

Risk assessment in fleet management system using OCTAVE allegro

Salman Alfarisi, Nico Surantha

Department Computer Science, Binus Graduate Program-Master of Computer Science Bina Nusantara University, Jakarta, Indonesia

Article Info

Article history:

Received Apr 12, 2021

Revised Jul 2, 2021

Accepted Dec 31, 2021

Keywords:

Fleet management system
GPS Tracking
OCTAVE allegro
Risk assessment
Risk management

ABSTRACT

The purpose of this study is to use the OCTAVE allegro methodology to identify risks in fleet management system (FMS), determine prioritized risks to be mitigated, provide mitigation recommendations for these prioritized risks, and shows how effective the recommendation is. The result of this study is expected to become an input for FMS service provider of possible risks in FMS services, and risk mitigation approaches that can be used to handle those risks. This risk assessment has successfully identified 6 critical information assets, 10 risks in total, and 4 risks that need to be mitigated, followed by proposed mitigation approaches for those risks. Some of the recommendation has been applied by the company and contribute to SLA achievement of the system. The result also showed that application and simulation software provide most prominent risks in FMS service, thus securing these two will eliminate most risk in FMS service.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Nico Surantha

Department Computer Science, Binus Graduate Program-Master of Computer Science

Bina Nusantara University, Jakarta, 11480, Indonesia

Email: nico.surantha@binus.ac.id

1. INTRODUCTION

IT service companies have to maintain three important aspects of information security, namely confidentiality, integrity, and availability [1], to provide trust to their customers. One of the steps to maintain those aspect is doing IT risk assessment, as part of IT security management in a whole. In conducting an IT risk assessment, the companies must use a suitable framework to make it efficient, because they cannot prevent all identified risks, due to lack of human, time, or financial resource. A framework that is quite simple and efficient, and suitable for most companies, especially middle to low company, is OCTAVE Allegro.

Several studies have shown that OCTAVE Allegro can be adapted to various environment. Masky *et al.* [2] used it in cloud environment. Jufri *et al* [3], used OCTAVE Allegro for identifying, analyzing, evaluating, and mitigating risk information systems in the university's academic environment, then uses the ISO 27001 standard as a guide for making information security policies. Suroso and Fakhrozi [4] also use it as risk assessment framework in education institution. Ali and Awad [5] applied the Allegro OCTAVE methodology to highlight various vulnerabilities in smart homes, present risk information to homeowners, and propose approaches to reduce the risk of the smart home. He mentioned that OCTAVE Allegro is very suitable for use in smart home risk assessment because of the possibility of the existence of container assets that require both cyber and physical security. Sardjono and Cholik [6] use it in bank environment.

OCTAVE operational critical threat, asset, and vulnerability evaluation is a risk assessment methodology developed by software engineering institute (SEI), Carnegie-Mellon University. OCTAVE Allegro itself comes from the development of the OCTAVE and OCTAVE-S methods that streamline and optimize the information security risk assessment process in such a way that an organization can obtain

sufficient results with small investment in time, human resources, and other limited resources [7]. The difference of OCTAVE Allegro and other OCTAVEs is shown in Table 1.

Table 1. Difference of OCTAVE allegro and other OCTAVE [7]

OCTAVE	OCTAVE-S	OCTAVE Allegro
Intended for organization of 300 more employee	Designed for organization of 100 less employee	Designed for organization of middle to low size (300 less employee)
Need to conduct workshop by interdisciplinary analysis team from organization business units	Performed by analysis team (3 to 5 people) that have extensive knowledge of the organization. No need to conduct workshop.	Flexible, can be performed by individuals or workshop by many analysis teams of business units. It doesn't require extensive risk assessment knowledge.
Consist of 3 phases: 1) identification of important information asset, its security requirement, and its threats, 2) perform evaluation infrastructure, 3) perform risk identification activities and develop risk mitigation plan	Similar phase with OCTAVE, but require less extensive examination on organization's information infrastructure	Consists of 8 steps in the 4 phases (will be mentioned in the next page), thus provide more robust result than OCTAVE or OCTAVE-S

OCTAVE Allegro's approach differs from other methodologies by focusing primarily on aspects of information assets in the context of how these assets are used, where they are stored, transferred and processed, and how these assets are faced with threats, vulnerabilities, and disturbances [2]. This study will implement OCTAVE Allegro methodology in Fleet management system (FMS) owned and operated by PT XYZ. FMS is a system used to monitor and control the fleet use of an organization. FMS consists of several components that can be categorized into three groups, namely sensors & actuators, networks, and computing [8]. The components of each group are presented in Table 2.

Table 2. Component of FMS

CPS/IoT component	FMS component
Sensor & actuator	GPS tracker
Network	Cellular network (GSM) Intranet network
Computing	FMS application server FMS database server

GPS Tracker is a sensor that is installed on a vehicle and collects location data from GPS and vehicle condition data sent from an electrical control unit (ECU) [9]. Application servers become interfaces for both the backend and frontend, the database server stores both raw data and processed data. Cellular networks and Internet networks are used for communication between GPS tracker and application server, and between users and FMS applications.

PT XYZ is an IT service company that has been established since 2013. The company's IoT business has just started in 2018, with the release of fleet management system (FMS), sold in subscription model. In 2018, the company obtained FMS managed service contracts with 414 units of managed vehicles with a 4-year contract period and 24 units with a 3-year contract period. Regarding contracts, PT XYZ customers set a high SLA, namely 95% for GPS tracker, and 99% for FMS applications. In its development, PT XYZ's FMS service experienced several security problems that affected the availability of FMS services, such as hacker bot that delete all FMS database, data center problem that cause interruption of service for more than 1 day, and driver fraud that use wifi hotspot beam by GPS tracker, causing data limit to be exceeded thus telematics information is not sent to server. Those incidents shown in Table 3.

Table 3. Incident in FMS PT. XYZ before risk assessment

Incident description	Date of the incident	Source	Affected area	SLA (at the month of the incident)
Redis servers that are open to the Internet result in the server being taken over by bot hackers who then wipe out the entire database system	June 2018	Hacker Bot	Availability	93.429%
The power system in the data center where the FMS server is hosted is experiencing problems, which affects service availability	July 2018	Data center power failure	Availability	93.429%
The wifi hotspot feature that was originally not allowed to be used, because it consumes the data quota intended for communication between the GPS tracker and the server, used by some users, has resulted in dozens of GPS trackers being unable to send updated data.	December 2018– February 2019	User Fraud	Availability	90.1435%
Emulator software that accidentally updated production data (known internally)	July 2020	Emulator Software	Data Integrity	(Not affecting SLA)

Risk assessment in fleet management system using OCTAVE allegro (Salman Alfari)

Risk assessment in FMS, whose output is a mitigation recommendation on prioritized risks, is needed to ensure that risks in FMS can be identified, classified, mitigated in accordance with company conditions, and can increase its SLA. This research result may become a reference for FMS service providers of common risk in FMS, and how to mitigate them.

2. RESEARCH METHOD

The sole methodology used in this research is OCTAVE Allegro, while the data used for the research is get from interview to stakeholders (IT manager & staffs, finance staff) and observation. Risk assessment using OCTAVE Allegro consists of 8 stages grouped in 3 phases: preparation, threat identification, and risk identification and mitigation. Preparation for risk assessment consist of the 3 steps: i) establishment of risk measurement criteria, ii) development of information asset profile, and iii) identification of information asset containers. In step 1, a series of qualitative measures (risk measurement criteria) are defined. They will be used to evaluate the impact of a risk to the mission and objectives of FMS. OCTAVE Allegro mention 5 example areas that need to be considered, namely i) customer reputation and trust, ii) financial, iii) productivity, iv) health and safety, v) fines and legal sanctions. User of OCTAVE Allegro can also define their own impact area based on their condition. OCTAVE Allegro worksheet 1 can be used to help define the criteria, and worksheet 7 for putting priority ranking of the criterias. In step 2, information asset profile is developed. These are information assets that need to be protected by the company. OCTAVE Allegro worksheet 8 can be used to define the information asset. In step 3, information asset containers are identified. It is the place or media where FMS information assets are stored, processed, or transferred. Container is divided into three (3) categories, i) technical, namely hardware and software of FMS services and those related to FMS services; ii) physical, i.e, physical location, application or document used in FMS services and related to FMS services; and iii) humans, namely anyone who knows and has access to important FMS service assets and those related to FMS services [10]. OCTAVE Allegro worksheet 9 can be used to help define the container.

The next step is threat identification. It can be identified by analyzing area of concern for each information asset, which is described by identifying the potential actors, means, and motives of the actors. Furthermore, the consequences of this incident were also described. The identification of areas of concern and threats can be put in a separate table. After the threat is identified, the probability of the event and what aspects are affected by the incident area are taken into account. This calculation is made into a score called the relative risk score. OCTAVE Allegro worksheet 10 can help identify threats and risks as described above. Additional step for preparation is the creation of risk pool. It is the reference to help decide which risks need to be mitigated and which can be ignored. The risk pool assigns risk based on the relative risk score and the probability of its occurrence. The higher the relative risk score and the probability of its occurrence, the more recommended the risk is for mitigation. The risk pool for this research is shown in Table 4.

Table 4. Risk pool

Relative risk matrix				Remarks
Probability	Risk score			
	25-36	13-24	0-12	
High	POOL 1	POOL 2	POOL 2	POOL 1=Mitigate
Medium	POOL 2	POOL 2	POOL 3	POOL 2 & 3=Mitigate or hold
Low	POOL 3	POOL 3	POOL 4	POOL 4=Accept

3. RESULTS AND DISCUSSION

3.1. Risk measurement criteria

This study only took into account 3 aspect in risk measurement criteria: i) reputation and customer confidence, ii) financial, and iii) productivity. The aspects of health & safety and fines & legal penalties were ignored, because their impact was not significant in FMS. Reputation and customer confidence are the top priority for PT XYZ's FMS services [11], because as a relatively new company in the FMS service business, damage to reputation and trust can have a huge impact on other aspects, namely finance due to loss of customers, and especially business continuity in the future. This is also driven by the tight competition factor in the FMS service business with the presence of companies that have been in business for a long time, with greater resources. The productivity aspect is quite important because if there is a disruption in the system, the employee productivity will decrease as well. Safety and health are ignored because in the FMS services provided by PT XYZ to customers, there are no factors that directly affect the safety and health of customers or FMS service providers. The FMS system component that is in direct contact with the customer, namely the

OBD GPS Tracker [12], is connected directly to the OBD port on the vehicle, without making changes to the electrical system in the vehicle. In addition, there are no additional sensors such as fuel tank sensors, tire sensors, or actuators to remotely shutdown the engine, which come into direct contact with sensitive components on the vehicle, that pose a risk to customer health and safety. The aspects of fines and legal sanctions are also ignored. There is relationship with the legal system, for example license of a GPS Tracker that must be obtained from the director general of post and telecommunication, ministry of communication & information (Dirjen Postel, Kemenkominfo), where if it doesn't comply, could result in considerable consequences, such as instruction for removing the GPS tracker, that will significantly affect reputation, productivity and financial aspects. However, this is outside the discussion of this study which emphasizes the aspects of information assets. The criteria obtained to be a reference in measuring risk are shown in Table 5.

Table 5. Priority of impact area

Priority value (measure)	Impact area
3 (5)	Reputation and customer confidence
2 (4)	Financial
1 (3)	Productivity

3.2. Information asset profile

There are 8 important information assets in FMS services, stated in Table 6. FMS administrator username/password is used to activate GPS Tracker, system configuration, and create operator and end-user level username/password in the FMS application. If the admin username/password is changed or taken over by another party without the knowledge of the authorities, this can result in data leakage, changes in application configuration, or loss of important information in the application which can harm PT XYZ in the aspect of reputation and financial. This applies to the database root user which is used to CRUD (create, update, delete) all tables in the database [13] and grants privileges to the user to CRUD certain database tables, where all FMS data is stored. The GPS tracker landing page username/password is used to access the GPS tracker setup page via the wifi hotspot generated from the GPS tracker itself. If an unauthorized user finds out the username/password of the GPS tracker landing page [14], he can change the GPS tracker configuration such as the destination server, so that the FMS software cannot detect this GPS tracker. The GPS tracker secret key is used as a key for remote configuration of the GPS tracker using SMS. If the secret key is found by an unauthorized party, then it can change the GPS tracker configuration. There are several GPS tracker software tools, namely the PC Tool, which is used for local configuration, an emulator that emulates GPS tracker data, and an ECU emulator [15] that emulates ECU data to be captured by the GPS tracker. If this tool is used by an unauthorized party, then it will be able to change the GPS tracker configuration and emulate the GPS tracker data into the FMS software, so that the data obtained is invalid. Telematics data [16] is the GPS coordinate and vehicle condition data captured by the GPS tracker and sent to the Telematics software, which processes the data into relevant information in the FMS application. This information is stored for a period of up to 1 year or according to the agreement between FMS provider and the customer. Telematics data is important information that underlies the FMS. The loss or change of this information without the knowledge of the authorities may result in losses, both in reputation and financial aspect. This applies to vehicle management data which contains information about the owner's username/password and detailed vehicle information, such as police numbers, taxes, maintenance and repair history, and contracts related to the vehicle (for corporate customers). Confidential system and service documentation consists of sensitive documentation related to software structures, databases, admin manuals, penetration testing results, customer contracts. System documentation and services are confidential, that if they are accessed by party with malicious intent, it can use it to destruct FMS and harm the company morally and financially.

Table 6. FMS information asset profile

Asset ID	Critical information asset	Owners
A1	Administrator username/password of FMS application	FMS software administrator
A2	Root password of database server	FMS software administrator
A3	GPS Tracker landing page username/password	FMS hardware administrator
A4	Secret key of GPS Tracker	FMS hardware administrator
A5	GPS tracker tool software (PC tool for configuring GPS tracker, GPS tracker emulator to emulate GPS tracker data in FMS software, ECU emulator to emulate ECU)	FMS hardware administrator
A6	Telematics data	All FMS administrator
A7	Vehicle management data	FMS software administrator
A8	Confidential documentation regarding systems and services (e.g., software documentation, database structure documentation, penetration testing results documentation, API documentation, contract documentation.)	All FMS administrator

3.3. Identified area of concern & threat

The area of concern is mapped based on the similarities of the actors, method and motives. Of the 8 information assets, there are 6 areas of concern, described in Table 7.

Table 7. Identified area of concern

Area of concern	ID of area of concern	Aset ID	Information asset name
Unauthorized person knows the application admin username/password, so he can log into the application with the highest access rights	C1	A1	Administrator username/password of FMS application
Unauthorized person knows the root database username/password, so he can log into the database with the highest access rights	C1	A2	Root password of database server
Unauthorized person knows the GPS tracker landing page username/password so he can change the GPS tracker configuration	C1	A3	GPS tracker landing page username/password
The unauthorized person knows the secret key of the GPS tracker so that he or she can remotely configure the GPS tracker	C2	A4	Secret key of GPS tracker
GPS tracker software is used by unauthorized persons, so that telematics data can be manipulated irresponsibly.	C3	A5	GPS tracker tool software (PC tool for configuring GPS tracker, GPS tracker emulator to emulate GPS tracker data in FMS software, ECU emulator to emulate ECU
The vehicle is not tracked by the system which is caused by not receiving telematics data from the GPS tracker	C4	A6	Telematics data
Telematics data and vehicle management cannot be accessed by users because the application does not work	C5	A7	Vehicle management data
Confidential documentation regarding FMS systems and services can be accessed and modified by unauthorized persons	C6	A8	Confidential documentation regarding systems and services (e.g., software documentation, database structure documentation, penetration testing results documentation, API documentation, contract documentation.)

Disclosure of FMS administrator username/password, database root password, and GPS tracker landing page username/password are categorized into one area of concern, because they have similarities in perpetrators, methods, and motives, namely the authorized person, by performing hacking tricks takes over the highest level of user of the application/database to gain certain advantages. Every GPS tracker has a default secret key, which is the last 6 digits of the GPS tracker serial number. This secret key can be changed using SMS or PC Tool, or given protection by limit only certain MSISDN number that can change the configuration. However, if the change not done or the protection is disabled, and the GPS tracker serial number is known to those with malicious intentions, then they can change the GPS tracker configuration using the default secret key. GPS tracker software (GPS tracker emulator, PC tool, ECU emulator) can be useful for development, but on the other hand can also harm data integrity because it can alter production data, which can harm reputation and customer confidence on the FMS. Telematics data is gathered from GPS tracker. If it or the SIM card is broken, then it will not be able to send data to server, thus telematics data is not available as well. Unavailability of the FMS application, due to server problem or attack, causing user unable to input data to the server, and causing vehicle management data will not be available as well. Confidential documents, such as those contain penetration test result, database structure, API documentation, is very harmful if they fall to those with malicious intent, because they enable them to access the system and change the configuration easily.

The area of concern above is then explained in more detail with the threat scenario, explained in Table 8. One area of concern can have several threat scenarios. As in C1, the area of concern for application assets, databases, and landing pages, threats can come from weak password policies [17] on the system (T1), lack of administrator awareness regarding information security (T2), and hacking tricks performed on the system (T3). While in C2, the area of concern for secret keys, attackers can take advantage of policies related to secret keys that are still weak (T4), meaning that there is no policy that requires changing the secret key or limiting the MSISDN number which can be configured via SMS. In C3, an area of concern for software tools, misuse of emulator software on production data is a threat to the integrity of FMS data (T5). In C4, fraud by drivers (T6 & T7) or damage to the GPS Tracker and SIM Card (T8) can disrupt the availability of telematics data. In C5, the external attacker can do defacement [18] or DDoS [19] on the FMS so that the website cannot be accessed, causing data to not be inputted (T9). In C6, external attackers perform hacking

techniques such as sniffing [20] to steal confidential documents related to FMS (T10). Based on identified threat and existing countermeasure, it can be determined what risks exist in FMS, and at what probability those risks will occur and create significant impact to the business.

Table 8. Identified threat to FMS

ID of area of concern	ID of threat	Threat scenario
C1	T1	External attackers exploiting weak password policies in FMS applications, databases, and landing pages to log into the system
	T2	External attackers take advantage of the weak security awareness of FMS administrators to successfully obtain username/password and log into the system
	T3	Attackers take advantage of the weak communication channels used by FMS Administrator personnel, by sniffing traffic, because the FMS application has not implemented the SSL method.
C2	T4	Exploitation of the policy regarding secret key GPS Tracker
C3	T5	Emulator software that should be used only for development assistance is used to manipulate production data on the telematics platform
C4	T6	Drivers or thieves who release the GPS Tracker from the vehicle so that they are not tracked, because they want to do something illegal or does not comply with the policy
	T7	Drivers who use wifi hotspot from GPS Tracker until the data package runs out, so that telematics data cannot be sent to the server
C5	T8	Damage to the GPS Tracker so that telematics data is not sent to the server
	T9	External attackers perform hacking techniques, such as website defacement and DDoS against the FMS system
C6	T10	An external attacker sniffs traffic to access files containing confidential documentation

3.4. Identified risk

Risk in [21] can be imagined as a threat that becomes a reality due to system vulnerabilities that have not been covered, whose probability is measured based on an estimate of the motives, means, consequences, and weaknesses of the system itself. The stronger the motive, the easier to attack due to the vulnerability of the system, and the greater the advantage the attacker gets, the greater the likelihood of it happening and vice versa. Table 9 in appendix describes the risks in FMS, existing conditions at PT XYZ FMS, and the risk probability based on a description of the risks and existing conditions. Sign (-) describes conditions that weaken the system, while sign (+) describes conditions that prevent risks.

3.5. Risk analysis

The identified risks are analyzed based on their impact on area defined in the Risk Measurement Criteria, resulting in a relative risk score. The calculation of the risk score is shown in Table 10. The risks R1, R2, R3 which result in the loss of administrator access to the system, hackers who enter the system and ask for a number of ransoms or execute malicious programs, have a high impact on reputation and financial aspects, and have a medium impact on productivity. Its relative risk score is 33. The risk R4 which results in loss of telematics data resulting in lowering SLA has a medium impact on aspects of reputation, finance, and productivity. Its the relative risk score is 24. Risk R5 which has consequences on the integrity of telematics data is damaged because the data does not come from the GPS tracker but from emulator, has a high impact on reputation, medium on finances, and low on productivity. Its relative risk score is 26. The risk R6 resulting in loss of GPS tracker or telematics data becoming unavailable has a medium impact on reputation, finances, and low on productivity. Its relative risk score is 21. The risk R7 which has consequences for telematics data is not available because internet data runs out has a low impact on reputation and productivity, and medium on finance. Its relative risk score is 16. The Risk R8 which results in the unavailability of telematics data has a medium impact on reputation and financial, and low on productivity, and the relative risk score is 21. The risk R9 which has consequences on reputation and system inaccessibility has a high impact on reputation and productivity, and medium on finance, and the relative risk score is 32. The risk R10 which has the consequence of tampering with data on the system has a high impact on reputation and productivity, and medium on finances, and the relative risk score is 32.

The risk is then put on action matrix (Table 3), that calculate the probability of risk occurrence and the relative risk score to gain recommended action. Based on action matrix, recommendations for action are shown in Table 11. One risk is accepted, namely R7 (the risk of drivers using the wifi hotspot from the GPS tracker until the data package runs out, so that telematics data cannot be sent to the server), due to preventive action already carried out by PT XYZ, so that the impact of these risks is small to the business. There are also five risks that need to be addressed, but they are not yet a priority because the probability of their occurrence is low or medium, namely R4, R6, R8, R9, and R10. Mitigation is prioritized on four risks, namely R1, R2, R3 (related to securing the FMS application and database), and R5 (securing the GPS tracker emulation tool).

Table 10. Relative risk score

Consequences		Severity		
R1, R2, R3				
<ul style="list-style-type: none">- The FMS/database/IT administrator loses access to the FMS/database server/landing page application- The attacker gains access to the main system of the FMS /database server/landing page application, and demands a fee- The attacker is executing an unauthorized/unwanted program	Impact area	Measure	Score	
	Reputation & customer confidence (5)	High (3)	15	
	Financial (4)	High (3)	12	
	Productivity (3)	Medium (2)	6	
Relative risk score				33
R4				
<ul style="list-style-type: none">- The attacker changed the configuration of the GPS tracker which resulted in illegible telematics data. This can lower SLAs and customer confidence levels.	Impact area	Measure	Score	
	Reputation & customer confidence (5)	Medium (2)	10	
	Financial (4)	Medium (2)	8	
	Productivity (3)	Medium (2)	6	
Relative risk score				24
R5				
<ul style="list-style-type: none">- Telematics data becomes invalid because it does not come from the GPS tracker but from the emulator software.	Impact area	Measure	Score	
	Reputation & customer confidence (5)	High (3)	15	
	Financial (4)	Medium (2)	8	
	Productivity (3)	Low (1)	3	
Relative risk score				26
R6				
<ul style="list-style-type: none">- Telematics data becomes unavailable- Financial loss if the GPS tracker is lost	Impact area	Measure	Score	
	Reputation & customer confidence (5)	Medium (2)	10	
	Financial (4)	Medium (2)	8	
	Productivity (3)	Low (1)	3	
Relative risk score				21
R7				
Consequences	Severity			
<ul style="list-style-type: none">- The Internet data runs out so that telematics data is not available	Impact area	Measure	Score	
	Reputation & customer confidence (5)	Low (1)	5	
	Financial (4)	Medium (2)	8	
	Productivity (3)	Low (1)	3	
Relative risk score				16
R8				
<ul style="list-style-type: none">- Telematics data becomes unavailable	Impact area	Measure	Score	
	Reputation & customer confidence (5)	Medium (2)	10	
	Financial (4)	Medium (2)	8	
	Productivity (3)	Low (1)	3	
Relative risk score				21
R9				
<ul style="list-style-type: none">- Website defacement can reduce customer confidence, and access to all telematics data becomes unavailable	Impact area	Measure	Score	
	Reputation & customer confidence (5)	High (3)	15	
	Financial (4)	Medium (2)	8	
	Productivity (3)	High (3)	9	
Relative risk score				32
R10				
<ul style="list-style-type: none">• Leaking confidential documents containing sensitive information such as username/password can cause unauthorized access by the attacker, which can destroy data on the platform	Impact area	Measure	Score	
	Reputation & customer confidence (5)	High (3)	15	
	Financial (4)	Medium (2)	8	
	Productivity (3)	High (3)	9	
Relative risk score				32

Table 11. Recommended actions against risk in FMS PT XYZ

Risk ID	Probability	Relative risk score	Pool (recommended action)
R1	High	33	POOL 1 (Mitigate)
R2	Medium	33	POOL 2 (Mitigate)
R3	Medium	33	POOL 2 (Mitigate)
R4	Medium	24	POOL 2 (Hold)
R5	Medium	26	POOL 2 (Mitigate)
R6	Medium	21	POOL 3 (Hold)
R7	Low	16	POOL 2 (Accept)
R8	Medium	21	POOL 2 (Hold)
R9	Low	32	POOL 2 (Hold)
R10	Medium	32	POOL 2 (Hold)

3.6. Risk mitigation recommendation

Based on recommended action for identified risk, there are 4 risks that need to be mitigated. The proposed mitigation approaches for those risk is stated in Table 12. There are 2 proposed risk handling

approaches, tactical and strategic methods. The tactical approach addresses these risks in the short term and the required effort is minimum, while the strategic approach is for long-term needs and the effort required is quite large.

Table 12. Mitigation recommendation

Risk ID	Mitigation approach
R1, R2, R3 (FMS application and database security)	Tactical handling: 1) Run policies regarding system passwords <ul style="list-style-type: none"> - Change the default password when logging in for the first time - Change password every month - Create password complexity standards 2) Add an SSL security system in the application (implement HTTPS) so that data from application users is encrypted. 3) Restrict database access, i.e., database (root user) cannot be accessed directly via the Internet Strategic handling: 1) Implement PAM (privileged access management) technology to manage and monitor the activities of admin/root level users 2) Perform a vulnerability assessment (penetration test) periodically (at least once every 6 months), or incidentally (in the event of an attack or interference) to find out new "holes" in the application, and do patches to "patch" those holes. 3) Provide security awareness training to FMS application administrators
R5 (emulator software used to manipulate production data)	Tactical handling: 1) Analyze the emulator's header or packet signature. Differentiate with the packet header or signature from a real hardware/GPS tracker. Create a filter on the FMS server firewall. 2) Limit the distribution of emulator software among internals. Strategic handling: 1) Periodically run data scans and reports to verify data integrity and detect anomalies.

For the risks R1, R2, and R3 that are related to passwords on the system, the tactical mitigation proposed is; i) implementing policies related to password security [14] that are commonly applied in IT systems, ii) adding SSL features to web applications [22], iii) limiting database access. Meanwhile, the proposed strategic mitigation is; i) implementing privileged account management [23], [24] in the system, ii) scheduling a security assessment on the system periodically, iii) providing training and campaign on security awareness [25] to personnel handling FMS. For risk R5 that is related to emulator software, the proposed tactical mitigation is; i) analyzing the packet header from the emulator to differentiate it from the packet header from the GPS tracker, then creating a filter on the FMS firewall, and ii) making policies to limit the circulation of emulator software in the internal environment. Meanwhile, the strategic mitigation proposed is running data scans and periodic reports to verify data integrity.

3.7. Risk mitigation result

The assessment drove some system hardening and release of new standard operating procedure (SOP) in FMS, shown in Table 13 and 14.

Table 13. System hardening

No.	System hardening	Remark
1	SSL installation (changing HTTP to HTTPS)	
2	Continuous Vulnerability Assessment	Using aptrana vulnerability scanner
3	Closure of SSH access to the server, except from jumphost (bastion host)	
4	Automatic change of password	Using the ansible (ansibel vault)

Table 14. New SOPs

No.	SOP
1	SOP password policy
2	SOP access limit
3	SOP vulnerability assessment
4	SOP distribution of development software

As seen from Tables 13 and 14, not all recommendation from OCTAVE Allegro implemented in FMS PT. XYZ, due to management consideration on cost and technical dependency. Only SSL, vulnerability assessment, bastion host, and automatic password change that are implemented in the system. The standard operating procedure (SOP) that are released following the recommendation are SOP for password policy, access limit, vulnerability assessment, and distribution of development software (emulator). The result of the

change is no more cases of information security breaches were recorded on the FMS. In addition, the SLA for services for 6 months after the mitigation was implemented is achieved, although not 100% but varied between 99.5-99.9%, due to damage to the SIM card and GPS tracker, as shown in Table 15. There is no application problem that contributes to the decrease of SLA.

Table 15. SLA in 6 months after mitigation (started in August 2020)

Month	SLA	Incident
1	99.5%	Fault of SIM card and/or GPS tracker
2	99%	Fault of SIM card and/or GPS tracker
3	99.5%	Fault of SIM card and/or GPS tracker
4	99%	Fault of SIM card and/or GPS tracker
5	99.5%	Fault of SIM card and/or GPS tracker
6	99.5%	Fault of SIM card and/or GPS tracker

4. CONCLUSION

There are several conclusions of this study. First, OCTAVE Allegro can be used as a risk measurement methodology in FMS. This can be seen from the success of this methodology in identifying priority risks in FMS. Second, this study has identified 10 risks in 6 information assets, which after the calculation has reduced them to 4 risks that require immediate prevention, 5 risks that can be deferred, and 1 risk that can be accepted. Mitigation recommendations for 4 risks that require prevention are also given. This research also shows that the most vulnerable container of FMS are applications and emulator software that can manipulate data, that if not handled can reduce the reputation and trust of customers, as well as be financially detrimental, thus the handling of these two aspects is mandatory, and it is necessary to carry out continuous prevention by conducting periodic vulnerability assessments and continuous analysis for data integrity. The assessment drove system hardening and release of SOPs that contribute to SLA achievement of the system.

This research takes a case study of FMS services in a small company, with a GPS tracker of less than 1000 units, and the complexity of service features is not too high, for example the features offered only include location tracking and driving behavior analysis, in addition to features such as vehicle administration management, and the only sensor installed on the vehicle is the GPS tracker itself. In the future, risk assessment can also be carried out in a larger FMS, with more complex features and more sensors, as well as riskier, such as an FMS that has a remote shutdown feature, a camera sensor for driver condition analysis, RFID for driver attendance, FMS that uses voice command, to see what risks are contained therein, and whether OCTAVE Allegro is also effective and efficient to use as a methodology.

ACKNOWLEDGEMENTS

This research publication is supported by Bina Nusantara University.

APPENDIX

Table 9. Identified risk and occurrence probability

Risk ID	Risk description	System existing condition	Risk probability
R1	External attackers successfully exploited a weak password policy to log into the system and make configuration changes	- There is no adequate password policy in FMS PT XYZ - There are many bots on the Internet that exploit weaknesses in passwords, especially the default passwords that are entered in the password dictionary	High
R2	External attackers managed to take advantage of the weak security awareness of personnel holding the Admin / root username/password to log into the system and make configuration changes	- PT XYZ FMS administrators have not received adequate security awareness training + The financial aspects of cracking FMS application passwords may not be very attractive for someone to make social engineering efforts.	Medium
R3	External attackers are successful in exploiting the weakness of the communication channel by sniffing traffic	- The FMS application has not implemented the SSL security method + The financial aspects of FMS application password cracking may not be that attractive for someone to attempt sniffing traffic.	Medium
R4	An external attacker has successfully exploited a weak secret key security policy so that he can remotely change the GPS Tracker configuration via SMS	- There is no policy or SOP that requires changing the default secret key and remote configuration protection. + The financial aspects of a GPS tracker secret key breach may not be very attractive to someone trying to look for it.	Medium

Table 9. Identified risk and occurrence probability (*continue*)

Risk ID	Risk description	System existing condition	Risk probability
R5	Emulator software that should be used only for development assistance is used to manipulate production data on the telematics platform	- There is no policy to limit the usage of software that is prone to abuse such as emulators. + Emulator software is currently not widely distributed, even by the principal himself.	Medium
R6	The driver or thief managed to remove the GPS Tracker from the OBD port so that the vehicle was not tracked	- GPS Tracker is not equipped with an external battery so there is no alarm when it is unplugged + GPS Tracker has been installed in a hidden place	Medium
R7	The driver uses the wifi hotspot from the GPS Tracker until the data packet runs out, so that telematics data cannot be sent to the server	+ The Wifi Hotspot feature of the GPS Tracker has been turned off, and most SIM cards have been protected from being used for Internet access	Low
R8	Damage to the GPS Tracker and SIM card, so information is not sent to the server	- GPS Tracker and backup SIM Card have not been provided at the nearest location - SIM Card has low resistance against heat on the vehicle + Hardware has a fairly good resistance, and is placed in a location that is not too extreme in the vehicle	Medium
R9	External attackers have successfully carried out hacking techniques, such as website defacement and DDoS against the FMS system, so that the FMS application cannot be accessed by users and administrators	+ There is an open source WAF that protects the FMS application + The FMS application is hosted on a cloud server that already has antiDDoS	Low
R10	The external attacker was able to successfully sniff the traffic to access files containing classified documentation	+ The financial aspects of stealing confidential documents may not be very attractive to someone to make an effort to sniff traffic. + Attempts can be made not to explicitly mention sensitive content such as username/password in documents - There is no SOP or policy regarding the storage of confidential documents, that would allow administrators to, without the intention of divulging secrets, share confidential files with unauthorized parties.	Medium





REFERENCES

- [1] R. V. Solms and J. V. Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97-102, 2013, doi: 10.1016/j.cose.2013.04.004.
- [2] M. Masky, S. S. Young and T. Choe, "A Novel Risk Identification Framework for Cloud Computing Security," 2nd *International Conference on Information Science and Security (ICISS)*, 2015, pp. 1-4, doi: 10.1109/ICISSEC.2015.7370967.
- [3] M. T. Jufri, M. Hendayun and T. Suharto, "Risk-assessment based academic information System security policy using octave Allegro and ISO 27002," *Second International Conference on Informatics and Computing (ICIC)*, 2017, pp. 1-6, doi: 10.1109/IAC.2017.8280541.
- [4] J. S. Suroso and M. A. Fakhrozi, "Assessment of information system risk management with octave allegro at education institution," *Procedia Computer Science*, vol. 135, pp. 202-213, 2018, doi: 10.1016/j.procs.2018.08.167.
- [5] B. Ali and A. Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," *Sensors*, vol. 18, no. 3, pp. 1-17, 2018, doi: 10.3390/s18030817.
- [6] W. Sardjono and M. I. Cholik, "Information Systems Risk Analysis Using Octave Allegro Method Based at Deutsche Bank," *International Conference on Information Management and Technology (ICIMTech)*, 2018, pp. 38-42, doi: 10.1109/ICIMTech.2018.8528108.
- [7] C. A. Richard, J. F. Stevens, L. R. Young and W. R. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," *Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst.*, 2007.
- [8] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui and K. P. Chow, "Security Issues and Challenges for Cyber Physical System," *IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*, 2010, pp. 733-738, doi: 10.1109/GreenCom-CPSCom.2010.36.
- [9] D. Yuniar, L. Djakfar, A. Wicaksono and A. Efendi, "Truck driver behavior and travel time effectiveness using smart GPS," *Civil Engineering Journal*, vol. 6 no. 4, pp.724-732, 2020, doi: 10.28991/cej-2020-03091504.
- [10] M. Evans, Y. He, L. Maglaras, and H. Janicke, "HEART-IS: A Novel Technique for Evaluating Human Error-related Information Security Incidents," *Computers & Security*, vol. 80, pp. 74-89, 2019, doi: 10.1016/j.cose.2018.09.002.
- [11] G. Davis and L. Miles, "Reputation management: theory versus practice," *Corporate reputation review*, vol. 2, no. 1, pp 16-27, 1998.
- [12] R. Malekian, N. R. Moloisane, L. Nair, B. T. Maharaj and U. A. K. Chude-Onkonkwo, "Design and Implementation of a Wireless OBD II Fleet Management System," *IEEE Sensors Journal*, vol. 17, no. 4, pp. 1154-1164, 2017, doi: 10.1109/JSEN.2016.2631542.
- [13] I. Zoratti, "MYSQL Security Best Practices," *IET Conference on Crime and Security*, 2006, pp. 183-198.
- [14] D. Silver, S. Jana and D. Boneh, "Password managers: Attacks and defenses," *23rd {USENIX} Security Symposium ({USENIX} Security)*, 2014, vol. 14, pp. 449-464.
- [15] O. Alvear, C. T. Calafate, J. Cano and P. Manzoni, "Validation of a vehicle emulation platform supporting OBD-II communications," *12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, 2015, pp. 880-885, doi: 10.1109/CCNC.2015.7158092.
- [16] S. Duri, J. Elliott, M. Guteser, X. Liu, P. Morkowitz, R. Perez, M. Singh and J. M. Tang, "Data Protection and Data Sharing in Telematics," *Mobile Networks and Applications* vol. 9, 693-701, 2004, doi: 10.1023/B:MONE.0000042507.74516.00.





- [17] V. Taneski, M. Hericko and B. Brumen, "Systematic overview of password security problems," *Acta Polytechnica Hungarica*, 2019, vol 16, no. 3.
- [18] C. J. Howell, G. W. Burruss, D. Maimon and S. Sahani, "Website defacement and routine activities: Considering the importance of hackers' valuations of potential targets," *Journal of Crime and Justice*, vol. 42, no. 5, pp. 536-550, 2019, doi: 10.1080/0735648X.2019.1691859.
- [19] K. Costantinos, G. Kambourakis and A. Stavrou, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80-84, 2017, doi: 10.1109/MC.2017.201.
- [20] D. Glăvan, R. Ciprian, M. Radu and S. Eftimie. "Sniffing attacks on computer networks," *Scientific Bulletin "Mircea cel Batran" Naval Academy*, vol. 23, no. 1, pp. 202-207, 2020, doi: 10.21279/1454-864X-20-11-027.
- [21] A. Samimi, "Risk Management in Information Technology," *Progress in Chemical and Biochemical Research* 3, no. 2, pp. 130-134, 2020, doi: 10.33945/SAMI/PCBR.2020.2.6.
- [22] I. Dolnák and J. Litvik, "Introduction to HTTP security headers and implementation of HTTP strict transport security (HSTS) header for HTTPS enforcing," *15th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, 2017, pp. 1-4, doi: 10.1109/ICETA.2017.8102478.
- [23] J. Banoczi, H. Perper and S. Prince, "[Project Description] Privileged Account Management: Securing Privileged Accounts for the Financial Services Sector (Draft)," *National Institute of Standards and Technology*, 2017.
- [24] M. J. Haber, "Privileged Account Management Implementation," *Privileged Attack Vectors*, 2020, pp. 335-359, doi: 10.1007/978-1-4842-5914-6_25.
- [25] A. Carella, M. Kotsoev and T. M. Truta, "Impact of security awareness training on phishing click-through rates," *IEEE International Conference on Big Data (Big Data)*, 2017, pp. 4458-4466, doi: 10.1109/BigData.2017.8258485.

BIOGRAPHIES OF AUTHORS



Salman Alfarisi     is currently IT development manager at one of IT Service Provider in Jakarta, Indonesia. He has 10+ years career on network engineering and product development. He loves IT and passionate on digital transformation on many sectors in Indonesia, such as agriculture, aquaculture, and mining, and believe that IT can enhance productivity and further increase economical benefit of those sectors. He can be contacted at email: hi.salman.alfarisi@gmail.com.



Nico Surantha     received his B. Eng (2007) and M. Eng. (2009) from Institut Teknologi Bandung, Indonesia. He received his Ph.D. degree from Kyushu Institute of Technology, Japan, in 2013. Currently, he serves as an assistant professor in Computer Science Department, Binus Graduate Program, Bina Nusantara University. His research interest includes wireless communication, health monitoring, network design, digital signal processing, system on chip design, and machine learning. He is an IEEE member. He can be contacted at email: nico.surantha@binus.ac.id.