SKYWATCH[sm] RISK PROCESS BRIEFING

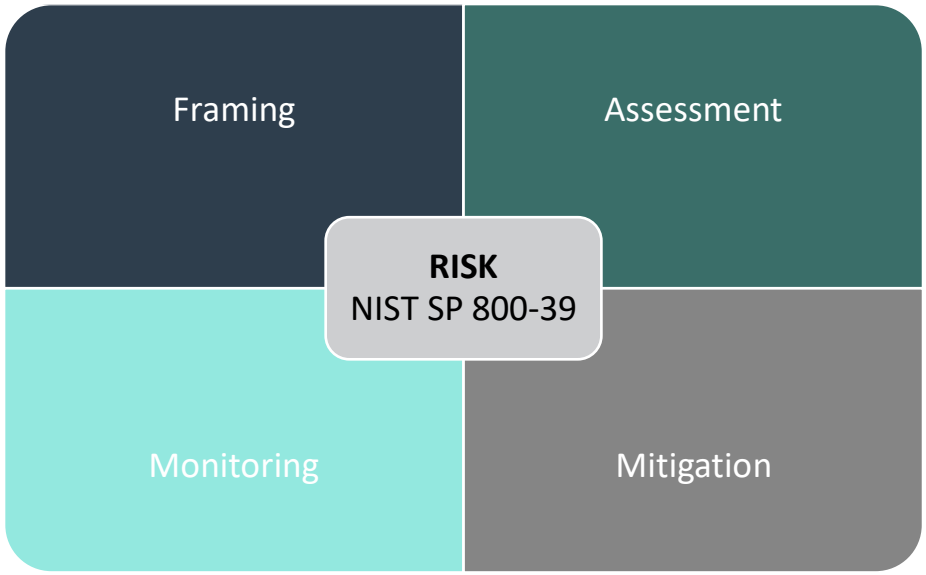
V071723

What is the SKYWATCH[sm] RISK PROCESS?

The SKYWATCH RISK PROCESS is a methodology to systematically reduce cybersecurity risk by following NIST Special Publication 800-39 using real-time cybersecurity information. The SKYWATCH RISK PROCESS depends on the combination of the SKYWATCH (ATTACK SURFACE MANAGEMENT) VULNERABILITY and THREAT MITIGATION processes.

How does it work?

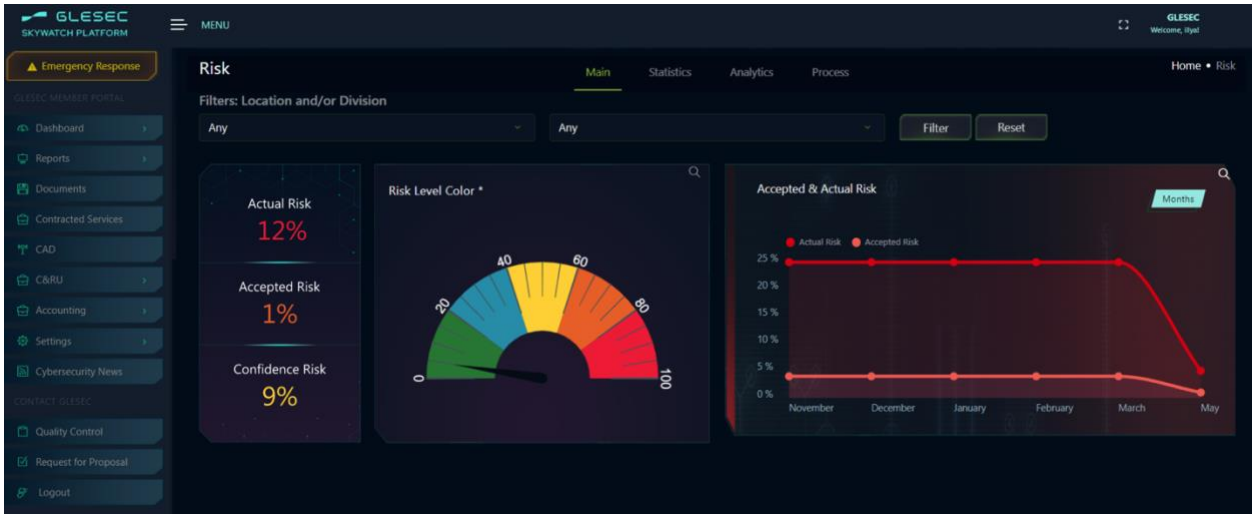
The SKYWATCH Platform is fully aligned and processes all the components of the NIST SP 800-39 model in real-time. Below an illustration of the components of the framework.



The Framing component is configured based on the client's environment and tolerance to risk conditions. The Risk Assessment is automated based on the Risk Matrix (see below) constructed with real-time information of threats and vulnerabilities to same assets. This also provides for monitoring and actionable intelligence. The latter is handled with GLESEC's Notable Events which are generated by SKYWATCH to alert the 7x24x365 SOC personnel that is involved in the mitigation aspects following the Vulnerability and the Threat Mitigation Processes.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

SKYWATCH represents RISK a vector of three variables as can be seen below.



Risk Element Dashboard presenting the three RISK metrics.

Actual Risk is the real-time risk calculated from the aggregation of conditions whereby threats are targeting client's assets that also have vulnerabilities.

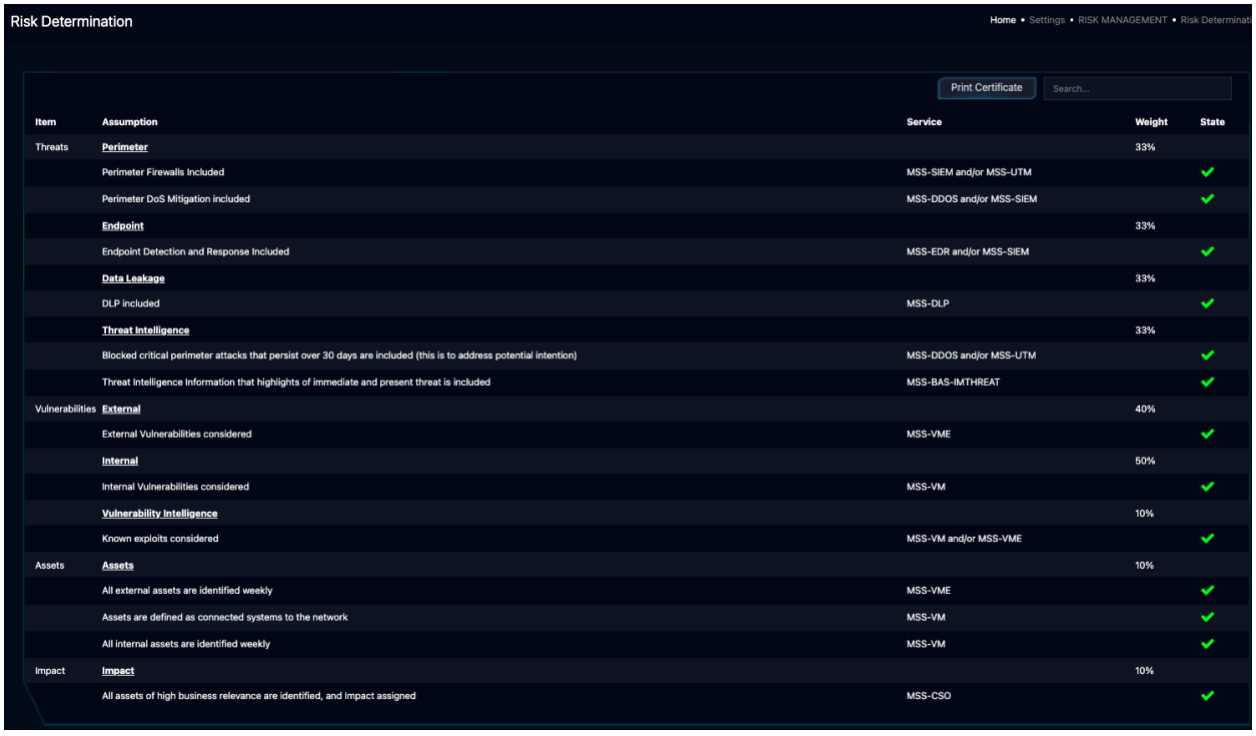
Risk Tolerance is derived from the weighted average of information in the Acceptable Risk Table (during setup) and applied to each of the components of threats and vulnerabilities obtained from Actual Risk.

Risk Confidence is the measure of confidence that the Risk information is representative. This is based on the quantity and quality of cybersecurity information. The more information we have the higher the confidence in the value of Risk. Note that if there is no Vulnerability or Threat information the Actual Risk becomes "undetermined", and the Risk Confidence is "0". With full information Risk Confidence is 100%, otherwise it is a calculated percentage based on the quantity and quality of the information.

How to use SKYWATCH to manage Risk?

The process starts with proper configuration setup. The client must complete answers to the tolerance level questions and setup the company divisions or departments. Then the Baseline Process takes place. This process is to discover assets (systems connected to the network), assign division, location, and impact level. Once this is completed, all the threats and vulnerability and hence Risk will be calculated based on the impact value, location, and division of these assets.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500



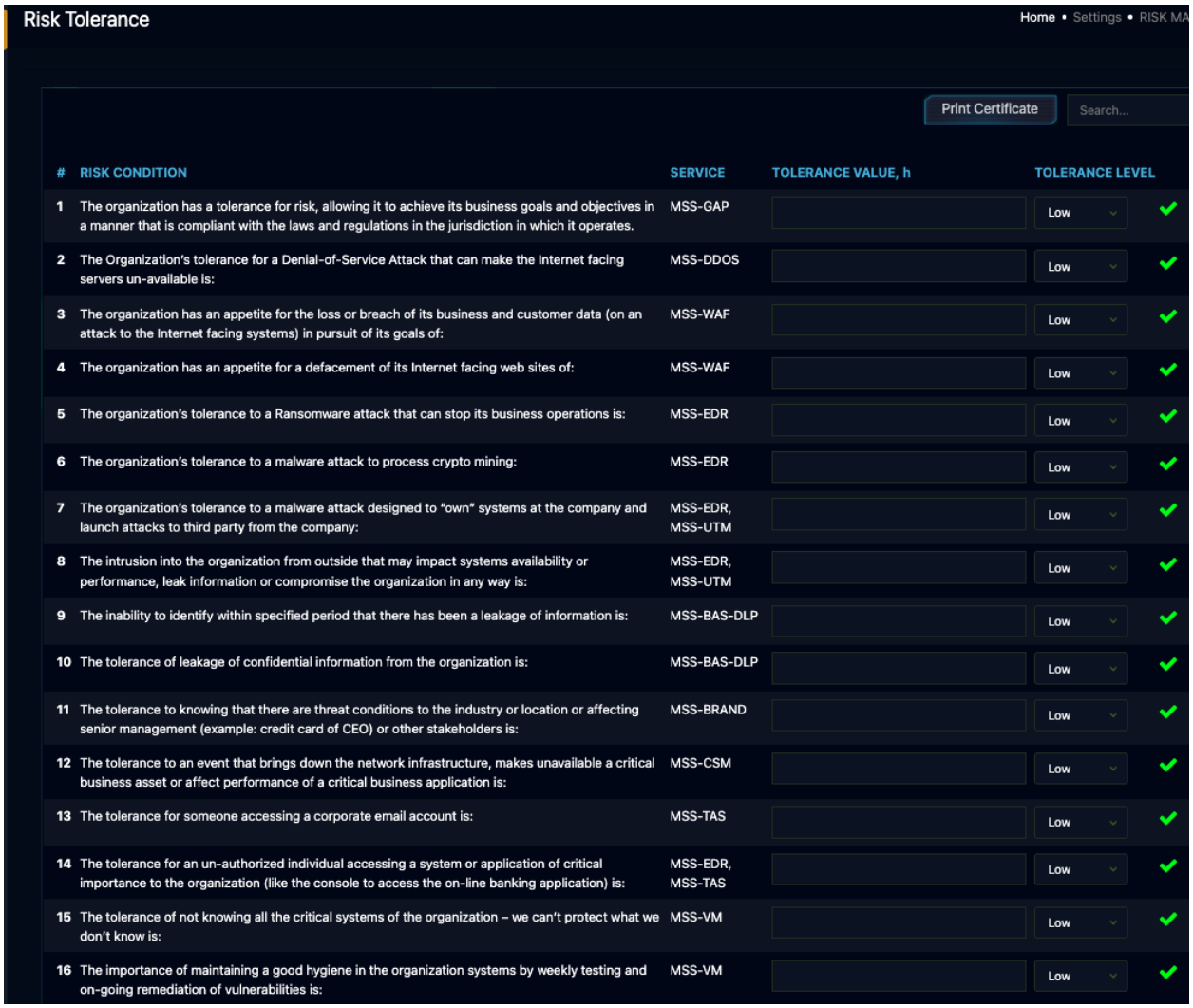
SKYWATCH Risk Determination information

There are two tracks to Risk Management for GLESEC, one is built into the process automation and SOC involvement and the other is performed by the client's stakeholders.
The first one is the one described above, whereby the security information is flowing in real-time, creating Risk Conditions and alerts which are followed up by the GLESEC SOC teams (GOCs) to remediate and mitigate.

The client can:

- Visualize Risk for the organization and departments.
- Generate Reports that highlight Risk.
- Monitor response by the organization and GLESEC in the process of Risk mitigation.
- Obtain certification from GLESEC of Risk status.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500



#	RISK CONDITION	SERVICE	TOLERANCE VALUE, h	TOLERANCE LEVEL
1	The organization has a tolerance for risk, allowing it to achieve its business goals and objectives in a manner that is compliant with the laws and regulations in the jurisdiction in which it operates.	MSS-GAP		Low
2	The Organization's tolerance for a Denial-of-Service Attack that can make the Internet facing servers un-available is:	MSS-DDOS		Low
3	The organization has an appetite for the loss or breach of its business and customer data (on an attack to the Internet facing systems) in pursuit of its goals of:	MSS-WAF		Low
4	The organization has an appetite for a defacement of its Internet facing web sites of:	MSS-WAF		Low
5	The organization's tolerance to a Ransomware attack that can stop its business operations is:	MSS-EDR		Low
6	The organization's tolerance to a malware attack to process crypto mining:	MSS-EDR		Low
7	The organization's tolerance to a malware attack designed to "own" systems at the company and launch attacks to third party from the company:	MSS-EDR, MSS-UTM		Low
8	The intrusion into the organization from outside that may impact systems availability or performance, leak information or compromise the organization in any way is:	MSS-EDR, MSS-UTM		Low
9	The inability to identify within specified period that there has been a leakage of information is:	MSS-BAS-DLP		Low
10	The tolerance of leakage of confidential information from the organization is:	MSS-BAS-DLP		Low
11	The tolerance to knowing that there are threat conditions to the industry or location or affecting senior management (example: credit card of CEO) or other stakeholders is:	MSS-BRAND		Low
12	The tolerance to an event that brings down the network infrastructure, makes unavailable a critical business asset or affect performance of a critical business application is:	MSS-CSM		Low
13	The tolerance for someone accessing a corporate email account is:	MSS-TAS		Low
14	The tolerance for an un-authorized individual accessing a system or application of critical importance to the organization (like the console to access the on-line banking application) is:	MSS-EDR, MSS-TAS		Low
15	The tolerance of not knowing all the critical systems of the organization – we can't protect what we don't know is:	MSS-VM		Low
16	The importance of maintaining a good hygiene in the organization systems by weekly testing and on-going remediation of vulnerabilities is:	MSS-VM		Low

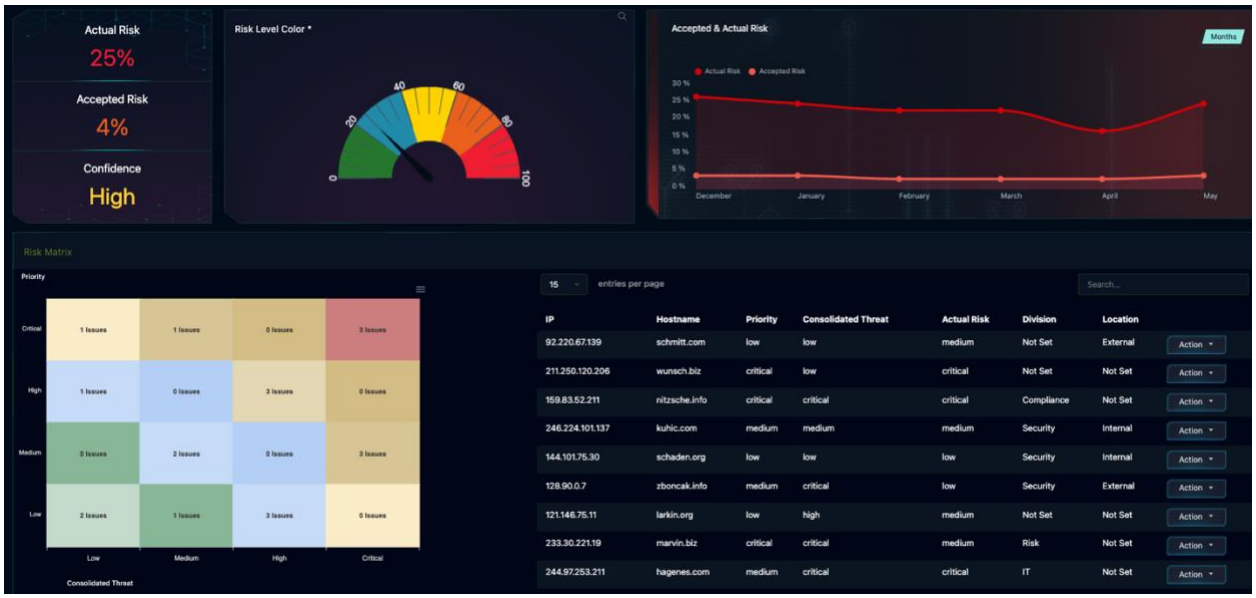
SKYWATCH Risk Tolerance Setting Table

Visualizing Risk

Clients can visualize Risk metrics in the SKYWATCH's main dashboard (Risk Element) and further to this, get more detailed information of risk gage, histogram, Risk matrix and Risk Conditions.

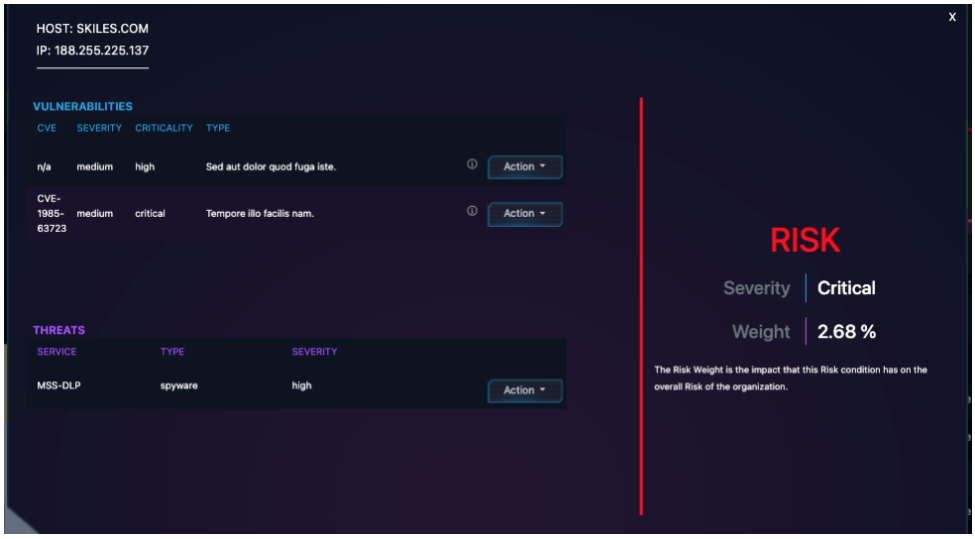
The Risk Matrix indicates the number of Risk Conditions for every quadrant of severity of *Priority* and *Threat Consolidation* for a host. By selecting any quadrant, the information to the right provides the list of all the Risk Conditions in that quadrant.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500



SKYWATCH Risk Element Dashboard

By selecting any Risk Condition, we can drill-down on its components of Threats and Vulnerabilities for a particular host. It also represents the Risk weight that this condition has and corresponding Severity.



SKYWATCH Risk Element – Risk Drill-down

Understanding SKYWATCH^{sm} Risk Metrics

The following table illustrates each of the three metrics used by SKYWATCH.

LATAM HQ +507 836-5355
US HQ +1 (321) 430-0500

Actual Risk	**Actual Risk** is the real-time risk calculated from the aggregation of conditions whereby threats are targeting client's assets that also have vulnerabilities.	Actual Risk is **Critical** when an asset (system/host) of the organization has Critical Priority, and it also is subject to Critical level Threats. To achieve this the asset must be of Critical business impact and have Critical Severity of Vulnerabilities. *While the vulnerabilities do not necessarily correlate to potential exploits by the threats that are being blocked, this condition must be considered of the highest level of concern to the organization and escalated to the senior management right away.* Actual Risk is **High** when an asset (system/host) of the organization has Critical Priority and High Consolidated Threat, or High Priority and High Consolidated Threat, or High Priority and Critical Consolidated Threat. To achieve this the asset must be of Critical or High business impact and have Critical or High Severity of Vulnerabilities. *The High Risk follows in priority handling to the Critical Risk and should be notified to management right away.* Actual Risk is **Medium** when an asset (system/host) of the organization has Medium Priority and Critical, High or Medium Consolidated Threats, or Medium Consolidated Threats and Critical, High or Medium Priority, or Critical Consolidated Threat and Low Priority, or High Priority and Low Consolidated Threat. To achieve this the asset must be of medium business impact and Medium Severity of Vulnerabilities, or Low Business Impact and Critical Severity of Vulnerability, or Critical Business Impact and Low Severity of Vulnerability. *The Medium Risk follows in priority handling to the High Risk.* Actual Risk is **Low** when an asset (system/host) of the organization has Low Priority, and it also is subject to High, Medium or Low-level Threats or Low Consolidated Threats and High, Medium or Low Priority. To achieve this the asset must be of Low business impact and High, Medium or Low Severity

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

		of Vulnerabilities, or Low Severity of Vulnerability and High, Medium or Low Business Impact. *While this is the lowest condition of concern to the organization it must not be ignored and consequently it will be pursued to be mitigated.*
Acceptable Risk	**Risk Tolerance** is derived from the answers to the questions during Setup under RISK Tolerance. These questions are mapped to threats, vulnerabilities, and assets and therefore to SKYWATCH services	**Critical** (80% to 100%) or **High** (70% to 80%) indicate that the questions are not of threat concern to the organization; while **Medium** (50% to 70%) or **Low** (0% to 50%) indicate that the organization is very concerned about these particular conditions and therefore the services that are mapped to this are of the greatest consequence to the organization.
Confidence	**Risk Confidence** is the adjustment of Actual Risk based on the quantity and quality of cybersecurity information. The more information we have the higher the confidence in the value of Risk.	The Confidence level implies that out of the threat mitigation countermeasures, vulnerability testing and asset management, **High** corresponds to 90% or more of the security data is available to determine Risk; **Medium** level to 60% to 90%; and **Low** Confidence level 0% to 60%. However, if no Threat or Vulnerability or Assets information is available, then the Confidence will be 0% since it will not be possible to determine risk.

Generating Reports

Clients can navigate to Executive Dashboards (Boardroom or CISO) to view the Risk and other cybersecurity parameters and choose to generate an on-demand report; or go to the Reports section to view or download a curated monthly report.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Monitoring Risk Mitigation

All the workflow activity of SKYWATCH and automated GLESEC Notable Events are CASES in the C&RU Utility of SKYWATCH. Then the GLESEC Operations Center personnel follow established Playbooks to work on Vulnerability Remediation and on Threat Mitigation activities for the contracted services by the client. This is performed 7x24x365. Clients can view the CASES at will or investigate the Reports section for the monthly Technical Reports for more information. There are many dashboards representing all the aspects of threats and vulnerabilities that can be used for additional insight if desired.

Risk Certification

The GLESEC Risk Certificate confirms that the organization is following NIST SP 800-39 alignment and represents that based on the functioning of SKYWATCH the Acceptable Risk and Risk Tolerance are of a specific value at the present time.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

The organization can generate a real-time Risk Certificate by selecting this button under the SKYWATCH / Settings / Risk Determination.

Definitions

The following are the definitions used in this document.

Term	Definition
Actual Risk	This is the real-time risk of the organization calculated from the Risk Matrix.
Acceptable Risk	The acceptable risk is the Actual Risk adjusted by the Risk Tolerance Table. This table is under the control of the client-organization.
Confidence	The confidence value is obtained by the quantity and quality of real-time cybersecurity information obtained. The more information the highest the confidence of Risk.
Priority	Priority is established by a matrix of Business Impact of the "asset" and Vulnerability Severity.
Threat Consolidation	This is the highest threat level for all the threats that a host is exposed to base on the information available to SKYWATCH.
Risk Conditions	A Risk Condition manifests when a threat and a vulnerability exist for a host that is in the baseline (inventor of system assets). This Risk Condition has a Risk weight (weighted average of all the Risk Conditions) and a Risk Severity (established by the Risk Matrix).

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500