats, including access controls, authentication, encryption, data integrity controls and audit controls.	www.rsa.com/glossary
PCI DSS	The Payment Card Industry (PCI) Data Security Standard is an industry regulation developed by VISA, MasterCard and other bank card distributors that requires organizations handling bank cards to conform to security standards and follow certain leveled requirements for testing and reporting. The Standards rely on the merchant banks to enforce them and they may do so with penalties for non-compliance and disclosures caused by non-compliance.	www.rsa.com/glossary

Term	Definition	Source
ITIL	ITIL is the most widely accepted approach to IT service management in the world. ITIL provides a cohesive set of best practice, drawn from the public and private sectors internationally.	www.itil-officialsite.com