UNIVERSITÀ DI PISA

DIPARTIMENTO DI INGEGNERIA DELL'ENERGIA DEI SISTEMI DEL TERRITORIO E DELLE COSTRUZIONI

RELAZIONE PER IL CONSEGUIMENTO DELLA LAUREA MAGISTRALE IN INGEGNERIA GESTIONALE

Sviluppo di un sistema di gestione finalizzato al raggiungimento della certificazione TISAX in una Azienda multinazionale del settore automotive

SINTESI

RELATORI

Prof. Gionata Carmignani
Dipartimento di Ingegneria dell'Energia, dei Sistemi, del Territorio e delle Costruzioni

Ing. Stefano Ughi
Magna Closures S.p.A.

IL CANDIDATO

Andrea Cargiolli
andrea.2.97.ac@gmail.com

Sessione di Laurea Magistrale del 27/04/2022

Sviluppo di un sistema di gestione finalizzato al raggiungimento della certificazione TISAX in una Azienda multinazionale del settore automotive

Andrea Cargiolli

Sommario

Questo lavoro di tesi consiste nel processo di preparazione svolto presso la Divisione Motrol della multinazionale Magna Closures S.p.A. al fine di farle raggiungere un livello di maturità adeguato a sostenere e superare un audit di certificazione TISAX (Trusted Information Security Assessment Exchange).

TISAX rappresenta uno strumento che permette, nell'ambito del settore automobilistico, lo scambio di autovalutazioni certificate relative alla sicurezza delle informazioni tra clienti e fornitori. Per portare avanti il processo di autovalutazione sono state seguite le indicazioni e i formati che VDA, Associazione tedesca dell'industria automobilistica, ha elaborato sulla base dei requisiti della norma ISO 27001. Il fulcro del lavoro si è tradotto principalmente nella procedurizzazione di una serie di attività importanti per garantire l'*Information Security* e nella creazione di consapevolezza aziendale nei confronti del tema, tramite l'organizzazione di corsi di formazione e l'inserimento di aspetti di sicurezza delle informazioni all'interno di processi che, in precedenza, non li contemplavano.

Abstract

This thesis work concerns the preparation process carried out in the Motrol Division of Magna Closures S.p.A. multinational in order to reach an adequate maturity level to perform and pass a TISAX (Trusted Information Security Assessment Exchange) certification audit.

TISAX is a tool that allows the exchange of certified Information Security assessments between clients and suppliers in automotive. Indications and formats that VDA, the German Association of the Automotive Industry, has developed on the ISO 27001 standard basis, have been used to carry out the self-assessment process. The main tasks of the work have been the formalization of procedures on activities needed to guarantee the Information Security and the raising of corporate awareness; this last goal has been accomplished through training courses and including Information Security aspects in processes that previously didn't comprehend them.

1. Contesto

Magna International è una multinazionale canadese che ha sede ad Aurora, in Ontario. Magna controlla una serie di Gruppi che producono una grande varietà di parti e componenti per le aziende automobilistiche: Cosma, Electronics, Exteriors, MML (Mechatronics, Mirrors & Lighting), Powertrain, Seating e Steyr.

La divisione Motrol, il luogo in cui è stato portato avanti il progetto di cui si discute in questo elaborato, fa parte di Magna Mechatronics. Motrol si trova in Italia, a Guasticce - Collesalvetti (LI), impiega circa 540 dipendenti e produce annualmente circa 14.000.000 di unità. La divisione è specializzata nella realizzazione di sistemi di chiusura: la produzione varia dal semplice scontrino, il componente metallico addetto alla chiusura della portiera, all'assemblaggio di intere serrature, fino ad arrivare alla creazione di interi moduli porta. Meno comune, invece, è la produzione di alzacristalli e sistemi anti-pinch[1].

Tra i prodotti "di punta" di Motrol ci sono, senza dubbio, le SmartLatch, modelli di serrature che sostituiscono il classico funzionamento meccanico dell'apertura della portiera con uno elettronico.

Motrol è un contesto aziendale modernamente organizzato, di conseguenza, presenta diversi sistemi di gestione integrati tra loro: un sistema di gestione della qualità che segue le prescrizioni delle norme ISO 9001 e IATF (International Automotive Task Force) 16949, un sistema di gestione ambientale conforme alla ISO 14001 e un sistema di gestione della salute e sicurezza sul lavoro basato sull'applicazione dell'ISO 45001. La sfida più grande del progetto di introduzione di TISAX consiste nello sviluppo di un sistema di gestione della sicurezza delle informazioni che vada ad integrarsi con le procedure e le regolamentazioni già in atto all'interno di un ambiente simile.

2. Information Security Assessment

La certificazione TISAX consiste in un processo di valutazione del livello di maturità del sistema di gestione della sicurezza delle informazioni di un'azienda. Il superamento di un audit TISAX comporta anche la condivisione di tale valutazione con altre aziende grazie a un portale dedicato, sviluppato da ENX, associazione che comprende produttori, relativi

Sistema anti-pinch[1]: Strumento in grado di fornire la funzione grazie alla quale a un portellone posteriore elettrico (questo nel caso di Motrol; il sistema in altri contesti è applicabile anche agli alza-cristalli) è impedito di portare a termine automaticamente il proprio movimento di chiusura nel caso in cui si imbatta in un'ostruzione.

fornitori e organizzazioni operanti nel settore automotive in Europa.

È stata proprio una di queste organizzazioni, VDA, a elaborare uno standard industriale basato sulle prescrizioni della norma ISO 27001, l'Information Security Assessment (ISA). Tale documento è stato scelto da ENX come quello tramite il quale effettuare la valutazione e la successiva concessione della certificazione TISAX.

L'ISA consiste in una serie di fogli Excel contenenti gli strumenti necessari per effettuare un *assessment* riguardante i temi di *Information Security*, *Prototype Protection* e *Data Protection.* Per ogni punto di ciascuna delle aree citate è presente una domanda di controllo che ne espone i contenuti, simulando il quesito che un auditor potrebbe formulare relativamente al tema. Al fine di chiarire ulteriormente che cosa sia richiesto dal documento, sono presenti alcune sezioni di requisiti che spiegano più nello specifico quali siano le condizioni necessarie sulla base delle quali è possibile ritenersi conformi alla norma in relazione alle tematiche espresse in ogni domanda di controllo.

Il completamento dell'ISA procede con l'assegnazione di un "Maturity level" da 0 (Incompleto) a 5 (Ottimizzato) a seconda di quanto si valuti di essere in *compliance* con i requisiti esplicitati; a supporto di ciò, devono essere inserite, nelle apposite sezioni, la descrizione delle misure in atto in azienda e, soprattutto, le evidenze in grado di dimostrare quanto dichiarato.

Alla divisione Motrol è stato richiesto di completare due sezioni su tre dell'ISA, quella di *Information Security* e quella di *Prototype Protection* (63 domande di controllo in totale), raggiungendo un punteggio minimo (media dei *Maturity Levels* di ognuno dei punti del documento) di 2.9. In realtà il valore minimo che si può totalizzare per ottenere la certificazione è di 2.7 ma è stato deciso dalla "Casa Madre" che, per stimolare la ricerca dell'eccellenza, la soglia limite dovesse attestarsi su un valore maggiormente sfidante per le proprie divisioni.

3. Condizione iniziale

L'Azienda, al momento dell'inizio del progetto di preparazione all'audit TISAX, presentava "fisiologicamente" alcuni gap con il livello di maturità richiesto per ottenere la certificazione. Nonostante ciò, non si sta trattando di un lavoro che è partito da zero: si ricorda che Motrol è una divisione di una multinazionale e di conseguenza è fortemente strutturata e procedurizzata per quanto riguarda i sistemi di gestione (qualità, ambiente e sicurezza).

Inoltre, diversi controlli suggeriti dalla norma, specialmente quelli riguardanti la sicurezza IT (*Information Technology*), erano già in atto senza che fossero richiesti da un ente di certificazione, semplicemente per garantire all'Azienda una protezione sufficiente dal punto di vista della sicurezza informatica.

Di seguito (Fig.1) viene riportato il grafico radar che riassume la conformità iniziale di Motrol in relazione ai requisiti espressi nei diversi capitoli dell'Information Security Assessment:

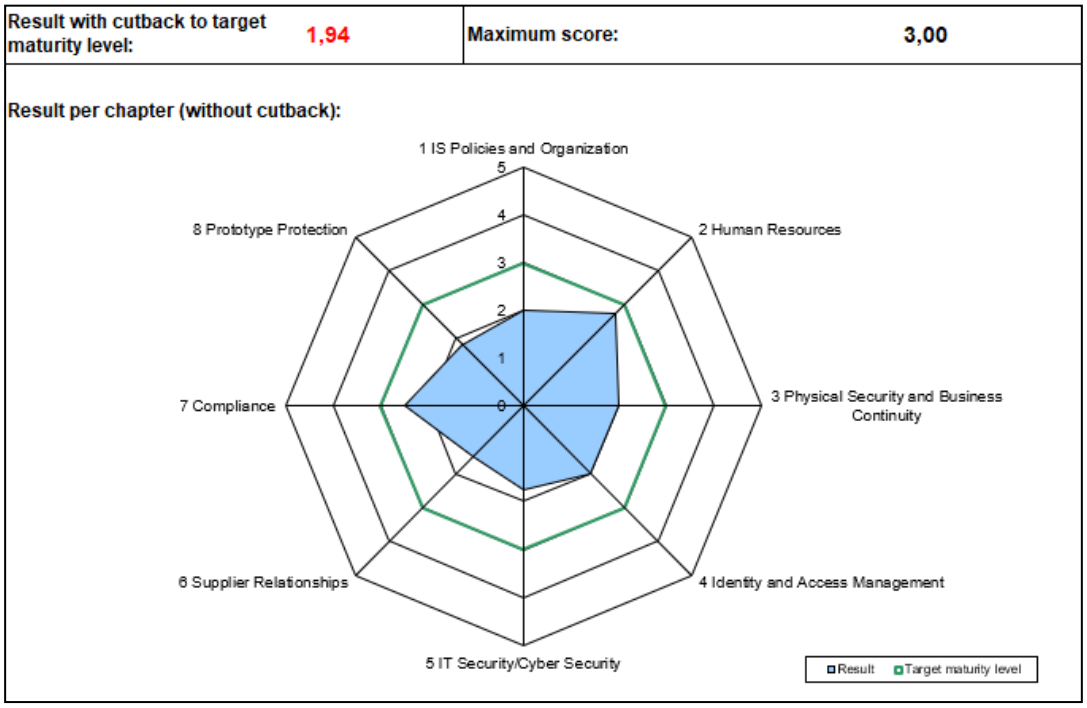

Fig.1 : Radar della condizione "as is" di Motrol

Dal grafico si può notare come poche aree di TISAX siano mediamente sotto al punteggio di 2; tra esse la più bassa è il capitolo 6, *Supplier Relationship*, ma tale valore è condizionato dal fatto che la sezione è costituita solamente da due domande di controllo. Per quanto riguarda gli altri punteggi, la motivazione per gli *score* che si attestano intorno al 2 consiste nel fatto che, nella maggior parte dei casi, i processi richiesti erano già stati implementati in Azienda, ma, talvolta, ne mancava una corretta formalizzazione o la documentazione sotto forma di procedura in maniera conforme a quanto richiesto da TISAX. Gli ambiti principali in cui è stato portato avanti il progetto saranno individuati in modo più specifico nel capitolo seguente.

4. Misure adottate

Come già riportato in precedenza, il progetto di autovalutazione TISAX e, di conseguenza, l'elaborato sviluppato sulla base di esso si "snodano" in 63 diversi argomenti, individuati da altrettante *control question*. Mentre nella tesi, l'ISA è stato trattato punto per punto, in questa sintesi, per motivi di brevità, saranno individuate e accorpate le attività chiave che hanno fatto in modo di migliorare il livello di maturità *Information Security* dell'Azienda fino ad arrivare ad un punto per il quale potesse essere ritenuta pronta ad affrontare un audit TISAX.

4.1. Sensibilizzazione aziendale

Una delle macro-attività cruciali che sono state affrontate nel corso del progetto è rappresentata, senza dubbio, dalla creazione di un livello di consapevolezza adeguato presso i dipendenti in merito al tema della sicurezza delle informazioni. Naturalmente, un ambiente in cui i soggetti conoscono i rischi e soprattutto le motivazioni per cui alcune misure o procedure devono essere rispettate si traduce spesso in un ambiente più sicuro e collaborativo.

Per essere precisi, anche in questo ambito, il lavoro non è partito da zero; Magna, infatti, fa seguire periodicamente dei corsi che definisce di "Security Awareness" ai suoi dipendenti, nei quali vengono comunicati concetti chiave riguardanti *l'Information Security*. Inoltre, tali nozioni vengono integrate all'assunzione di ogni dipendente con un corso incentrato sull' "altra faccia" della sicurezza delle informazioni, la componente *Data Privacy*.

Nonostante ciò, un'attenta analisi del contenuto dei vari corsi di formazione ha evidenziato la necessità di approfondire alcuni argomenti specifici. Per tale motivo, con l'ausilio delle indicazioni contenute nell'Information Security Assessment stesso e con i consigli del team di esperti TISAX che mi ha supportato durante lo svolgimento del progetto, mi è stato possibile preparare del materiale sotto forma di slide Power Point e tenere dei corsi integrativi di sicurezza delle informazioni. Uno di questi, battezzato come "Aggiornamento su temi di Information Security" si è svolto tramite Teams meeting e ha coinvolto tutti coloro che in Motrol hanno accesso alla rete aziendale tramite dispositivo fisso o portatile.

I temi approfonditi nel corso sono stati: la classificazione delle informazioni e l'utilizzo di Unified Labeling di Azure, la classificazione delle zone aziendali a seconda della confidenzialità delle informazioni che contengono e la Clean Desk Policy.

Per quanto riguarda la prima tematica, vi è necessità di fornire delle precisazioni. La norma TISAX prevede che ogni documento venga classificato con un livello di criticità diverso a seconda della delicatezza dell'informazione che contiene, in modo che sia possibile adottare misure adeguate alla preservazione della confidenzialità di ogni tipo di dato. Relativamente al tema, Motrol, già nella sua condizione "as is", aveva un importante grado di conformità, sia dal punto di vista delle *policy* aziendali che da quello dell'applicazione pratica: quest'ultima era garantita dall'uso di Unified Labeling, un software di Microsoft Azure in grado di integrarsi in ambienti Word, Excel e Outlook per "marcare" l'informazione in base ai livelli di confidenzialità stabiliti dalle politiche aziendali (in Magna si parla di *Internal*, *Confidential* e *Strictly Confidential*, con livello di riservatezza crescente). Il corso di formazione, quindi, è risultato necessario per sensibilizzare i dipendenti relativamente a tali livelli di confidenzialità, che non erano noti a tutti, e, soprattutto, per trasmettere la necessità di una corretta catalogazione dei documenti tramite Microsoft Azure (si consideri che qualsiasi documento non classificato viene di default definito "Internal", di conseguenza, i dipendenti che non conoscono la modalità di classificazione possono inconsapevolmente etichettare come "Internal" dei dati che in realtà presentano una riservatezza maggiore).

Il secondo punto del corso è stato la comunicazione dell'output del processo di classificazione delle aree aziendali, che è stato portato avanti per garantire la conformità a TISAX e che verrà approfondito nel prossimo paragrafo della sintesi (si può trovare anche al capitolo 2.3.1 della tesi). Basti sapere che Motrol è stata suddivisa in 4 differenti tipi di area, a seconda della riservatezza delle informazioni contenute al loro interno.

Infine, si è trattato di Clean Desk Policy, una politica che espone il corretto trattamento del materiale cartaceo e non, che si può trovare su una scrivania di un ufficio, in modo che vengano evitate fughe o perdite di informazioni riservate.

Un altro corso che è stato necessario tenere, sempre tramite piattaforma Microsoft Teams, è stato quello di *handling*[2] dei prototipi, sviluppato con l'aiuto del Prototype Manager di Motrol.

Handling[2]: Manipolazione, l'azione effettuata da chi maneggia; è lasciata espressa con il termine inglese perché non presenta un corrispettivo italiano che renda il concetto.

In questo caso, il training è stato erogato a tutti i dipendenti che trattano materiale prototipale, a partire dal personale che lavora in area prototipi, fino ad arrivare a progettisti, personale del testing, addetti alla qualità. I temi affrontati nel corso sono stati ricavati dal Prototype Protection Standard, documento adottato da alcune divisioni Magna che ho riadattato e ufficializzato anche per Motrol. Esso stabilisce i requisiti minimi per un trattamento adeguato dei prototipi relativamente a: classificazione dei progetti, security area addette a ospitare prototipi, trasporto e immagazzinamento di materiale prototipale, acquisizione di materiale video e fotografico.

Sia per quanto riguarda il corso di aggiornamento sui temi di sicurezza delle informazioni che per quello di *handling* dei prototipi, sono state collezionate le evidenze della partecipazione del personale e sono state ripetute delle sessioni dedicate agli assenti. Inoltre, la corretta comprensione dei contenuti del training prototipi è stata verificata tramite la compilazione da parte dei partecipanti di un test realizzato ad hoc. Questo è stato utile per analizzare la frequenza e la distribuzione degli errori in modo da poter individuare i punti meno chiari e spiegarli nuovamente.

4.2. Definizione di aree aziendali e procedure di accesso

Un altro importante insieme di attività portato a termine per ottenere la conformità alla norma è stato quello inerente alla definizione delle aree aziendali in relazione al livello di riservatezza delle informazioni in esse contenute e alla conseguente formalizzazione di adeguate misure di sicurezza industriale e di procedure scritte per l'accesso.

Per precisione, in Motrol, all'inizio del processo, erano già presenti aree aziendali ad ingresso limitato ai soli autorizzati tramite l'utilizzo del badge, con gestione dei diritti di accesso effettuata dalle Risorse Umane grazie ad un apposito software. Quindi, per ottenere la conformità alla norma, è stata ritenuta necessaria la procedurizzazione del processo già in atto, con l'aggiunta di alcune migliorie in ambito di comunicazione degli aventi diritto di accesso ai responsabili delle diverse aree e di controllo periodico dei tentativi di accesso. Per rendere la procedura più comprensibile, tutte le 15 zone ad accesso ristretto sono state identificate sulla pianta dello stabilimento e documentate indicando le misure tecniche, fisiche e organizzative in atto per proteggerle.

In aggiunta a ciò, seguendo le indicazioni di TISAX e di Magna stessa, si è deciso di suddividere lo stabilimento in 4 diversi tipi di zone di sicurezza e di fissarlo tramite documentazione. Come zona 1 (verde) è stata definita l'area recintata esterna allo

stabilimento, la quale comprende parcheggi e reception, con accesso possibile sia per i dipendenti che per i visitatori, dopo l'identificazione alla reception stessa. La zona 2 (gialla) è stata fatta coincidere, invece, con l'area aziendale interna, alla quale si accede dopo aver effettuato l'ingresso dalla porta principale. Tale accesso è possibile ad ogni dipendente tramite l'utilizzo del badge e ai visitatori nel caso essi siano registrati e accompagnati da un referente interno a Motrol. La zona gialla comprende la maggior parte degli uffici, l'area produttiva dello stabilimento e le aree comuni.

La zona 3 (arancione) e la zona 4 (rossa) sono proprio quelle che includono le sopra citate aree ad accesso ristretto, gestite in conformità con la procedura.

In zona 4 le risorse contenute sono ancora più critiche e confidenziali; di conseguenza, l'accesso è garantito a un numero ancora più ristretto di persone e può presentare una metodologia alternativa al badge.

4.3. Risk management e physical internal assessment

L'analisi di rischi e opportunità è un'attività cardine per qualsiasi moderno sistema di gestione. In questo, un sistema di gestione della sicurezza delle informazioni non fornisce un'eccezione. La norma TISAX ritiene che l'identificazione e la conoscenza di tutte le potenziali criticità *Information Security* sia la chiave per lo sviluppo di un sistema aziendale sicuro. La consapevolezza delle proprie possibili debolezze e dei propri punti di forza, infatti, sia per quanto riguarda la parte IT che il tema di sicurezza fisica delle informazioni, fa in modo che si implementino delle misure volte alla risoluzione delle criticità o, nell'altro caso, alla creazione di *best practice* da condividere con le altre divisioni.

Parlando di "minacce IT" ho lavorato, con l'ausilio di IT Manager e IT Specialist, alla creazione di un Risk Register aziendale a partire da un formato standardizzato Magna. Tale documento consiste in un foglio Excel suddiviso in quattro sezioni; in esse si ha: l'identificazione del rischio e delle sue possibili cause, la quantificazione della minaccia come prodotto tra impatto e probabilità di accadimento, l'elenco delle misure per la mitigazione del rischio esistenti e di quelle (se ritenuto necessario) da implementare, con indicazione relativa allo stato dell'attività, alla data prevista per il completamento e al rischio residuo (sempre calcolato come impatto x probabilità). Come output del *risk assessment* sono stati individuati 8 scenari di rischio medio che si è ritenuto di dover mitigare con altrettante proposte di implementazione di nuove misure; inoltre, si è

deciso, in ottica di miglioramento continuo, di suggerire altre 3 azioni mitigatrici per scenari a rischio basso, ma comunque ancora migliorabili.

Dal lato sicurezza fisica, invece, le criticità sono state rilevate mediante un *internal assessment* effettuato tramite ispezione delle varie zone e segnalazione da parte dei responsabili delle aree. Anche in questo caso le non conformità sono state registrate su un foglio Excel e reindirizzate ai rispettivi responsabili in modo che potessero indicare le attività che intendevano svolgere per la loro risoluzione, con data prevista di "fine lavori".

4.4. Gestione dei fornitori

Una volta migliorate le proprie prestazioni in ambito *Information Security*, l'Azienda non può ancora considerarsi conforme alla norma TISAX. Infatti, la *compliance* alla norma non dipende solo dall'Organizzazione stessa ma anche dalla sua *supply chain*. In effetti, anche se si trattano i propri dati in maniera impeccabile, si può rischiare la loro diffusione o compromissione nel caso in cui vengano condivisi con dei fornitori che non rispettano determinati requisiti di sicurezza delle informazioni.

Per questo motivo TISAX insiste molto sul tema (3 domande di controllo, delle quali 2 relative ai fornitori di servizi IT e 1 ai fornitori in generale), richiedendo in vari punti che l'Azienda che intende certificarsi valuti i propri fornitori dal punto di vista *Information Security*.

Motrol, nella sua condizione "as is" aveva già a disposizione delle misure piuttosto importanti quali l'uso di *non-disclosure agreement* (NDA) e l'utilizzo di clausole legate a requisiti IS (*Information Security*) all'interno delle Condizioni generali d'acquisto. Scendendo più nello specifico, l'NDA consiste in uno strumento legale tramite il quale il soggetto che lo emana vincola colui che lo sottoscrive, in questo caso il fornitore, a rispettare degli obblighi di riservatezza relativi alle informazioni con esso condivise.

Nelle Condizioni generali d'acquisto, invece, l'Azienda fa firmare un'articolata serie di requisiti che il fornitore dovrà rispettare durante il rapporto lavorativo; tra questi, due specifici paragrafi sono dedicati ai temi di protezione dei dati Magna e di *cyber security*.

Nonostante ciò, si è ritenuto internamente che servisse un ulteriore strumento di controllo del livello di conoscenza e comprensione dei principi IS da parte dei fornitori. Per tale motivo, ho sviluppato un documento, che riprende i più importanti requisiti

contenuti nell'ISA, e li pone sotto forma di 39 domande, in modo che il fornitore possa condividere con Motrol la propria autovalutazione in materia *Information Security*.

Le macro-tematiche trattate nel documento sono: gestione del rischio, politiche di sicurezza, *organizational security*, gestione degli *asset*, sicurezza HR (*Human Resources*), sicurezza (delle informazioni) fisica e ambientale, gestione delle comunicazioni e delle *operation*, controllo degli accessi, acquisizione, sviluppo e manutenzione di *Information Systems*, *Business Continuity* e *Disaster Recovery*. Il processo di autovalutazione è strutturato nel modo seguente: il potenziale fornitore ha il compito di rispondere alle domande di controllo (Sì, No, N/A) e di attribuirsi un punteggio da 0 a 5 sulla base di un sistema di *maturity level* identico a quello utilizzato da VDA nell'ISA; infine, ha da inserire prove di ciò che sta dichiarando o giustificazioni e commenti, a seconda che il livello raggiunto sia sufficiente (maggiore o uguale a 3) o meno. Una volta terminata la compilazione del questionario, in alto a destra compare il punteggio finale totalizzato: anche in questo caso si è preso come riferimento il metodo usato da TISAX e, di conseguenza, si ottiene un risultato positivo con uno score maggiore o uguale a 2.7.

Il "Supplier maturity questionnaire" è da considerarsi uno strumento completo: non si limita esclusivamente a misurare il livello di maturità *Information Security* del fornitore, ma lo aiuta anche a colmare i gap individuati tramite la redazione di un "Action Plan".

Il documento in questione è stato validato effettuando un invio "pilota" ad alcuni fornitori ritenuti rappresentativi da Motrol, in modo che offrissero un *feedback* utile a segnalare i suoi limiti e le sue possibilità di miglioramento. Ottenuto il modello definitivo, il questionario di maturità IS dei fornitori è stato inserito ufficialmente all'interno della procedura di approvazione dei fornitori.

Il suo campo di applicazione è stato stabilito internamente e non si espande solamente ai fornitori di servizi IT (come richiesto dalla norma), ma anche ai fornitori di materiali diretti che, per collaborare con Magna hanno bisogno che ci sia una condivisione di dati sensibili (es. disegni tecnici 2D / 3D, informazioni tecniche, informazioni commerciali).

4.5. *Compliance* IT

Da non dimenticare sono i punti IT *specific*, concentrati principalmente nei capitoli 4 e 5 del VDA ISA. Essi, infatti, trattandosi di una certificazione legata in gran parte all'*Information Technology*, sono da ritenersi degli aspetti chiave per il corretto sviluppo di un sistema di gestione della sicurezza delle informazioni.

All'interno del progetto, per la maggior parte dei casi, mi sono limitato ad interpretare i requisiti TISAX e a richiederne l'applicazione al team di specialisti IT presenti in Azienda, dedicandomi maggiormente al controllo dell'avanzamento delle attività che alla loro realizzazione operativa.

5. Situazione finale e conclusioni

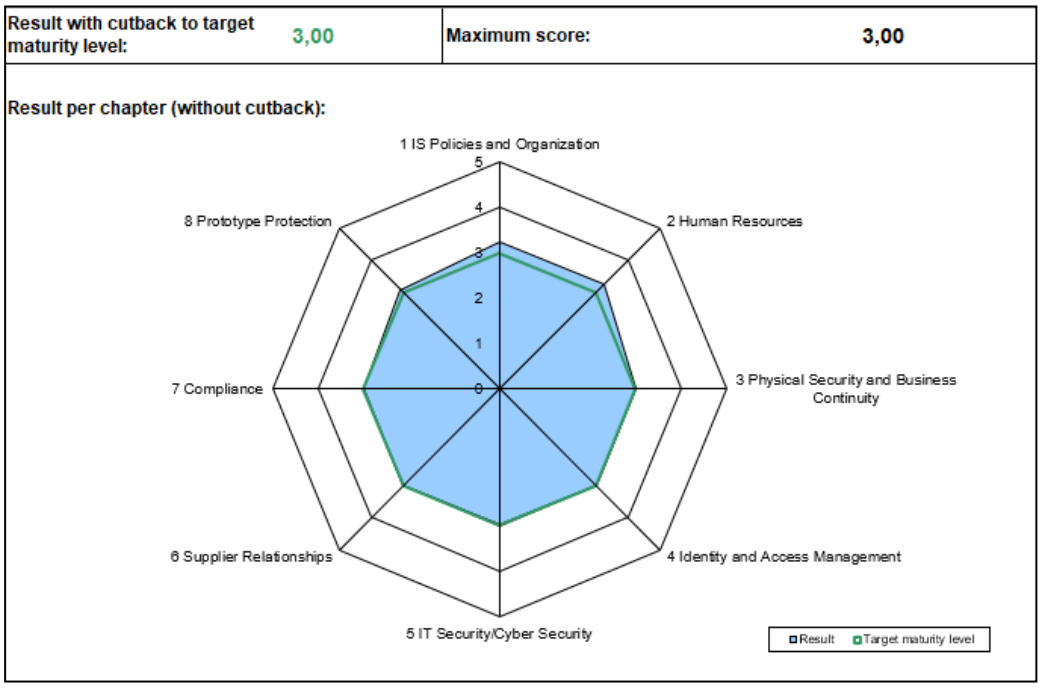

Fig.2 : Radar della condizione di Motrol a fine progetto

Al termine del lavoro descritto in questo elaborato, abbiamo raggiunto, e talvolta superato, un livello di 3.00 in tutti i punti di TISAX, come visibile dalla Fig.2.

L'obiettivo di inserire nel sistema integrato QEHS (Quality, Enviromental, Health and Safety) un sistema di gestione aziendale della sicurezza delle informazioni, destinato a diventare parte integrante dei processi Motrol, è stato raggiunto: è stata creata una base robusta di *Information Security*, a disposizione per essere regolarmente utilizzata, rivista e aggiornata, in modo da poter ottenere prestazioni ancora superiori.

Fig.3 : Elenco dei fogli contenuti nella Matrice aziendale dei documenti; gli ultimi due sono relativi a TISAX

La fase successiva che l'Azienda dovrà affrontare sarà la verifica di terza parte effettuata da un ente esterno di certificazione.