1 Security capabilities metrics in the CHMM

1.1 Smart Grid Infrastructure indicators

The following table includes the base metrics that describe the level of adoption of SPEAR instruments in Smart Grids.

Table 1: Smart Grid Infrastructure metrics

Metric	Metric ID	Indicator ID	What is measured	Measure-ment value	Frequency of monitoring the metric	Who measures	Metric mapping to CHL
Monitoring of traffic data	SGI1	I.2.01	Existence of instruments and their usage for monitoring traffic data	Yes/No	weekly	Auditor	CHL1 no CHL2 periodically CHL 3,4,5 continuously
Monitoring of devices logs	SGI2	I.2.02	Existence of instruments and their usage for monitoring device logs	Yes/No	weekly	Auditor	CHL1 no CHL2 periodically CHL 3,4,5 continuously
Forensics is done on anomalies detected	SGI3	I.3.03	Existence of instruments and their usage for anomaly detection	Yes/No	weekly	Auditor	CHL1, 2 no CHL3 periodically CHL 4,5 continuously
Information sharing	SGI4	I.4.04	Existence of instruments and their usage for information sharing	Yes/No	weekly	Auditor	CHL1, 2 no CHL3 periodically CHL 4,5 continuously

1.2 Security policy organization metrics

Table 2 shows metrics that measure the Cyber Hygiene Policy in organization.

Table 2: Security policy organization metrics

Metric		Metric ID	Indicator ID	What is measured	Measurement value	Frequency of monitoring the metric	Who measures	Metric mapping to CHL
Security policy		SPO1	O.2.01	Existence of policy that includes Awareness & Training (AT)	Yes/No	Annually	Auditor	CHL1 No CHL 2, 3, 4, 5 Yes.
			O.3.01	Existence of fully documented policy that includes the AT	Yes/No	Annually	Auditor	CHL1,2 No CHL 3, 4, 5 Yes.
Incident response plan		SPO2	O.2.02	Existence of incident response plan	Yes/No	Monthly	Auditor	CHL1 No CHL 2, 3, 4, 5 Yes.
			O.3.02	Existence of fully documented incident response plan	Yes/No	Monthly	Auditor	CHL1,2 No CHL 3, 4, 5 Yes.

AT program		SPO3	O.2.03	Existence of AT program	Yes/No	Monthly	Auditor	CHL1 No CHL 2, 3, 4, 5 Yes.
			O.3.03	Existence of documented strategic plan with justification for the AT	Yes/No	Monthly	Auditor	CHL1,2 No CHL 3, 4, 5 Yes.
			O.3.13	The coverage of the AT program with various departments within SG organization	Yes/No	Monthly	Auditor	CHL1,2 No CHL 3, 4, 5 Yes.
			O.3.23	Existence of standardized CH process across SG organization	Yes/No	Monthly	Auditor	CHL1,2 No CHL 3, 4, 5 Yes.
			O.3.33	Existence of target groups based on roles/risks documented	Yes/No	Monthly	Auditor	CHL1,2 No CHL 3, 4, 5 Yes.
			O.3.43	Existence of the top human risks documented	Yes/No	Monthly	Auditor	CHL1,2 No CHL 3, 4, 5 Yes.
			O.4.13	The coverage of the AT program with multiple different target groups with unique training requirements	Yes/No	Monthly	Auditor	CHL1,2,3 No CHL 4, 5 Yes.
			O.4.23	Existence of standardized CH process tailored for specific departments	Yes/No	Monthly	Auditor	CHL1,2 No CHL 3, 4, 5 Yes.
			O.5.13	The coverage of documented approach for AT across all SG units	Yes/No	Annually	Auditor	CHL1,2,3,4 No CHL 5 Yes.
AT activities		SPO4	O.3.04	Existence of updates of AT program on annual basis	Yes/No	Annually	Auditor	CHL1,2 No CHL 3, 4, 5 Yes.
			O.3.14	Existence of continuous reinforcement of AT program throughout the year	Yes/No	Annually	Auditor	CHL1,2 No CHL 3, 4, 5 Yes.
			O.4.04	Existence of updates of AT program on monthly basis	Yes/No	Monthly	Auditor	CHL1,2,3 No CHL 4, 5 Yes.
			O.4.14	Existence of the review and measuring AT activities for effectiveness	Yes/No	Monthly	Auditor	CHL1,2,3 No CHL 4, 5 Yes.

Data back-up policy		SPO5	O.3.05	Existence of data back-up policy	Yes/No	Monthly	SPEAR SIEM	CHL1,2 No CHL 3, 4, 5 Yes.
Hardware documented		SPO6	O.X.06	Percentage of computers, connected devices (i.e. printers), and mobile devices (i.e. smartphones, tablets) documented.	(number of documented devises / total number of devices)*100%	Monthly	System administrator	CHL 1, 2 X<50% CHL 3 70%<X<50% CHL 4 X>70% CHL 5 X=100%
Software documented		SPO7	O.X.07	Percentage of programs, used by everyone on a particular network, that are installed directly onto computers documented.	(number of documented soft / total number of soft)*100%	Monthly	System administrator	CHL 1, 2 X<50% CHL 3 70%<X<50% CHL 4 X>70% CHL 5 X=100%
Applications documented		SPO8	O.X.08	Percentage of web apps (i.e. Dropbox, Google Drive), applications on phones and tablets, and any other program that isn't directly installed on devices that were documented.	(number of documented apps / total number of apps)*100 %	Monthly	System administrator	CHL 1, 2 X<50% CHL 3 70%<X<50% CHL 4 X>70% CHL 5 X=100%
Password changes		SPO9	O.X.09	Complex passwords changed regularly (changing passwords every 30 days)	Yes/No	Monthly or weekly	SPEAR SIEM	CHL1, 2, No CHL 3, 4, 5 Yes.
Hardware Updates		SPO10	O.X.010	Percentage of outdated and/or unused hardware (Unused equipment should be wiped and disposed of properly)	(number of unused equipment/ total number of equipment) *100%	Monthly	System administrator	CHL 1, 2 X<50% CHL 3 70%<X<50% CHL 4 X>70% CHL 5 X=100%
Software and app updates		SP O11	O.X.011	Check for updates at least once per week	Yes/No	Monthly	SPEAR SIEM	CHL1, 2, No CHL 3, 4, 5 Yes.
Not used software		SP O12	O.X.012	Percentage of unused software (If the programs aren't in regular use, they should be properly uninstalled).	(number of unused soft / total number of soft)*100%	Monthly	System administrator	CHL 1, 2 X<50% CHL 3 70%<X<50% CHL 4 X>70% CHL 5 X=100%

Data back-up policy		SP O13	O.X.01 3	Existence of data backup policy	Yes/No	Monthly	Auditor	CHL1, 2, No CHL 3, 4, 5 Yes.
Netiquette and Online Ethics		SP O14	O.X.01 4	Existence of set of rules for behaving properly online	Yes/No	Monthly	Auditor	CHL1, 2, No CHL 3, 4, 5 Yes.

1.3 Impact behaviour metrics

These metrics measure the impact of the SPEAR security awareness trainings. Specifically, the metrics aim to get insights on whether the SPEAR training sessions attended are changing people's behaviours, attitudes, or perceptions.

Table 3: People awareness metrics

Metric	Metric ID	Indicator ID	What is measured	Measu-rement method	Frequency	Who measures	Metric mapping to CHL
Operators / end users awareness	IBP1	P.2.01	Do SG operators and end-users confirm their awareness of security risks associated with their activities?	Yes/No	Annually	Auditor	CHL 1, No CHL 2, 3, 4, 5 Yes.
		P.3.01	Number of employers who confirm their awareness of security risks associated with their activities	Yes/No	Annually	Auditor	CHL 1, 2 X<50% CHL 3 50%<X<70% CHL 4 X>70% CHL 5 X=100%
		P.3.11	SG security team demonstrate awareness of using SPEAR FRF tool	Yes/No	Annually	Auditor	CHL 1, 2 X<90% CHL 3 X>90% CHL 4, 5 X=100%
		P.4.01	SG security team demonstrate awareness of using SPEAR RI tool	Yes/No	Annually	Auditor	CHL 1, 2, 3 X<90% CHL 4 X>90% CHL 5 X=100%
Ad hoc training topics	IBP2	P.2.02	Existence of ad hoc training topics + SPEAR SIEM	Yes/No	Annually	Auditor	CHL1 No CHL 2, 3, 4, 5 Yes.
		P.2.12	Do operators pass periodically security awareness training?	Yes/No	Annually	Auditor	CHL1 No CHL 2, 3, 4, 5 Yes.
		P.2.22	Do operators pass periodically computer-based training?	Yes/No	Annually	Auditor	CHL1 No CHL 2, 3, 4, 5 Yes.
		P.3.02	Existence of training topics focused on	Yes/No	Annually	Auditor	CHL1, 2 No CHL 3, 4, 5 Yes.

			general principles of CH in SG, phishing, social engineering, advanced persistent threat actors, suspicious behaviours + SPEAR FRF				
		P.4.02	Existence of training topics focused on practical exercises and information sharing using SPEAR RI	Yes/No	Annually	Auditor	CHL1, 2 ,3 No CHL 4, 5 Yes.
		P.5.02	The training is updated at least annually or when there are significant changes to the threat	Yes/No	Annually	Auditor	CHL1, 2 ,3, 4 No CHL 5 Yes.
AT program leadership	IBP3	P.3.03	Is there an AT program lead who is working on the full-time basis and is responsible for the AT program?	Yes/No	Annually	Auditor	CHL1, 2 No CHL 3, 4, 5 Yes.
		P.4.03	Department leads and teams request security reviews/audits	Yes/No	Annually	Auditor	CHL1, 2, 3 No CHL 4, 5 Yes.
		P.5.03	Leadership actively requests and uses security awareness metrics to measure their organizational progress / compare departments across organization	Yes/No	Annually	Auditor	CHL 1, 2, 3, 4 No CHL 5 Yes.
Phishing Awareness	IBP6	P.X.06	Percentage of people who fall victim to a phishing simulation. The definition of falling victim is clicking on the link or opening an attachment.	(number of people who clicked on the link/ total number of the training participants)*100%	Monthly	SPEAR RI	CHL 1 X>50% CHL 2 30%<X<50% CHL 3 10%<X<30% CHL 4 5%<X<10% CHL 5 X<5%
Phishing Reporting	IBP7	P.X.07	Percentage of people who detect and report a phishing email	Phishing assessment	Monthly	SPEAR RI	CHL 1 X>50% CHL 2 30%<X<50% CHL 3

			(regardless of whether it's an assessment or real attack).				10%<X<30% CHL 4 5%<X<10% CHL 5 X<5%
Phishing Repeat Offenders	IBP8	P.X.08	Number of workforce that repeatedly fall victim to phishing simulations. These individuals are not changing behaviour and represent a high risk.	Phishing assessment	Monthly	SPEAR RI	CHL 1 X>50% CHL 2 30%<X<50% CHL 3 10%<X<30% CHL 4 5%<X<10% CHL 5 X<5%
Updated Devices	IBP9	P.X.09	Percentage of devices that are updated and current.	When employees connect to an internal server or use the external services	Monthly	System adminis trated	CHL 1 X>50% CHL 2 30%<X<50% CHL 3 10%<X<30% CHL 4 5%<X<10% CHL 5 X<5%
Lost/Stolen Devices	IBP10	P.X.01 0	Number of devices that were lost or stolen. What percentage of those devices were encrypted?	Reports to security team or by physical asset audits	Monthly	Security team	CHL 1 X>50% CHL 2 30%<X<50% CHL 3 10%<X<30% CHL 4 5%<X<10% CHL 5 X<5%
Secure Desktop	IBP11	P.X.01 1	Number of employees who are securing their desk environment before leaving, per organizational policy.	Nightly walkthrough	Monthly or weekly	Auditor	CHL 1 X>50% CHL 2 30%<X<50% CHL 3 10%<X<30% CHL 4 5%<X<10% CHL 5 X<5%
Passwords	IBP12	P.X.01 2	Number of employees using strong passwords.	Password brute forcing	Monthly or quarterly	Security team	CHL1 X>50% CHL 2 30%<X<50% CHL 3 10%<X<30% CHL 4 5%<X<10% CHL 5 X<5%
Social Engineering	IBP13	P.X.01 3	Number of employees who can identify, stop, and report a social engineering attack.	Phone call assessments	Monthly	Auditor	CHL 1 X>50% CHL 2 30%<X<50% CHL 3 10%<X<30% CHL 4 5%<X<10% CHL 5 X<5%
Sensitive Data	IBP14	P.X.01 4	Number of employees securely disposing of any sensitive	Online searches for key terms	Monthly	Security team	CHL 1 X>50% CHL 2 30%<X<50% CHL 3 10%<X<30%

			documents into the shared bin.				CHL 4 5%<X<10% CHL 5 X<5%
Data Wiping or Destruction	IBP15	P.X.015	Number of employees who are properly following data destruction processes.	Check digital devices that are disposed of for proper wiping. Check dumpsters for sensitive documents.	Random	Security team	CHL 1 X>50% CHL 2 30%<X<50% CHL 3 10%<X<30% CHL 4 5%<X<10% CHL 5 X<5%
Device Physical Security	IBP16	P.X.016	Number of employees who left their devices unsecured.	Do a physical walkthrough of the sensitive areas and identify any off-handed devices that are visible.	Monthly	Security team	CHL 1 X>50% CHL 2 30%<X<50% CHL 3 10%<X<30% CHL 4 5%<X<10% CHL 5 X<5%
Engagement	IBP17	P.X.017	Number of requests the security awareness team gets to do security briefings for other business units or teams.	Tracking by the security awareness team	Monthly	Security team	CHL 1 X>50% CHL 2 30%<X<50% CHL 3 10%<X<30% CHL 4 5%<X<10% CHL 5 X<5%
Knowledge	IBP18	P.X.018	Does workforce know and understand what is expected of them?	Knowledge assessments and online quizzes	Annual or after training	Auditor	CHL 1 X>50% CHL 2 30%<X<50% CHL 3 10%<X<30% CHL 4 5%<X<10% CHL 5 X<5%
Workforce attitude towards security	IBP19	P.X.019	Does the workforce understand the need for security, the important role they play, and support the behaviors needed?	Cultural survey	Annual or after training	Auditor	CHL 1 X>50% CHL 2 30%<X<50% CHL 3 10%<X<30% CHL 4 5%<X<10% CHL 5 X<5%

1.4 Impact strategic metrics

These metrics measure how security awareness program is supporting the overall security program of SG infrastructure, and ultimately the mission of the SPEAR stakeholders.

Table 4: Impact strategic metrics

Metric	Metric ID	Indicator ID	What is measured	Measurement method	Frequency	Who measures
Time to Detect an Incident	ISS1	S.X.01	What is the average time it takes to detect an incident?	Standard incident report tracking processes	Monthly	SPEAR SIEM

Policy Violations	ISS2	S.X.02	Number of times workforce violates SG security policies.	Standard violation reporting processes	Monthly	SPEAR SIEM
Data Loss Incidents	ISS3	S.X.03	Number of times there is a data loss incident, either accidental or due to a deliberate attack.	Standard incident report tracking processes	Monthly	SPEAR SIEM
Infected Computers	ISS4	S.X.04	Number of infected computers.	Help Desk or centralized AV management software	Monthly	SPEAR SIEM
Privileged Account Abuse	ISS5	S.X.05	Number of privileged users that improperly use or abuse their privileged access.	Standard violation reporting processes	Monthly	SPEAR SIEM
Misconfigured Systems	ISS6	S.X.06	Number of incidents of systems or applications misconfigured.	Standard violation or incident reporting processes	Monthly	SPEAR SIEM
Compliance or Audit Violations	ISS7	S.X.07	Number of compliance or audit violations or fines.	Audit or compliance reports	Annual	Auditor

1.5 Compliance metrics

The following metrics measure the impact of SPEAR awareness trainings, specifically who we are training and how. These metrics are most valuable for compliance and auditing purposes.

Table 5: Compliance metrics

Metric	Metric ID	Indicator ID	What is measured	Measurement method	Frequency	Who measures
Training Completion	CMT1	T.X.01 P.2.02	Who has or has not completed annual security awareness training	Reports from LMS or sign-in sheets for on-site workshops	Annually	Auditor
Communication Methods	CMT2	T.X.02	Types of reinforcement training, who is consuming that training, and how often	Track and document when and how security awareness materials are communicated to the workforce.	Monthly	Auditor
Policy Sign-Off	CMT3	T.X.03	Ensuring employees have completed training, acknowledge they understand the training, and will adhere to the policies	Signature or sign-off	Part of annual review	Auditor

Security capabilities metrics can be used to effectively and consistently measuring the current CH maturity via simplified information collection and reporting, consistent testing procedures and scoring enabling SG organizations to clearly identify improvement points in order to reach higher maturity levels.

2 Cyber Hygiene Maturity Assessment Framework

Complementary to the SPEAR Cyber Hygiene Maturity Model (CHMM), in this Section we propose a self-assessment methodology based on a questionnaire for Smart Grid (SG) cyber hygiene practices evaluation. The result of the assessment can be used as a health check to define countermeasures and to reapprove cyber hygiene rules as well as security standards and specifications adopted by the Smart Grid operator organisation.

2.1 Methodology

The SPEAR CHF addresses two major goals in the cyber hygiene playground; firstly, it adopts base cyber hygiene practices for smart grid landscape and secondly, it guides the Smart Grid operator organizations by taking simple measures to boost their overall cybersecurity posture and achieve high cyber hygiene level with respect to cyber security, privacy and data protection issues.

The structure of the framework adopted for the SPEAR CHMM is inspired from DoD Cybersecurity Maturity Model Certification (CMMC) v1.02 (of 18 March 2020). It enables to evaluate the level of cyber hygiene in the SG organization. Furthermore, the SPEAR-CHF, developed in WP5, aims at assuring cyber awareness and readiness of Smart Grid personnel and customers to different cyber threats and cyber-attack incidents.

To collect information relevant to the evaluation of the CHL, we developed a questionnaire. Most of the questions need to be answered with Yes/No type of responses. The SPEAR CHMM auditor (who could be internal or external staff of the Smart Grid operator organisation) would assess the maturity level by making questions to cybersecurity responsible personnel oriented to measure Yes/No availability of practices proposed by the CHMM and in case the practice is measurable, evaluate the metrics of indicator tables 1-5.

The final result of the assessment would therefore be the identification of the cyber hygiene level the organisation is in, with the results of the values of the metrics measured for each of the practices, and then a report on the recommended activities to carry out or adopt in the organisation to progress to the next maturity level so as the organisation can increase in cyber protection and preparedness against cyber incidents or attacks.

2.2 Cyber Hygiene Maturity Assessment

SPEAR-CHF enables to verify if SG organization matches the requirements to reach a certain cyber hygiene maturity level and due to simplified information collection can be used to automate CH maturity assessment. The assessment also emphasizes the level of adoption of standards and best practices in cyber hygiene for each control area, as well as its effectiveness and maturity of internal policies and procedures.

As in many risk assessment approaches, assessors in SPEAR-CHF typically evaluate indicators based on whether they are in place or implemented, resulting in a binary (Yes/No), and compliance-oriented manner.

The CHM assessment procedure usually starts by creating an assessment plan. Information about schedule, people involved and measuring methods can be found in tables 1-5. Then a group of assessors collect all the necessary evidence, calculate the maturity levels and generate the report which details the findings and CH maturity levels for each domain. Based on the assessment results, the SG organization can plan for improvement by following a new ML target.

Table 6 presents the summary of the assessment items evaluated by the SPEAR CHMM Assessment Framework proposed.

Table 6: SPEAR Cyber Hygiene Maturity Assessment v1.0

Domain	ID	Indicators	CHL				
			1	2	3	4	5
Smart Grid Infrastructure	I.2.01	The tool(s) that monitor traffic data have been installed	N/A	ML2	ML3	ML4	ML5
	I.2.02	The tool(s) that monitor device logs have been installed	N/A	ML2	ML3	ML4	ML5
	I.2.11	The monitoring traffic data is done periodically (at least once a month)	N/A	ML2	ML3	ML4	ML5
	I.2.22	The monitoring device logs is done periodically (at least once a month)	N/A	ML2	ML3	ML4	ML5
	I.3.11	The monitoring traffic data is done continuously (at least once a week)	N/A	N/A	ML3	ML4	ML5
	I.3.22	The monitoring device logs is done continuously (at least once a week)	N/A	N/A	ML3	ML4	ML5
	I.3.03	The tool(s) for anomaly detection have been installed	N/A	N/A	ML3	ML4	ML5
	I.3.13	The tool(s) for anomaly detection are used periodically (at least once a month)	N/A	N/A	ML3	ML4	ML5
	I.4.23	The tool(s) for anomaly detection are used continuously (at least once a week)	N/A	N/A	N/A	ML4	ML5
	I.4.04	The tool(s) for information sharing (e.g. SPEAR-RI) have been installed	N/A	N/A	N/A	ML4	ML5
	I.4.14	The tools for information sharing are used for sharing information between SG organizations periodically (at least once a month)	N/A	N/A	N/A	ML4	ML5
	I.5.24	The tool(s) for information sharing are used continuously (at least once a week)	N/A	N/A	N/A	N/A	ML5
Organization (policies, standards)	O.2.01	A policy that includes Awareness & Training (AT) has been established	N/A	ML2	ML3	ML4	ML5
	O.2.02	An incident response plan exists	N/A	ML2	ML3	ML4	ML5
	O.2.03	The AT program has been established	N/A	ML2	ML3	ML4	ML5
	O.3.01	A policy that includes the AT is fully documented	N/A	N/A	ML3	ML4	ML5
	O.3.02	An incident response plan is fully documented and includes strategic plan and schedule of trainings	N/A	N/A	ML3	ML4	ML5
	O.3.03	A strategic plan that has identified the scope, goals, objectives and justification for the AT is documented	N/A	N/A	ML3	ML4	ML5
	O.3.05	Data back-up policy has been established	N/A	N/A	ML3	ML4	ML5

	O.3.33	Organization has clearly defined target groups, usually based on roles / risks but can also be defined by language, region or other drivers.	N/A	N/A	ML3	ML4	ML5
	O.3.43	The top human risks and the behaviours that most effectively manage those risks have been identified and explained.	N/A	N/A	ML3	ML4	ML5
	O.3.13	The AT program coordinates and collaborates with various departments within organization, including Communications, Human Resources, and Help Desk.	N/A	N/A	ML3	ML4	ML5
	O.3.04	The AT program is actively reviewed and updated on an annual basis	N/A	N/A	ML3	ML4	ML5
	O.3.23	A cyber hygiene process is defined as a standard across the organization	N/A	N/A	ML3	ML4	ML5
	O.3.14	The AT program includes continuous reinforcement throughout the year	N/A	N/A	ML3	ML4	ML5
	O.4.23	A cyber hygiene process is tailored for specific departments	N/A	N/A	N/A	ML4	ML5
	O.4.04	The AT program is actively reviewed and updated on a monthly basis	N/A	N/A	N/A	ML4	ML5
	O.4.13	The AT program includes identified multiple different target groups that have unique training requirements, including skills-based training for IT-department groups, developer groups, etc.	N/A	N/A	N/A	ML4	ML5
	O.4.14	A review and measure AT activities for effectiveness is performed on a monthly basis	N/A	N/A	N/A	ML4	ML5
	O.5.13	A documented approach for AT across all SG units has been standardized and optimised across the organization (on an annual basis)	N/A	N/A	N/A	N/A	ML5
People (awareness, education and training)	P.2.01	Operators and end-users declare that they are made aware of security risks associated with their activities and of the applicable policies, standards and procedures related to the security of SG systems	N/A	ML2	ML3	ML4	ML5
	P.2.02	Operators pass periodically security awareness training on recognizing and reporting potential insider threat as well as on using SPEAR SIEM tools	N/A	ML2	ML3	ML4	ML5
	P.2.12	There are on-time ad hoc training topics deployed once a year	N/A	ML2	ML3	ML4	ML5
	P.2.22	Operators pass periodically computer-based training, with support materials during the year	N/A	ML2	ML3	ML4	ML5
	P.3.03	There is an AT program lead who is working on the full-time basis and is responsible for development, implementation and updating the AT program	N/A	N/A	ML3	ML4	ML5

	P.3.02	Training topics are focused on general principles of cyber hygiene in Smart Grid, phishing, social engineering, advanced persistent threat actors, suspicious behaviours and using SPEAR FRF tool (including demonstrations) and deployed on periodic basis	N/A	N/A	ML3	ML4	ML5
	P.3.01	Operators and end-users demonstrate awareness of security risks associated with their activities and of the applicable policies, standards and procedures related to the security of SG	N/A	N/A	ML3	ML4	ML5
	P.3.11	SG security team demonstrate awareness of using SPEAR FRF tool	N/A	N/A	ML3	ML4	ML5
	P.3.05	Training topics include practical exercises in awareness training aligned with current threat scenarios, provide feedback to individuals involved in training, information sharing, using SPEAR RI	N/A	N/A	ML3	ML4	ML5
	P.4.03	Department leads and teams request security reviews/audits	N/A	N/A	N/A	ML4	ML5
	P.4.02	SG security team demonstrate awareness of using SPEAR RI tool	N/A	N/A	N/A	ML4	ML5
	P.5.02	The training is updated at least annually or when there are significant changes to the threat	N/A	N/A	N/A	N/A	ML5
	P.5.03	Leadership actively requests and uses security awareness metrics to measure their organizational progress / compare departments across organization	N/A	N/A	N/A	N/A	ML5