Independent Commission Against Corruption

Statement in the matter of Operation Gerda

Name: Paul CHONG Kai Yew

Title: President & Group Chief Executive Officer of Certis CISCO Security Pte Ltd ("Certis") and Chairman, Certis Security Australia Pty Ltd

Place: Singapore

Date: 3 May 2019

==

A. Experience and qualifications

1. I, Paul Chong, am the President and Group Chief Executive Officer of Certis CISCO Security Pte Ltd ("**Certis**"). I am also an Executive Director of Certis and the Chairman of Certis Security Australia Pty Ltd ("**Certis Australia**").

2. I started my career in the Singapore Armed Forces ("**SAF**") and last held the post of Head of Joint Communications & Electronics ("**HJCE**"). As HJCE, I was the most senior SAF officer responsible for designing, building, operating and protecting the SAF's critical computers and communication systems against adversaries.

3. I left the SAF to join the largest telecommunications company in Singapore, where I rolled out the world's first nationwide broadband network in Singapore.

4. I attended Cambridge University (UK) in 1982 on a SAF Overseas Scholarship, graduating with Honours in Economics and Operations Research. I am also a graduate of the US Army Command & Staff College.

5. I joined Certis in 2004 when it was restructured from a statutory board under Singapore's Ministry of Home Affairs into a private entity wholly owned by Temasek Holdings Pte Ltd.

B. Introduction to Certis and SNP

6. Certis Australia acquired Sydney Night Patrol & Inquiry Pty Ltd ("**SNP**") in April 2018. Certis Australia is a wholly owned subsidiary of Certis.

7. In 2016-2017, SNP had approximately 2,200 employees and over 1,700 clients nationally. Since that time, SNP has increased the number of its employees and clients, including securing

Signature of witness

Laura Low Shuek Lin

Signature of deponent

contracts for the provision of security services at a number of key security sites, including Adelaide Airport.

8. Headquartered in Singapore, Certis commenced operations in 1958 as the Guard and Escort Unit under the Police Force, and became a statutory board known as "The Commercial & Industrial Security Corporation" ("**CISCO**") thereafter. It was later restructured in June 2005 and incorporated as a corporate entity.

9. Certis has established itself as the leading physical security provider in Singapore. It provides security services to key government and private installations, and is an important player in Singapore's cash processing and secure logistics ecosystem.

10. Since its restructure in 2005, Certis has increased the range of security services it provides to include security manpower, enforcement, security consulting and training, security technology, outsourced manpower and IT security and information management.

11. Today, Certis is a leading advanced integrated security organisation that develops and delivers multi-disciplinary security and integrated services, with more than 34,000 staff and an international presence that extends to Australia, Singapore, Hong Kong, Macau, China, Malaysia and the Middle East.

12. As a member of the global security community, Certis has been admitted into the International Security Ligue since 2008. SNP was also admitted into the International Security Ligue in 2015. The International Security Ligue is an association of private security organisations responsible for defining, establishing and maintaining the highest ethical and professional standards of the private security industry worldwide.

13. Our areas of strength include those set out in paragraphs 14 to 17 below.

Aviation Security and Services

14. Certis is a recognised leader in the provision of aviation security expertise, and our aviation business employs more than 3,000 security personnel who work round the clock to ensure the safety and security of passengers at one of the world's busiest airports, Singapore Changi Airport.

15. Certis is also the leading provider of security services at Hamad International Airport in Doha, Qatar.

Key Infrastructure & Installations

Signature of witness

Signature of deponent

16. Certis is the largest armed auxiliary police force and unarmed security guarding agency in Singapore, providing 24x7 guarding for key infrastructure and installations such as prisons, government buildings, hospitals, utilities assets and immigration checkpoints.

Large commercial malls

17. Certis provides services to a number of major mall operators in Singapore, including security guarding, centralised remote command and control for security, and non-security (e.g. car park gantry, lift communications, fire alarm monitoring) operations.

B. Acquisition of SNP

18. In around February 2018, Certis entered into a binding sale agreement for the purchase of 100% of the shares in SNP, Australia's third largest security firm. The acquisition was completed in April 2018.

19. SNP was established in 1923 and is one of the foundation members of the Australia Security Industry Association Ltd (**ASIAL**), Australia's peak national security industry body, which was established in 1969.

20. I am aware that SNP is the pre-eminent provider of aviation security services in Australia, having providing security services to Sydney Airport since 1969. In addition, SNP is a recognised market leader in developing systems and processes for the provision of its security services in Australia. The acquisition of SNP in 2018 provided an opportunity for both SNP and Certis to draw upon each other's strengths and experiences to update and strengthen our existing policies, implement new systems, processes and procedures to meet global best-practice.

C. What happened at the University of Sydney was an isolated event

21. As outlined above, following the acquisition of SNP in April 2018, Certis was focused on integrating SNP into the Certis Group by aligning our core values, ethics, systems and processes so that SNP leverages off Certis' strong track record in those areas (including a zero-tolerance policy towards fraud and corruption), building on SNP's foundations as a leading and respected security provider.

22. It was during this period of integration that Certis became aware of the ICAC raid at the University of Sydney which led to the subsequent public inquiry in February 2019. Once we learnt of the inquiry, SNP took steps to instruct solicitors and senior counsel to advise it as well as retaining solicitors and counsel for its Senior Managing Director, Mr Tom Roche. Certis also

Signature of witness

Signature of deponent

took immediate steps to introduce greater oversight of SNP by the Certis Australia Exco (Executive Committee) and also by Certis.

23. Through SNP's participation in the public inquiry, I was saddened to learn of the conduct which occurred at the University of Sydney between 2016 and early 2018.

24. Based on the evidence led at the public inquiry, I understand that the conduct was a concerted and deliberate fraud on SNP and the University that was perpetrated by the SNP site manager, his second in command, the team leader and the sub-contractor. Rosters and time-sheets were manipulated and SNP was actively misled to ensure that alarms were not raised which allowed the fraud to go undiscovered.

25. As a result of the matters uncovered in the public inquiry, both Certis and SNP have been concerned to ensure that any steps which could assist in the detection of such conduct be taken to prevent, in so far as is possible, a recurrence.

26. By the time of the public inquiry in February 2019, and even during the initial phases of the integration of SNP, Certis had already taken first steps to further strengthen the supervision, management and governance environment in Certis Australia (including SNP).

27. As a first step, Certis implemented the Certis Group Whistle-blower policy in July 2018 (replacing the existing SNP Whistle-blower Policy), with the hotline manned by an external law firm. This updated policy centralised SNP's procedures and gave whistle-blowers confidence that their report will be kept confidential.

28. Near the end of 2018, Certis implemented an Incident Reporting and Investigation Management System ("**IRIMS**") in Certis Australia (including SNP). IRIMS is a system which the Certis group uses to aid and standardise the reporting of incidents (see **Annexure A**).

D. Lessons Learnt – Governance, Policies and Accountability, Awareness & Training

29. The evidence at the public inquiry has indicated that there are lessons to be learnt from this incident. We intend to continue to review these matters, reflect on them and train our staff to be better able to prevent and detect such behaviour. Certis has implemented, or is implementing, processes to address the circumstances which allowed the conduct to occur, including strengthening SNP's existing policies and practices to ensure they are consistent with global best-practice.

Signature of witness

Signature of deponent

30. There appears to me to be three risk themes arising from the public inquiry and I have set out below how Certis is addressing each of them. The processes set out below apply to Protective Services Division and a similar process is also applicable to the Aviation Services Division.

D.1 Enhancing checks and balances

(i) Re-organisation of NOC to ensure Segregation of Duties

31. One of the issues raised in the public inquiry was the risks arising from employees having responsibility for completing and checking rosters at a client site, without sufficient segregation of duties or supervision from the SNP Head Office.

32. The SNP National Operations Centre ("**NOC**") has been reorganised to be responsible for centrally supervising the rostering function. This means:

(a) the rosters are prepared by the Services Delivery team in consultation with the NOC planning team;

(b) NOC will be responsible for verifying that the rosters are prepared in accordance with the requirements stated in the underlying contracts. Any deviations from contractual requirements will be escalated to Head NOC and respective State Managers for joint approval.

(c) after security officers have been deployed at the client site, the NOC will then verify the time and attendance of each deployed employee or subcontractor to ensure it matches the roster, which will confirm that the employee or subcontractor did attend the client's location as planned. Essentially, NOC has responsibility for ensuring the service is actually delivered as required by the client.

33. NOC is independent from the Services Delivery team and has a different reporting line. As the NOC team works at Headquarters, it does not spend time on-site or meet with Resource Partners, nor are members of the NOC team allowed to meet with Resource Partners without prior authorisation from the Head of the NOC and General Manager, Head Protective Services. This ensures proper segregation of duties and a robust compliance regime, providing checks and balances to the Account Managers who work closely with clients and Resource Partners.

34. Segregating the roster planning and supervisory functions in this way will ensure that services requested by the client are actually performed and prevent unperformed shifts being claimed, as was uncovered in the public inquiry.

Signature of witness

Signature of deponent

35. The reorganisation of the NOC referred to above has been completed in NSW, and is expected to be completed in all other states and territories by the second half of 2019.

(ii) Implementation of Systems and End-to-End Processes

Improved Employee and Resource Partner Management

36. SNP's employee management processes have been made more robust to ensure that all employees (employed directly or through Resource Partners) have only one employee ID and secondary employment with our Resource Partners is prohibited, unless specifically authorised by Senior Managing Director or GM, Head Protective Services, and only in limited circumstances. These processes will be cross-verified by our Human Resources system and the Resource Partner management system. Human Resources and Compliance teams, respectively, provide supervision of these employee management processes and have independent reporting lines from NOC and Account Managers. This prevents individuals from: (a) being rostered separately as both SNP employees and Resource Partner staff; and (b) circumventing fatigue rules and working an unrealistic number of hours.

37. In addition, operators at the NOC have a mandatory computer screen which displays any fatigue breaches. The NOC has also been reorganised so that there are now separate roles, with independent and separate reporting structures, responsible for identifying and raising any suspected breaches of fatigue rules with either Senior Managing Director or GM, Head Protective Services.

BOSS System

38. Following the acquisition of SNP and the integration of the SNP business into Certis, Certis has taken steps to roll out the proprietary electronic time and attendance system, BOSS (Business Operations Support System), to all SNP client locations.

39. BOSS has the following features which will provide data to enable checks and balances functions to be performed by NOC:

    (a) When a security officer (either employee or Resource Partner) reports at a client location to commence work, BOSS verifies the identity of the officer through requiring a unique login to be entered, and tracks the GPS location and time using a cloud system clock which cannot be manipulated.

    (b) The BOSS system will be updated by August 2019 to require the security officer to take a photo of himself or herself at the client location, and upload it to the cloud system.

Signature of witness

Signature of deponent

Algorithms will be checking the photos in the back-end cloud system against file reference photos to verify the identity of the security officers. These samples are checked randomly, and checks are increased on sites where there are other indicators of potential fraudulent activity (such as an increase in overtime or fatigue breaches). In the next phase of development, the BOSS system will be enhanced to introduce new facial recognition software, which will allow the identity of all security officers to be automatically verified onsite. We anticipate that these facial recognition software will be in operation by the end of 2019.

(c) BOSS then compares the captured time and attendance data against the roster approved by the client and the NOC, and flags exceptions through an Exception Management Module, which captures the exception such as wrong identity, wrong location or wrong time and the operational actions taken by NOC to verify. For example, wrong time may be verified as "late due to traffic based on phone call with security officer".

(d) The system comes with an audit functionality which captures every user interaction within the system.

(e) Thus, if a staff member is not rostered and turns up at a client site to start work, BOSS will detect and automatically alert the NOC to intervene and verify. If an SNP employee or Resource Partner is rostered, but does not turn up at a client site on time (or at all) and later claims payroll, BOSS will alert the NOC that the corresponding time and attendance data is not available and secondary verification will be required. This "secondary verification" includes the following measures designed to verify whether the security officer was present for the rostered shift:

(i) confirming with the on-site Manager or client representative;

(ii) reviewing CCTV footage on-site;

(iii) reviewing contemporaneous work reports, such as sheet logs or incident reports, which would indicate the presence of the officer on site; and

(iv) accessing and reviewing the use of swipe cards or other electronic system measures and reconciling this data.

40. The data BOSS will capture is at **Annexure B**. We intend to implement BOSS across all SNP Client sites (475 sites in total) in NSW by the end of 2019.

Signature of witness

Signature of deponent

41. In the interim period, timesheets will be completed manually by SNP employees and Resource Partners and will be reviewed by the NOC to confirm all information has been completed. Once NOC staff are satisfied that all information has been completed, the data is keyed into Microster, which will automatically cross-check against the roster and the relevant shift is locked at the end of the day, such that any changes/further inputs will require NOC manager approval. Where the timesheet is missing information or is inconsistent with the roster, NOC staff will escalate this to NOC manager for resolution, which includes conducting the secondary verification measures identified at subparagraph 39(i) - (e)(iv) above.

D.2 Clear policies and accountability

42. One of the issues arising from the public inquiry was the need to strengthen SNP's policies and accountability procedures in relation to conflicts of interest and subcontractor management, to ensure that SNP staff cannot also work for a Resource Partner without specific approval from Senior Managing Director or GM, Head Protective Services, and to prevent a Resource Partner's performance being managed by the site manager without proper oversight. Although SNP's existing offers of employment precluded employees from accepting secondary employment with a Resource Partner, it was clear from the public inquiry that this was not being adequately enforced.

43. SNP was tasked by the Certis Australia Exco to conduct a review of SNP's policies. There will now be a diligent enforcement of a conflicts of interest policy by Human Resources team. Separately, an independent Compliance team will use SNP systems to track whether any employee works for a Resource Partner.

44. SNP has also updated its existing Subcontractor Management Policy to strengthen the underlying framework and implement appropriate escalation process. Under the Subcontractor Management Policy:

    (a) A Resource Partner will be appointed by a committee (the "**Resource Partner Management Committee**") comprising the Senior Managing Director, Mr Roche, Head of Protective Services, Head of Aviation Services, Head of Sales, Head of Finance and Head of Risk, rather than by the site manager .

    (b) Security officers deployed will be screened for suitability in accordance with Client contract requirements.

    (c) Security license information will be lodged with the Compliance Team, which will check to ensure that no employee is also working for a Resource Partner.

Signature of witness

Signature of deponent

(d) Performance issues, such as breaches of fatigue rules, will be escalated and dealt with by NOC Management, the Client Service Manager and the State Managers. If the resolutions are not satisfactory resolved (as determined by NOC Manager), the issue is escalated to the Compliance Team and they will report to the Resource Partner Management Committee.

(e) Termination of a Resource Partner must be approved by the Head of Compliance.

(f) There will be on-going due diligence checks by NOC and Compliance Teams, in particular for breaches of fatigue rules. Resource Partners will be made aware of, and will be asked to adhere to, these compliance checks.

45. The updated Subcontractor Management Policy was rolled out across all SNP sites on 16 April 2019.

D.3 Awareness and Training

46. As mentioned above, Certis has introduced IRIMS reporting system to SNP. This will give ground and senior managers better oversight of the issues at sites based on the categories of issues.

47. Another issue which arose from the public inquiry was the perceived lack of awareness and training by the NOC staff in relation to some areas, including escalation of concerns to their supervisors. I understand from Linda Willard, National Scheduling Manager at SNP, that the NOC implemented a series of training on 17 April 2019 and 23 April 2019 to assist the NOC staff understand SNP's legal obligations under Section 35 of the *Security Industry Legislation* and train them on time-sheet fraud detection, fatigue management and the escalation process. All new starters will be required to undergo this training.

48. At **Annexure C** is a copy of the NOC training materials and attendance sheets of personnel who attended training.

E. Audit and Integrated Assurance Framework

49. The Certis Group Internal Audit will be conducting an advisory audit commencing in the week beginning 10 June 2019 to affirm the implementation and effectiveness of the controls outlined at sections D.1 and D.2 above to prevent the reoccurrence of such incidences. The Internal Audit team is an independent team from SNP Management and will report to the Certis Group Audit & Risk Committee and, in respect of this incident, to the Special Committee (see below) as well.

Signature of witness

Signature of deponent

50. The Certis Group will also be rolling out an Integrated Assurance Framework ("**IAF**") across the entire organisation, including SNP. We anticipate that the IAF will be implemented in Australia by December 2019. The IAF is a framework that encompasses two or more assurance plans (e.g. audit, risk, compliance) to show the collective assurance coverage of risks and controls across the organisation. Embedded in the IAF is a management controls assessment where key risks within business-as-usual processes are reviewed by Management and assurance given (as Line 1) and its effectiveness and controls are counter-checked by a risk or compliance team (Line 2) and audited by internal and/or external auditors (Line 3). At **Annexure D** is a diagrammatic representation of the IAF.

E. Ethos and Values

51. Notwithstanding the measures we have put in place to address the three themes referred to above, we believe that doing the right thing begins with our people. We work hard to ensure that the right people with the right values are brought into the Certis Group.

52. As stated above, the Certis Group has a zero-tolerance policy towards fraud and corruption. Anti-bribery and corruption principles are and have been part of the Certis Business Ethics Policy since 2008. Last year, Certis updated the Business Ethics Policy and introduced a stand-alone Anti-Bribery & Corruption Policy to place even further emphasis on Certis' position on corruption. Certis introduced these policies to SNP in February 2019, supported by videos and communications programs to ensure that the message is clearly received by our staff.

53. Reflecting the level of importance Certis places on the lessons learnt from this incident, Certis is instituting the following additional measures:

    (a) The above actions and other corrective actions are now directed and supervised by the Certis Australia Executive Committee chaired by me; assisted by the Chief Corporate Officer & Chief Risk Officer and General Counsel.

    (b) The Certis Group Board has constituted a Special Committee led by the Board Chairman, Mr Olivier Lim, assisted by fellow Board Directors:

        (i) Mr Boon Hui Khoo - who is the former President of Interpol and former Commissioner of the Singapore Police Force; and

        (iii) Mr Paul Retter - who is the former Chief Executive of the National Transport Commission,

    to oversee Certis' response to the incident.

Signature of witness

Signature of deponent

54. This Special Committee will be aided by Mr Mick Keelty, who is the former Commissioner of the Australian Federal Police, and a member of the Certis Group International Advisory Panel. Mr Keelty is working with Certis in implementing the enhancements described above, advising Certis of any other enhancements which he considers are appropriate (such as emphasising our ethical work culture), and identifying any other areas of risk.

Signature of witness

Signature of deponent

Annexure A
IRMS

Document Profile

Title	National Incident Reporting & Investigation Management System (IRIMS)
Type	Procedure
Division	Risk, Safety and Compliance
BU/Department	Operational Risk
Branch	National
Audience	Aviation Duty Shift Manager (DSM), National operations centre (NOC) operators, National operational risk team

Purpose

The Incident reporting and investigation management system is a standardized system of reporting across the Certis group.

All Certis business units are required to report all relevant incidents via IRIMS. This procedure will provide the process for the IRIMS.

The Australian Certis business unit will follow this procedure by reporting all incidents via the normal reporting lines and processes. The National Operations center (NOC) and the Aviation Duty Shift Manager (DSM) will enter all relevant incidents into the IRIMS.

The IRIMS will be managed by the Integrated Operations Center (IOC) in the Singapore head office.

Responsibilities

1 Category 1

Role	Requirements
1.1 Market head/Supervising SLT	- The Market head or respective supervising Senior Leadership Team (SLT) is the final authority on incident classification. They will approve Cat 1 incident report prior to its submission to IOC.
BU Head **State or branch manager**	- BU head is to ensure that the current processes to detect and report incidents on time is working adequately and that these incidents are classified correctly. - BU head is to seek approval from his supervising ELT / SLT. The BU head is also required to assess the need for inputs from Group Communications for media impact of any incident. - In the event there are any queries by the Board of Directors (BOD), the BU Head is required to provide clarification after consultation with their supervising ELT / SLT.
NOC/DSM	- NOC/DSM is responsible for classifying the incidents based on the IRIMS classification guide, preparing the incident reports and forwarding these reports to IOC duty Operations Manager (OM). - In the event of a Cat 1 incident, they are to forward the incident report to respective BU Head and then Supervising ELT/SLT for approval.
Frontline Staff	- Frontline staff are responsible for reporting the facts of the incident to their supervisor / manager.
IOC Duty OM **(Singapore)**	- IOC Duty OM is to check that the incident is classified correctly before raising IRIMS. - IOC Duty OM is also responsible to check for missing details, accuracy and completeness of the report and advise the BU accordingly. - IOC Duty OM is to inform Head IOC and send the incident report to Head IOC for clearance. Once cleared, he will proceed to raise the Cat 1 IRIMS. - The IOC Duty OM will prepare the notification to the Board of Directors (BOD). The notification will be sent to Head IOC for clearance, after which the OM will send the notification.
Head IOC **(Singapore)**	- Head IOC is responsible to clear both the Cat 1 IRIMS and notification to Board of Directors.

1.2 Group Communications (GC)	- GC is required to work with the BU head to draft the media management plan and include it as part of the incident report, if necessary as per the crisis communication SOPs for the AU market.

2 Category 2-6

Role	Requirements
Supervising ELT / SLT	• The ELT/SLT will review all Category 2 incidents received from IRIMS and follow up where required.
BU Head	• BU head is to ensure that the current processes to detect and report incidents on time is working adequately and that these incidents are classified correctly. • The BU head is to ensure timely follow up and closure of Cat2 and Cat 3 IRIMS • The BU head is to review and action the report from the IOC head on outstanding IRIMS.
NOC/DSM	• NOC/DSM is responsible for classifying the incidents based on the IRIMS classification guide, preparing the incident reports and forwarding these reports to IOC duty Operations Manager (OM).
Frontline Staff	• Frontline staff are responsible for reporting the facts of the incident to their supervisor / manager.
IOC Duty OM **(Singapore)**	• IOC Duty OM is also responsible to check for missing details, accuracy and completeness of the report and advise the BU accordingly.
2.2 Group Communications (GC)	• GC is required to work with the BU head to draft the media management plan for category 2 and include it as part of the incident report, if necessary as per the crisis communication SOPs for the AU market.

Incident Classification

For IRIMS, Certis uses 6 categories to classify incidents. The table below sets out the definitions, recipients and approving authority for each category. Examples of the types of incidents for each category are given in **Annex C.**

Category	Definitions	Recipients	Approving Authority
Category 1	• Incidents with major impact • Incidents which require immediate notification and investigation • Incidents which the BOD must be informed	• BOD# • All ELT • Group Comms • Hd IA • GHR • Legal • Chief Security Officer • Risk Mgmt • IOC Mgmt • BU concerned* • AU SLT	• Supervising ELT / SLT
Category 2	• Incidents with moderate impact • Incident which require notification but not immediate • Incidents which the ELT must be informed	• All ELT • IOC Mgmt • AU SLT • BU	• NOC Team Lead/DSM
Category 3	• Incidents with minor impact • Incidents which BU KAH must be informed	• IOC Mgmt • BU	• NOC Team Lead/DSM
Category 4	• Compliments	• IOC Mgmt • Customer Service Division • AU SLT • BU	• NOC Team Lead/DSM
Category 5	• Complaints	• IOC Mgmt • Customer Service division • AU SLT • BU	• NOC Team Lead/DSM

Category 6	• Miscellaneous, e.g. - Site visits - Mustering parade - Staff dialogue session	• IOC Mgmt • BU	• NOC Team Lead/DSM

# BOD to be notified via email. See **Annex D**

* BU concerned will determine respective recipients in the various categories.

1 Turnaround Time

All CAT1 incidents must be reported to IOC promptly. If full facts are not available, an interim report can be submitted. Further updates can be provided as and when available. IOC duty OM can be contacted via email at iom@certissecurity.com

All incidents that fall into category 2-6 as per the tables above, must be entered into IRIMS as per the below table based on incident severity.

The turnaround time for reporting of incidents are:

Category	Lead Time for BU to send incident report to IRIMS officer upon incident reported	Lead Time for IRIMS officer to create IRIMS upon receiving incident report
Category 1	<30 mins	<2 hours
Category 2	<2 hours	<4 hours
Category 3	<8 hours	<12 hours
Category 4	<8 hours	<12 hours
Category 5	<8 hours	<12 hours
Category 6	<8 hours	<12 hours

2 Format of Reports

The IRIMS will require the following fields completed.

Category	**National BU and incident severity** **E.g.** • AU – Cat 1 • AU – Cat 2 • AU – Cat 3
Sub-Category	**Division, branch & AU BU** **E.g.** • PS-NSW-Metro • AVI-SYD-T1
Type	**Brief description of incident** **E.g.** • Loss of weapons • WHS safety incident

Status	**Inform if this is a new incident or update to a previous IRIMS raised** **E.g.** • First Incident Report (new incident) • Incident Update (follow-up to a previous IRIMS)
Occurred Date & Time (of Country)	**Date and time of incident in the following format** **E.g.** • 1. 10-04-2018 10:00:04 AM
Location	**Location of incident** **E.g.** • Toll Banksmeadow • Newcastle Airport
Incident Details (Who, What, where, Why, How)	**Description of the incident** **E.g.** On the a/m date, time and location, officer xxx …

3 Administration of IRIMS

3.1 Follow-up on IRIMS Report - Open / Closed

By default, when IOC/NOC/DSM creates a new IRIMS for Cat 1 to 3, the IRIMS status will be left as 'open', as the BU may need to provide further updates to the IRIMS. For Cat 1 incidents the BU will need to inform IOC during the incident reporting to indicate the status as 'closed', if it deems that there shall not be further updates.

On a monthly basis, IOC will forward the 'open' IRIMS reports to respective BU for follow-up, and for BU to advise the NOC/DSM to update the status (open or closed) accordingly.

Cat 4 and Cat 5 will be routed to Customer Service Division for follow-up. Cat 6 is logged for the main purpose of repository.

4 Recipient List

BU will submit its recipient list (of BU) for all categories to IOC. Further, to ensure that the correct personnel promptly receive the IRIMS, the BU will need to inform the reporting officer whenever there is a change in KAH.

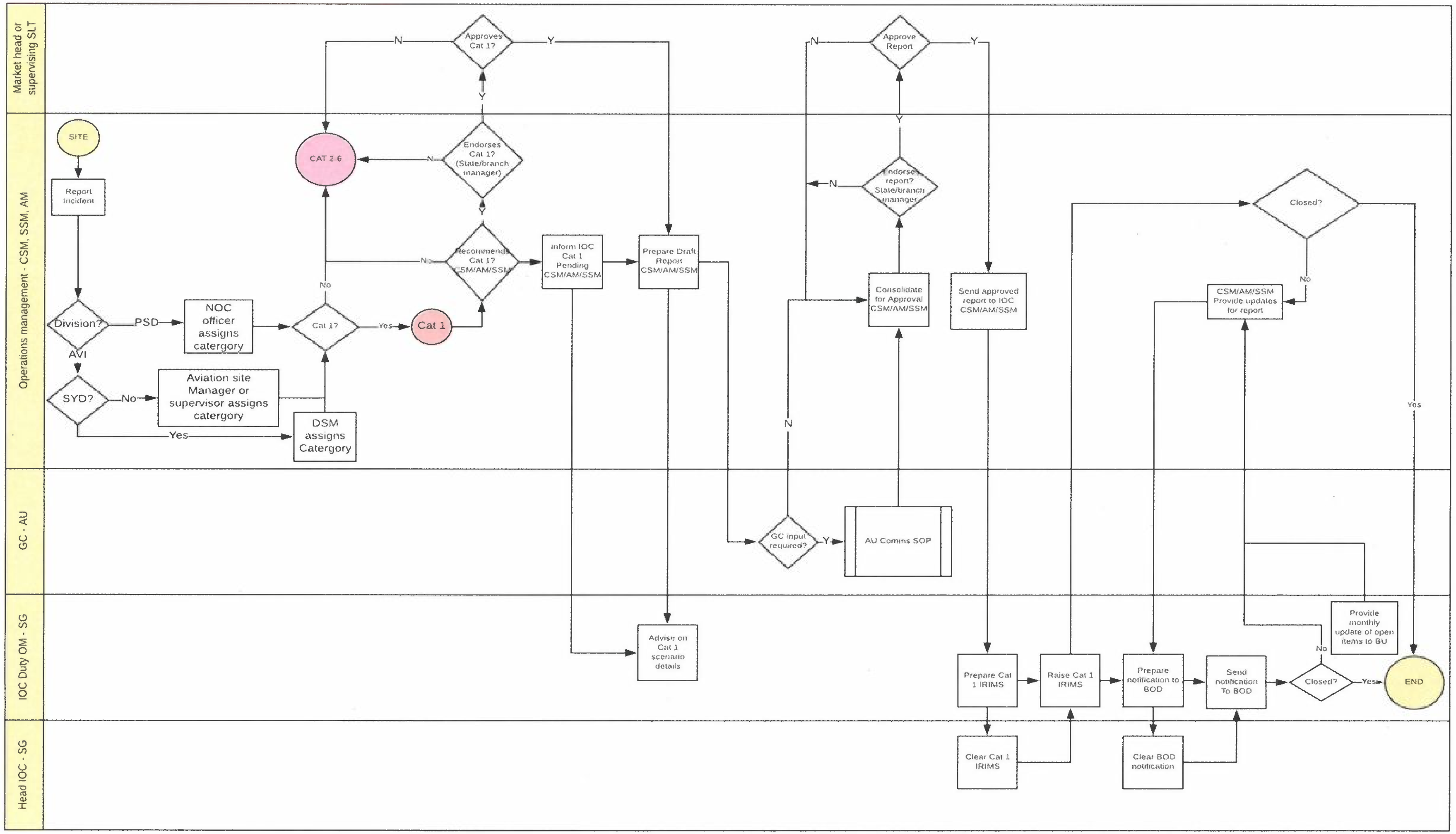
Additionally, on a 6-monthly basis, IOC will extract the Incident data from the IRIMS system and send to the BU / SU its recipient list for review.

5 Conclusion

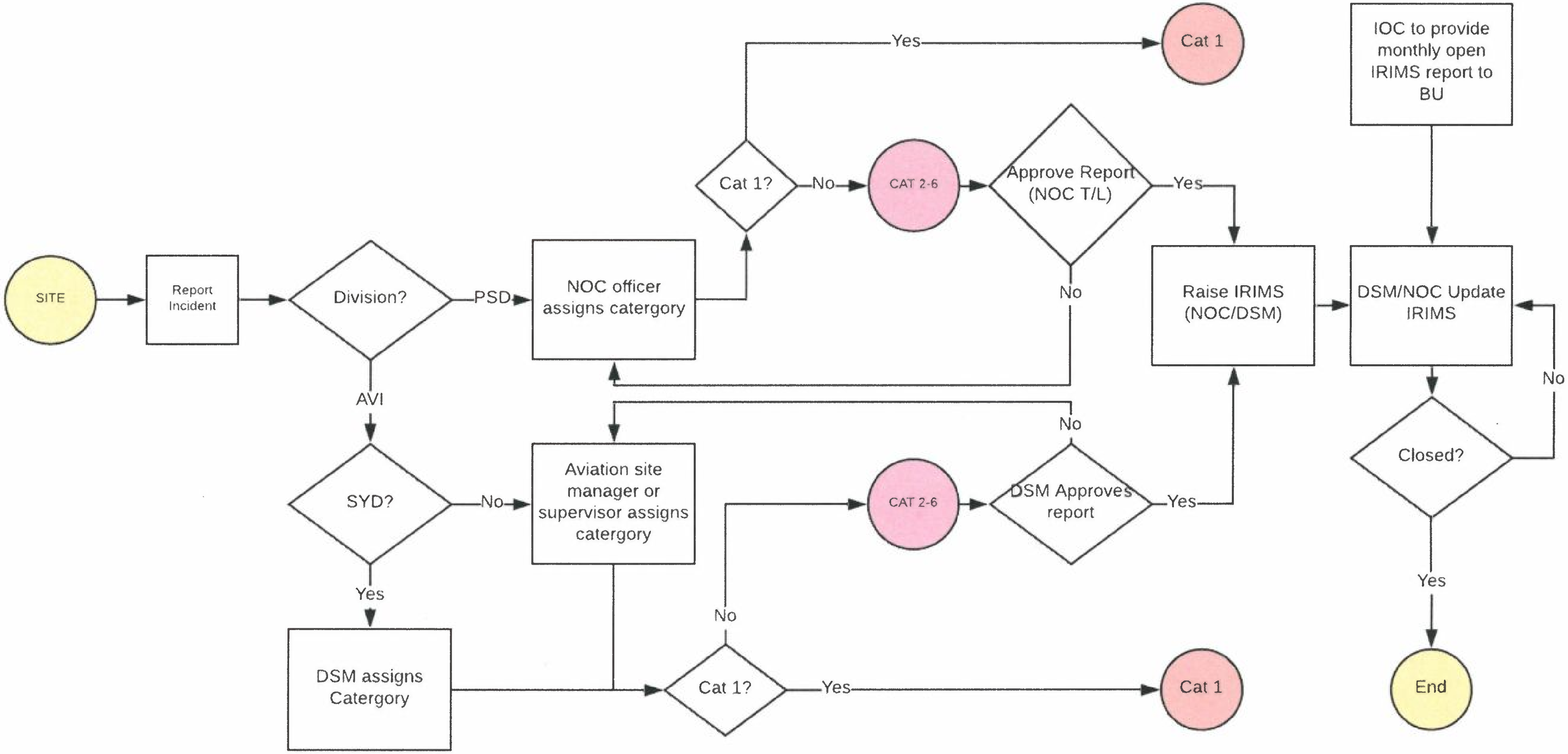
Prompt reporting of incidents will allow the management to respond and manage the incidents in a timely, appropriate and effective manner, including allocating additional resources to mitigate any untoward impact arising from the incidents. It is therefore imperative that all BU adhere to the IRIMS policy.

Flowcharts

Process for Incident Reporting for Cat 1 (AU)


Market head or supervising SLT
Operations management - CSM, SSM, AM
GC - AU
IOC Duty OM - SG
Head IOC - SG
SITE
Report Incident
Division?
PSD
AVI
NOC officer assigns catergory
SYD?
No
Aviation site Manager or supervisor assigns catergory
Yes
DSM assigns Catergory
Cat 1?
No
Yes
Cat 1
CAT 2-6
Recommends Cat 1? CSM/AM/SSM
No
Y
Endorses Cat 1? (State/branch manager)
N
Y
Approves Cat 1?
N
Y
Inform IOC Cat 1 Pending CSM/AM/SSM
Prepare Draft Report CSM/AM/SSM
Advise on Cat 1 scenario details
GC input required?
Y
N
AU Comms SOP
Consolidate for Approval CSM/AM/SSM
Endorses report? State/branch manager
N
Y
Approve Report
N
Y
Send approved report to IOC CSM/AM/SSM
Prepare Cat 1 IRIMS
Clear Cat 1 IRIMS
Raise Cat 1 IRIMS
Prepare notification to BOD
Clear BOD notification
Send notification To BOD
Closed?
Yes
No
END
Provide monthly update of open items to BU
CSM/AM/SSM Provide updates for report
Closed?
No
Yes

Process for Incident Reporting for Cat 2-6 (AU)



Annex B

1 List of business units

Descriptor	Division	Branch	BU	Primary Email address
PS-NSW-Metro	PS	NSW	NSW Metro	NSW MetroIRIMS@snpsecurity.com.au
PS-NAT-PSI	PS	NAT	PSI	PSIIRIMS@snpsecurity.com.au
PS-NSW-REG	PS	NSW	NSW Regional	NSWRegionalRIMS@snpsecurity.com.au
PS-VIC	PS	VIC	VIC	VICIRIMS@snpsecurity.com.au
PS-QLD	PS	QLD	QLD	QLDIRIMS@snpsecurity.com.au
PS-ACT-Corroboree	PS	ACT	Corroboree	CorroboreeIRIMS@snpsecurity.com.au
PS-ACT	PS	ACT	ACT	ACTIRIMS@snpsecurity.com.au
AVI-SYD-T1	AVI	SYD	T1	T1IRIMS@snspecurity.com.au
AVI-SYD-T2	AVI	SYD	T2	T2IRIMS@snspecurity.com.au
AVI-SYD-T3	AVI	SYD	T3	T3IRIMS@snspecurity.com.au
AVI-SYD-PS	AVI	SYD	CBS	CBSIRIMS@snspecurity.com.au
AVI-SYD-CBS	AVI	SYD	PS	AVIPSIRIMS@snspecurity.com.au
AVI-SYD-AVSEC	AVI	SYD	AVSEC	AVSECIRIMS@snspecurity.com.au
AVI-ACT	AVI	ACT	Canberra airport	ACTAVIIRIMS@snpsecurity.com.au
AVI-VIC	AVI	VIC	Melbourne airport	VICAVIIRIMS@snpsecurity.com.au
AVI-NSW-Reg	AVI	NSW	NSW Regional Aviation	NSWRegAVIIRIMS@snpscurity.com.au
AVI-QLD	AVI	QLD	Sunshine coast airport	QLDAVIIRIMS@snpsecurity.com.au
AVI-SA	AVI	SA	Adelaide airport	SAAVIIRIMS@snpsecurity.com.au
AVI-NAT-QF	AVI	NAT	QF	QFAVIIRIMS@snpsecurity.com.au
CORP-NAT-IT	CORP	NAT	IT	ITIRIMS@snpsecurity.com.au
CORP-NAT-CM	CORP	NAT	Sales/Customer service	CSIRIMS@snpsecurity.com.au
CORP-NAT-HR	CORP	NAT	HR	AUIRIMS@snpsecurity.com.au
CORP-NAT-SLT	CORP	NAT	SLT	AUSLTIRIMS
CORP-NAT-Safety	CORP	NAT	Safety	Incidents@snpsecurity.com.au

ANNEX C

1 Types of Incidents for Each Category

The tables for the six categories serve as a guide for classifying incidents. For Cat 1, the classification is also aligned with the Certis Australia Enterprise Risk Management (ERM) framework.

2 Category 1 (Major Incidents) and Category 2 (Moderate Incidents)

S/no	Subjects	Descriptions (Cat 1)	Descriptions (Cat 2)
1	(R3) Weapon Management	• Misfire / negligent discharge of firearms • Loss of weapons and / or ammunition • Incidents whereby firearms have been used • AWOL of any APO with firearms and / or ammunition or any APO bound missing from duty post.	• Near misses on loss of firearms / ammunition
2	(R5A) Cyber Security External	• Successful cyber-attack that has penetrated through customer's system (provided by Certis) and caused damage in terms of service disruption, data loss or financial loss	• Successful cyber-attack that has penetrated through customer's system (provided by Certis) but did not cause any damage in terms of service disruption, data loss or financial loss
4	(R7) Regulatory Noncompliance	• Non-compliance with applicable key laws and regulations leading to termination of license / freeze hiring / substantial fine by relevant authorities • Fair work Act 2009 • Anti-Discrimination Act 1977 • Workplace injury and Workers compensation Act 1998 • Privacy Act 1988 • Industrial relations Act 1996 • State based WHS Act and Regulations	• Non-compliance with applicable key laws and regulations leading to warning by the relevant authorities • Fair work Act 2009 • Anti-discrimination Act 1977 • Workplace injury and Workers compensation Act 1998 • Privacy Act 1988 • Industrial relations Act 1996

			• State based WHS Act and Regulations
5	(R8A) Competition Risk	Loss of clients / business opportunities Cancellation notice or tender feedback.	Warning letter issued by Client for a possible contact cancellation.
6	(R8B) Concentration Risk	Notice of cancellation of top 20 Clients due to increased competition and slow reaction	Warning letter issued by top 20 clients for a possible contact cancellation.
7	(R11) Workplace Safety	• Death of staff while on duty, or to and from duty	Regulator notifiable injury
8	(R21) Fraud & Corruption Risk	Dishonesty using influence or deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose or the improper use of information or position for personal financial benefit. Fraudulent or corrupt conduct by internal parties or external entities targeting the organisation or fraudulent or corrupt conduct by the organisation itself targeting external entities.	Unintentional breach of Certis Governance policy.
9	(R22) Vendor Management Risk	Repetitive/Deliberate breach of Service Level Agreement by third-party products, IT suppliers and service providers resulting in potential business disruption and negative impact on business performance	Unintentional breach of service level agreement.
10	(R23) Industrial Relations Risk	Significant industrial action by a Union which might result in disrupt of business as usual. Fine issued by a regulator or adverse court findings.	Breakdown in communication with unions or employee representative groups. Warning issued by a regulator or by the court.

3 CATEGORY 3 (Minor Incidents)

4 S/No	5 Subjects	6 Descriptions
7 1	**8** Internal Compliance	• Internal Audit exercises • Internal compliance checks
9 2	**10** Routine Incidents	• Security breach • Security incident • Weapon
11 3	**12** Suggestions	• Process improvement suggestions
13 4	**14** Offences	• Loss of security license • Expiry of first aid certificates • Breach of SOP • Breach of Code of Conduct
15 5	**16** Workplace Safety	• Workplace safety Medical treatment • Workplace safety First aid treatment • Workplace safety notification only • Workplace near miss

17 CATEGORY 4 (Compliments)

S/No	**Subjects**	**Descriptions**
1	Compliments	• From client or members of the public e.g. o Excellence in customer service o Exemplary honesty o Going the extra mile

18 CATEGORY 5 (Complaints)

S/No	**Subjects**	**Descriptions**
1	Complaints (BU to upgrade Category if deemed necessary.)	• From client or members of the public e.g. o Poor working attitude o Unprofessional o Failure to meet SLA

19 CATEGORY 6 (Miscellaneous)

S/No	Subjects	Descriptions
1	Miscellaneous	• Internal performance feedbacks • Maintenance observations • Safety hazard report • Safety near miss report

ANNEX D

1 Email Recipients for Cat-1 Notification to Board of Directors

The following table lists out the recipients for the Cat-1 notification to BOD.

Send	Recipients
To:	To: BOD: 1. Chairman – Olivier Lim 2. Director – Yap Chee Keong 3. Director – Khoo Boon Hui 4. Director – Jonathan E Popper 5. Director – Retter Paul Bernard 6. Director – Chong Ee Rong
CC:	CC: Corporate: 1. GCEO – Paul Chong 2. CE (SG) – Ronald Poon 3. CCO – Kelvin Ling 4. CGTO – Chua Chwee Koh 5. SVP GHR – Ivy Ho 6. SVP Legal – Laura Low 7. SVP GC – Tan Toi Chia

	8. VP GHR – Daniel Low 9. VP PMP – Isabelle Lim 10. SM IOC – Brijesh Kumar Rai BU concerned: 11. Supervising ELT / SLT 12. Head of BU

Associated Forms & Records

Forms required by this process referenced above, must be held **[enter where records are held physically and/or electronically]** and are maintained in accordance with Records Management [943].

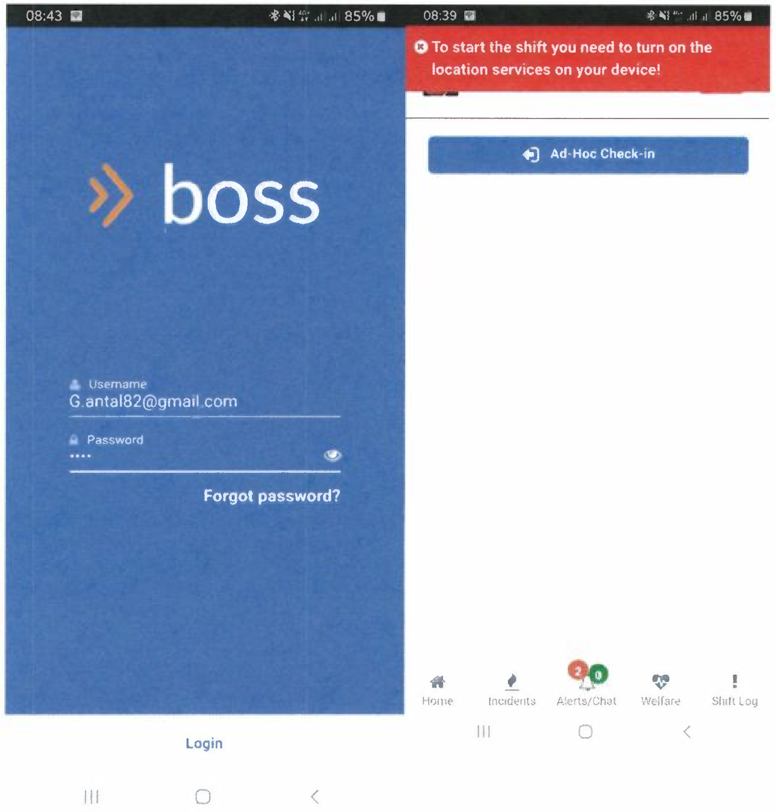
1

Annexure B
(BOSS)

BOSS Time and Attendance

Geolocation and Unique Login Credentials

- BOSS captures geolocation data in real time and displays it in the Admin Portal where Management can easily identify who, where, when and how the officer is signing into their shift
- Each officer uses their unique username to sign into their account, this is either their personal email address or Employee ID number. Officers are initially provided a default password to access BOSS and are advised to change it during their first login
- In order to sign into BOSS there are prerequisites that must be met in order to proceed. As BOSS uses geolocation to capture where the officer has signed in from, officers must have their location services enabled on their mobile device otherwise BOSS will not allow them to sign in and will prompt a message to enable location services
- BOSS uses the device clock to identify the time the officer signs into their shift. There are measures in place on the Admin Portal to ensure the Device time matches the Server time
- All site devices have Mobile Device Management (MDM) software enabled to restrict device settings being adjusted meaning officers are unable to adjust the time or disable location services



Username
G.antal82@gmail.com

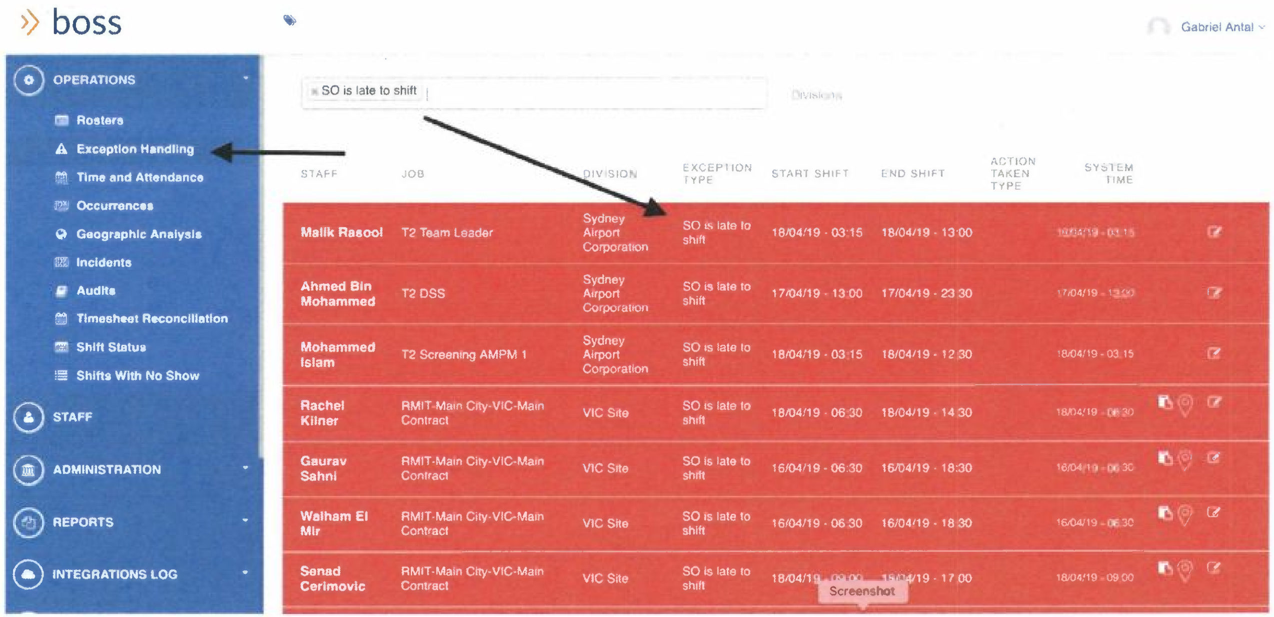
Password
••••

To start the shift you need to turn on the location services on your device!

BOSS Time and Attendance

Geolocation and Unique Login Credentials

- If an officer has not signed into their shift, this will log an exception "SO is late to shift" which is monitored by the NOC who will then contact the officer and have them sign in

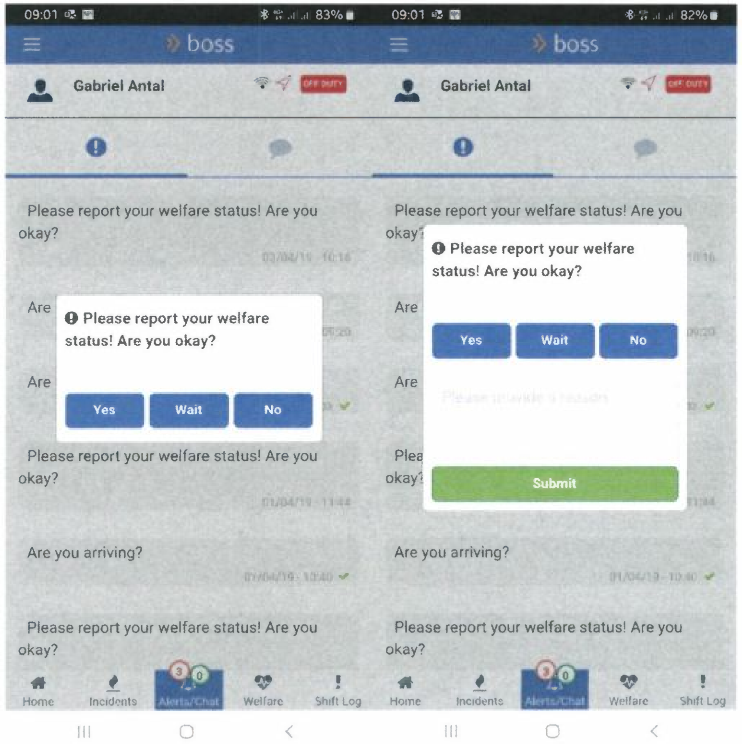


STAFF	JOB	DIVISION	EXCEPTION TYPE	START SHIFT	END SHIFT	ACTION TAKEN TYPE	SYSTEM TIME
Malik Rasool	T2 Team Leader	Sydney Airport Corporation	SO is late to shift	18/04/19 - 03:15	18/04/19 - 13:00		18/04/19 - 03:15
Ahmed Bin Mohammed	T2 DSS	Sydney Airport Corporation	SO is late to shift	17/04/19 - 13:00	17/04/19 - 23:30		17/04/19 - 13:00
Mohammed Islam	T2 Screening AMPM 1	Sydney Airport Corporation	SO is late to shift	18/04/19 - 03:15	18/04/19 - 12:30		18/04/19 - 03:15
Rachel Kilner	RMIT-Main City-VIC-Main Contract	VIC Site	SO is late to shift	18/04/19 - 06:30	18/04/19 - 14:30		18/04/19 - 06:30
Gaurav Sahni	RMIT-Main City-VIC-Main Contract	VIC Site	SO is late to shift	16/04/19 - 06:30	16/04/19 - 18:30		16/04/19 - 06:30
Walham El Mir	RMIT-Main City-VIC-Main Contract	VIC Site	SO is late to shift	16/04/19 - 06:30	16/04/19 - 18:30		16/04/19 - 06:30
Senad Cerimovic	RMIT-Main City-VIC-Main Contract	VIC Site	SO is late to shift	18/04/19 - 09:00	18/04/19 - 17:00		18/04/19 - 09:00

BOSS Welfare System

Welfare Checks

- BOSS is equipped with a Welfare check system which prompts officers to perform a welfare check regularly. BOSS will ask the officer “Please report your welfare status. Are you ok?” The officer then must respond with Yes or No in order to proceed using BOSS
- If officers answer “No” they will be asked to provide a reason, this is then logged as an exception which is monitored by the National Operations Centre (NOC) who will then attempt to contact the officer directly. If the officer does not respond, further action is taken to establish communication with the officer
- If officers answer “Yes”, no further action is required and officers continue on their shift as per normal



Please report your welfare status! Are you okay?

Are

Are

Please report your welfare status! Are you okay?

Are you arriving?

Please report your welfare status! Are you okay?

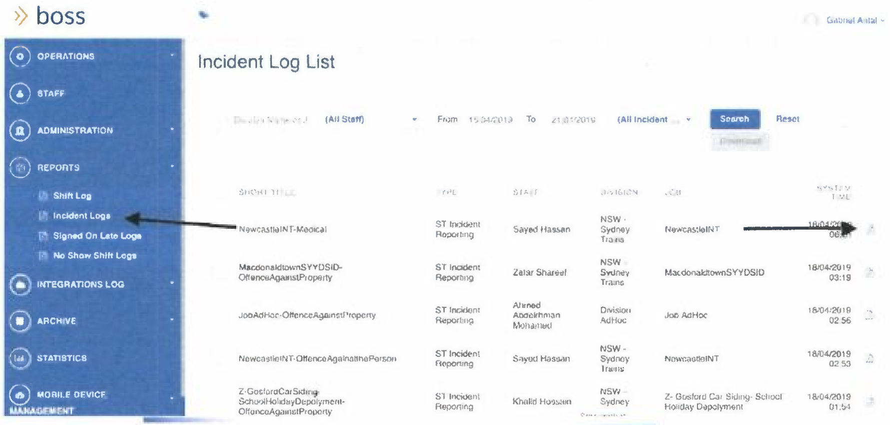
Please report your welfare status! Are you okay?

Please report your welfare status! Are you okay?

BOSS Reporting

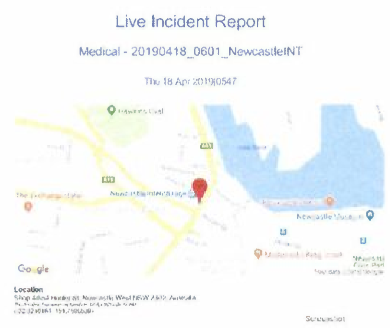
Incident Reports

- BOSS gives officers the ability to complete Incident Reports at a live location making it easier to capture accurate information and in real time
- When an officer opens a new Incident Form, BOSS captures the location of where the Incident Report is being completed
- Incident reports are time stamped and once submitted cannot be altered or adjusted
- Incident reports capture important details such as the officers Location, Name, Date and Licence Number automatically as well as the officers e-signature which is presented at the bottom of each report
- All Incident Reports are accessible from the Admin Portal and can be downloaded in PDF format



Incident Log List

SHORT TITLE	TYPE	STAFF	DIVISION	JOB	SYSTEM TIME
NewcastleINT-Medical	ST Incident Reporting	Sayed Hassan	NSW - Sydney Trains	NewcastleINT	18/04/2019 06:01
MacdonaldtownSYYDSID-OffenceAgainstProperty	ST Incident Reporting	Zafar Shareef	NSW - Sydney Trains	MacdonaldtownSYYDSID	18/04/2019 03:19
JobAdHoc-OffenceAgainstProperty	ST Incident Reporting	Ahmed Abdelrhman Mohamed	Division AdHoc	Job AdHoc	18/04/2019 02:56
NewcastleINT-OffenceAgainsttheParson	ST Incident Reporting	Sayed Hassan	NSW - Sydney Trains	NewcastleINT	18/04/2019 02:53
Z-GosfordCarSiding-SchoolHolidayDeployment-OffenceAgainstProperty	ST Incident Reporting	Khalid Hossain	NSW - Sydney	Z- Gosford Car Siding- School Holiday Deployment	18/04/2019 01:54



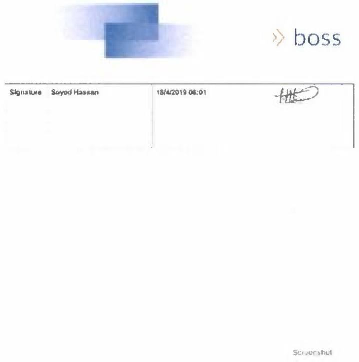
Live Incident Report

Medical - 20190418_0601_NewcastleINT

Thu 18 Apr 20190547

Location
Shop Allied Hunter St, Newcastle West NSW 2302, Australia
[illegible]

Screenshot



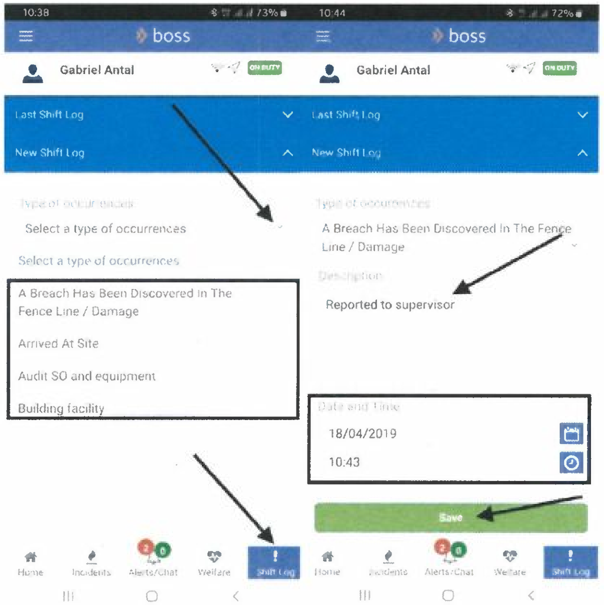
Signature	Sayed Hassan	18/4/2019 06:01

Screenshot

BOSS Occurrences

Shift Logs

- A Shift Log is created for each officer that captures all Occurrences during an officers shift. This is basically a personal Logbook for an individual officer
- This begins from the moment the officers signs into their shift and ends when the officer signs out
- Officers can easily navigate to the Shift Log tab and select an Occurrence
- Once an Occurrence is selected, the officer can type in any additional notes if required, select the time of the occurrence then hit “Save”



10:38 73%

boss

Gabriel Antal ON DUTY

Last Shift Log

New Shift Log

Type of occurrences

Select a type of occurrences

Select a type of occurrences

A Breach Has Been Discovered In The Fence Line / Damage

Arrived At Site

Audit SO and equipment

Building facility

10:44 72%

boss

Gabriel Antal ON DUTY

Last Shift Log

New Shift Log

Type of occurrences

A Breach Has Been Discovered In The Fence Line / Damage

Description

Reported to supervisor

Date and Time

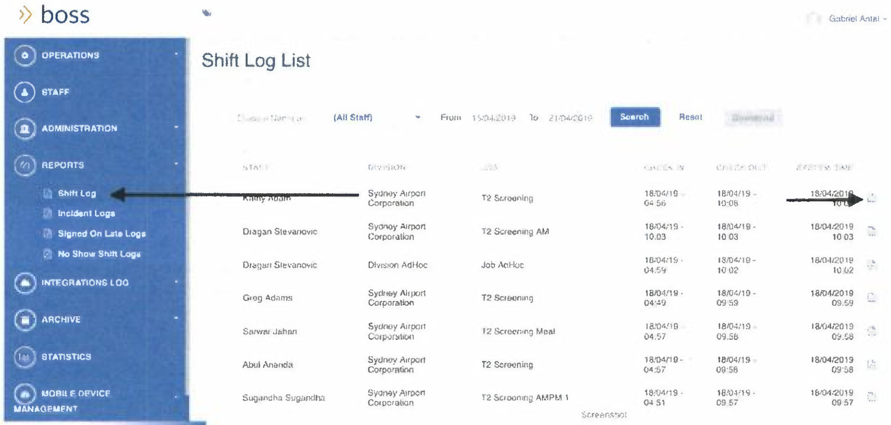
18/04/2019

10:43

BOSS Occurrences

Shift Logs

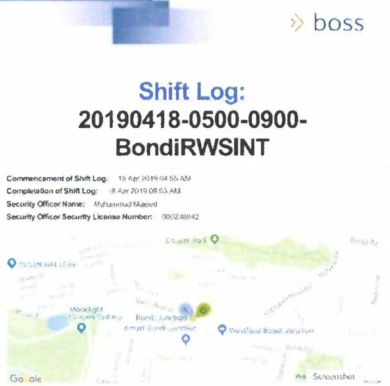
- Each time one of these Occurrences are selected, BOSS captures the location of the selection and records it in the Time and Attendance tab of the Admin Portal as well as the officers Shift Log
- Shift Logs are time stamped and cannot be altered or adjusted
- Shift Logs capture important details such as the officers Location, Name, Date and Licence Number automatically as well as the officers e-signature which is presented at the bottom of each report
- Shift Logs are accessible from the Admin Portal and can be downloaded in PDF format



Shift Log List

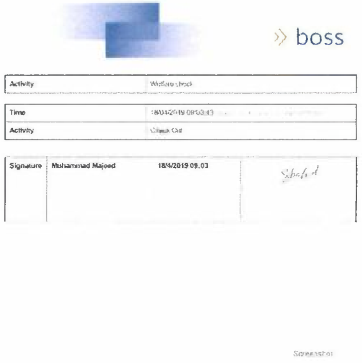
From 15/04/2019 To 21/04/2019

STAFF	DIVISION	JOB	CHECK IN	CHECK OUT	[illegible]
Kathy Adam	Sydney Airport Corporation	T2 Screening	18/04/19 - 04:56	18/04/19 - 10:08	18/04/2019 10:0[illegible]
Dragan Stevanovic	Sydney Airport Corporation	T2 Screening AM	18/04/19 - 10.03	18/04/19 - 10 03	18/04/2019 10 03
Dragan Stevanovic	Division AdHoc	Job AdHoc	18/04/19 - 04:59	18/04/19 - 10 02	18/04/2019 10 02
Greg Adams	Sydney Airport Corporation	T2 Screening	18/04/19 - 04:49	18/04/19 - 09:59	18/04/2019 09.59
Sarwar Jahan	Sydney Airport Corporation	T2 Screening Meal	18/04/19 - 04.57	18/04/19 - 09.58	18/04/2019 09.58
Abul Ananda	Sydney Airport Corporation	T2 Screening	18/04/19 - 04:57	18/04/19 - 09:58	18/04/2019 09:58
Sugandha Sugandha	Sydney Airport Corporation	T2 Screening AMPM 1	18/04/19 - 04 51	18/04/19 - 09 57	18/04/2019 09 57



Shift Log:
20190418-0500-0900-BondiRWSINT

Commencement of Shift Log: 18 Apr 2019 04:55 AM
Completion of Shift Log: 18 Apr 2019 09:03 AM
Security Officer Name: Muhammad Majeed
Security Officer Security License Number: 000288842



Activity	Welfare check

Time	18/04/2019 09:03:43
Activity	Check Out

Signature	Muhammad Majeed	18/4/2019 09.03	Shahid

CERTIS

Annexure C

NOC training material and attendance sheets

CERTIS

SECURITY+

NOC Training Session
Attendance Management

April 2019

CERTIS

LEARNING OUTCOMES

❑ *Verify* the 3 Principals of Time and Attendance

❑ *Recall* the Security Industry Legislation (NSW) Section 35

❑ Detect fraud

❑ *Manage* fatigue

❑ *Follow* escalation process

❑ *Update:* BOSS Certis AU Vision and demo

CERTIS

Section 1:
The 3 Principals of Time and Attendance

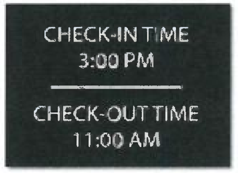
Verification of (W-W-W):

1. (Who?) Personnel

The personnel rostered for the shift, is the person who is working the shift

2. (When?) Time

The time rostered to work the shift, is the time actually worked



CHECK-IN TIME
3:00 PM

CHECK-OUT TIME
11:00 AM

3. (Where?) Location

The personnel rostered to work the shift, is at the expected location

Section 1:
Security Industry Legislation (NSW) - Section 35

In NSW, we (the master licensee) are required to hold sign-on and sign-off records for the following activities that are carried out on a recurrent basis - guarding, crowd control, dog handling, and armed guarding; or where we provide 3 or more security officers for a shift.

The security officer is required to record their:

name

license number

time when they start the shift

time they finish the shift

signature or **other unique identifier** (when signing on and off). *Refer Next Slide*

CERTIS

Section 1:
Security Industry Legislation (NSW) - Section 35

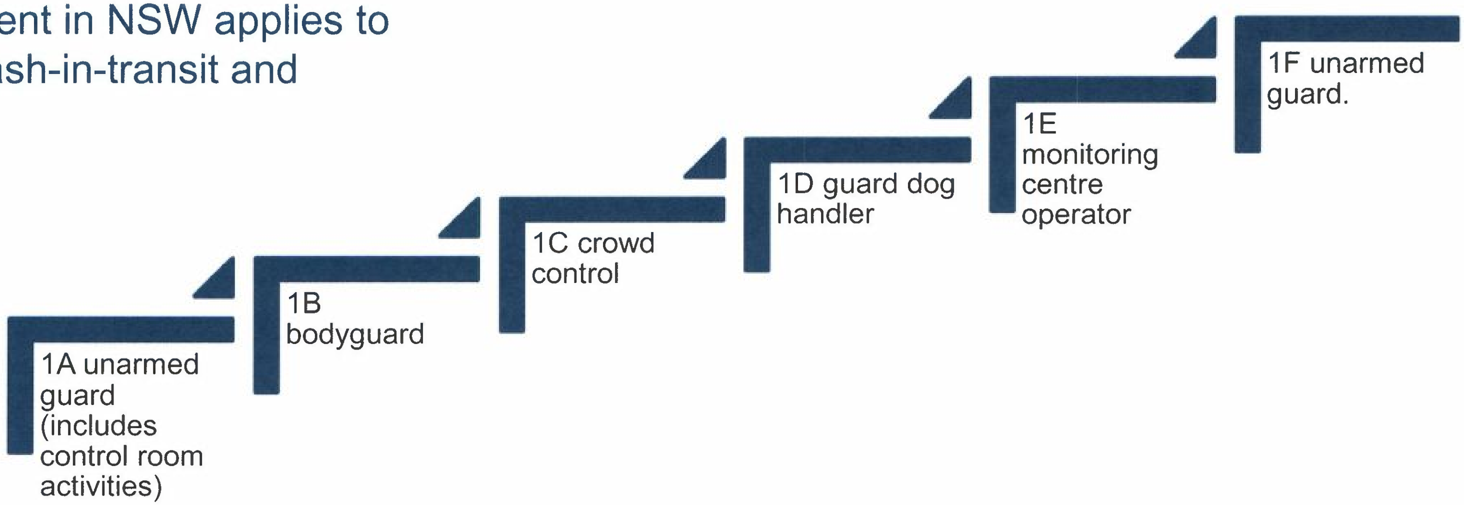
What about Electronic Time and Attendance?

- Electronic register - no requirement to also have a paper based/hard copy records
  - except for crowd control as liquor licensing requires a crowd control register to be held at the premises)
- We need to provide NSW police (licensing) or SLED auditors/compliance officers with records almost immediately
  - for example, if they attend a site we need to be able to immediately email or otherwise provide them with the sign-on and sign-off records for the site in question for the past 1 month (preferably 3 months).
- In most other states and territories, there is a similar requirement for crowd control activities.

Section 1:
Security Industry Legislation (NSW) - Section 35

All activities that the requirement applies to:

Sign-on and sign-off requirement in NSW applies to all class 1 licensees except cash-in-transit and patrols.



1A unarmed guard (includes control room activities)

1B bodyguard

1C crowd control

1D guard dog handler

1E monitoring centre operator

1F unarmed guard.

Section 3:
Fraud Detection - How to complete a Paper Timesheet

- ✓ All fields and sections of the timesheet **MUST** be completed, this includes Security Licence number, dates, times
- ✓ Use full legal name, no nicknames or preferred shorthand
- ✓ Clear notes and approval for any varied hours to planned
- ✓ Write information neatly and clearly, take care when completing forms by hand

Section 3:
Fraud Detection - How to complete a Paper Timesheet

- ✓ Liquid paper / whiteout is **NEVER** to be used on timesheets.
  - ✓ *Note….If an error is made, simply cross it out, initial the change and rewrite your information*

- ✓ At **NO** time should anyone sign on / off or alter another team member's information

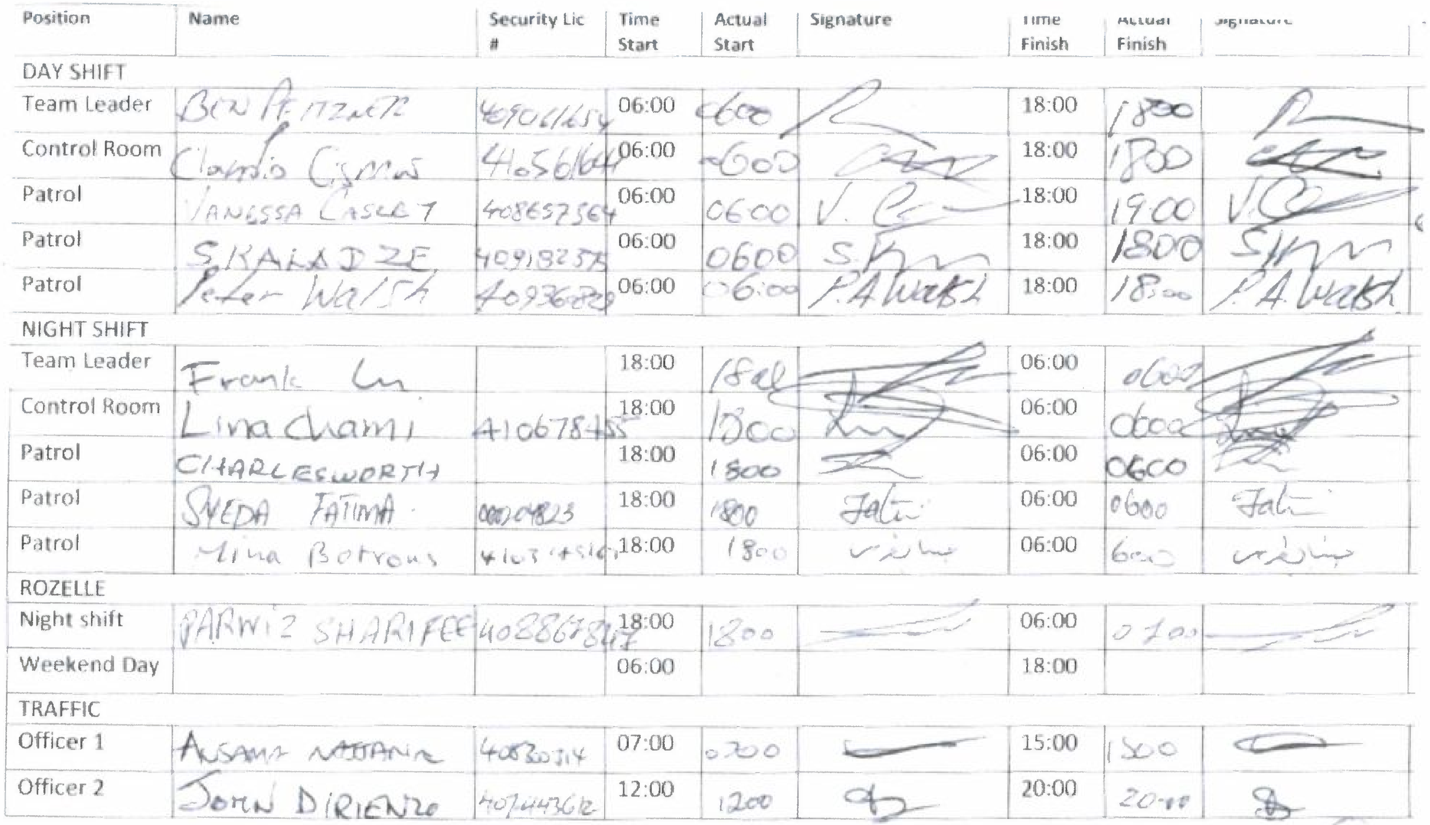
- ✓ Get the timesheet reviewed and signed off by a supervisor / senior officer.

- ✓ A Statutory Declaration will be required in the following circumstances before a shift will be paid:
  - fail to sign on / off,
  - All required fields of timesheet was not completed
  - Liquid Paper was used
  - Timesheet was not legible or
  - Any other questionable activity on the timesheet

CERTIS

Section 3:
Fraud Detection - Group Activity 1

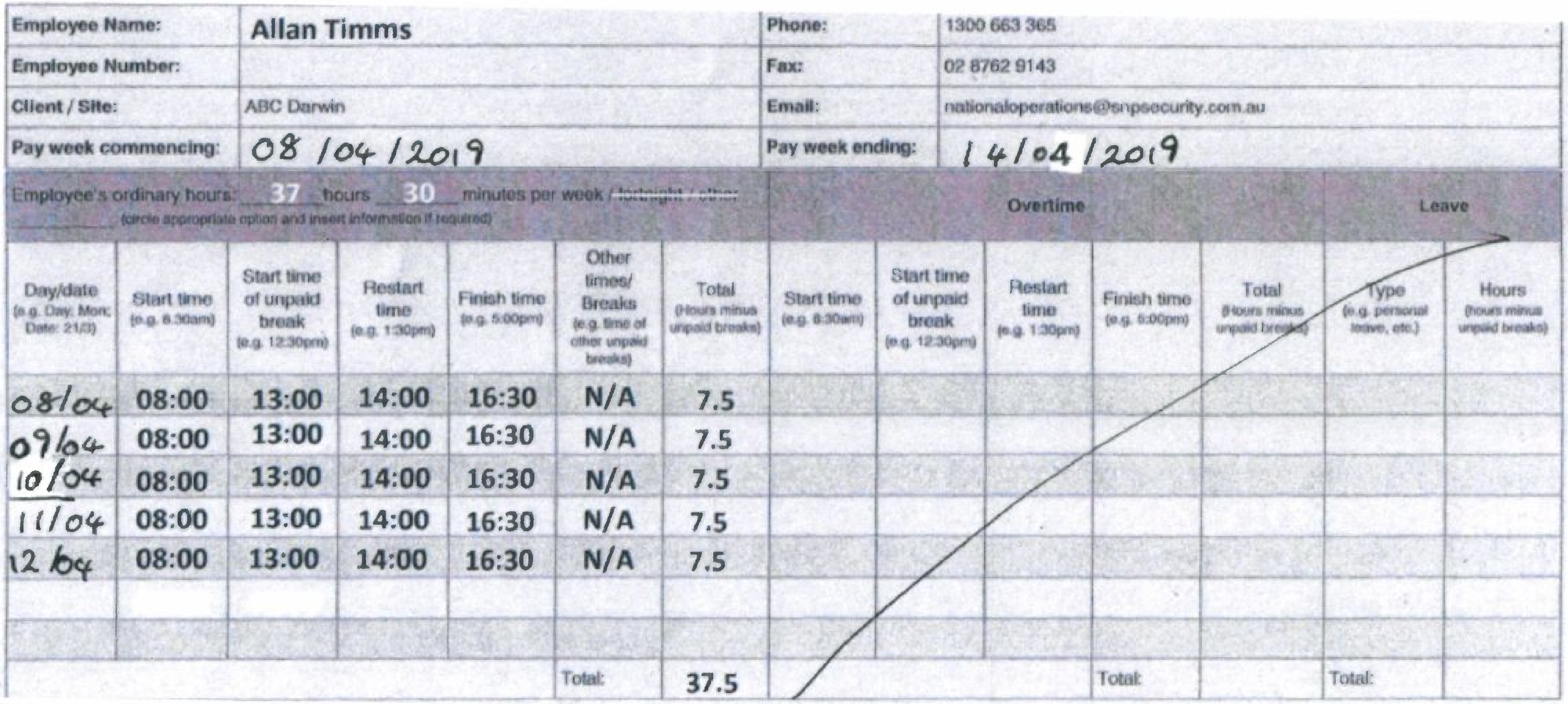
Question: What is wrong with this timesheet?



Position	Name	Security Lic #	Time Start	Actual Start	Signature	Time Finish	Actual Finish	Signature
DAY SHIFT								
Team Leader	BEN PETZNER	469011654	06:00	0600		18:00	1800	
Control Room	Claudio Cosmas	4056164	06:00	0600		18:00	1800	
Patrol	VANESSA CASLEY	408657564	06:00	0600	V. C	18:00	1900	V.C
Patrol	SKALADZE	409182375	06:00	0600	S.K	18:00	1800	SK
Patrol	Peter Walsh	40936829	06:00	06:00	P.A Walsh	18:00	18:00	P.A Walsh
NIGHT SHIFT								
Team Leader	Frank Lu		18:00	1800		06:00	0600	
Control Room	Lina chami	41067845	18:00	1800		06:00	0600	
Patrol	CHARLESWORTH		18:00	1800		06:00	0600	
Patrol	SYEDA FATIMA	00004823	18:00	1800	Fati	06:00	0600	Fati
Patrol	Mina Botrous	410314516	18:00	1800	مينا بطرس	06:00	600	مينا بطرس
ROZELLE								
Night shift	PARWIZ SHARIFEE	408867817	18:00	1800		06:00	0700	
Weekend Day			06:00			18:00		
TRAFFIC								
Officer 1	AUSAMA NAJJAR	40830314	07:00	0700		15:00	1500	
Officer 2	JOHN DIRIENZO	40744362	12:00	1200		20:00	20:00	

Section 3:
Fraud Detection - Group Activity 2

Question: What is wrong with this timesheet?

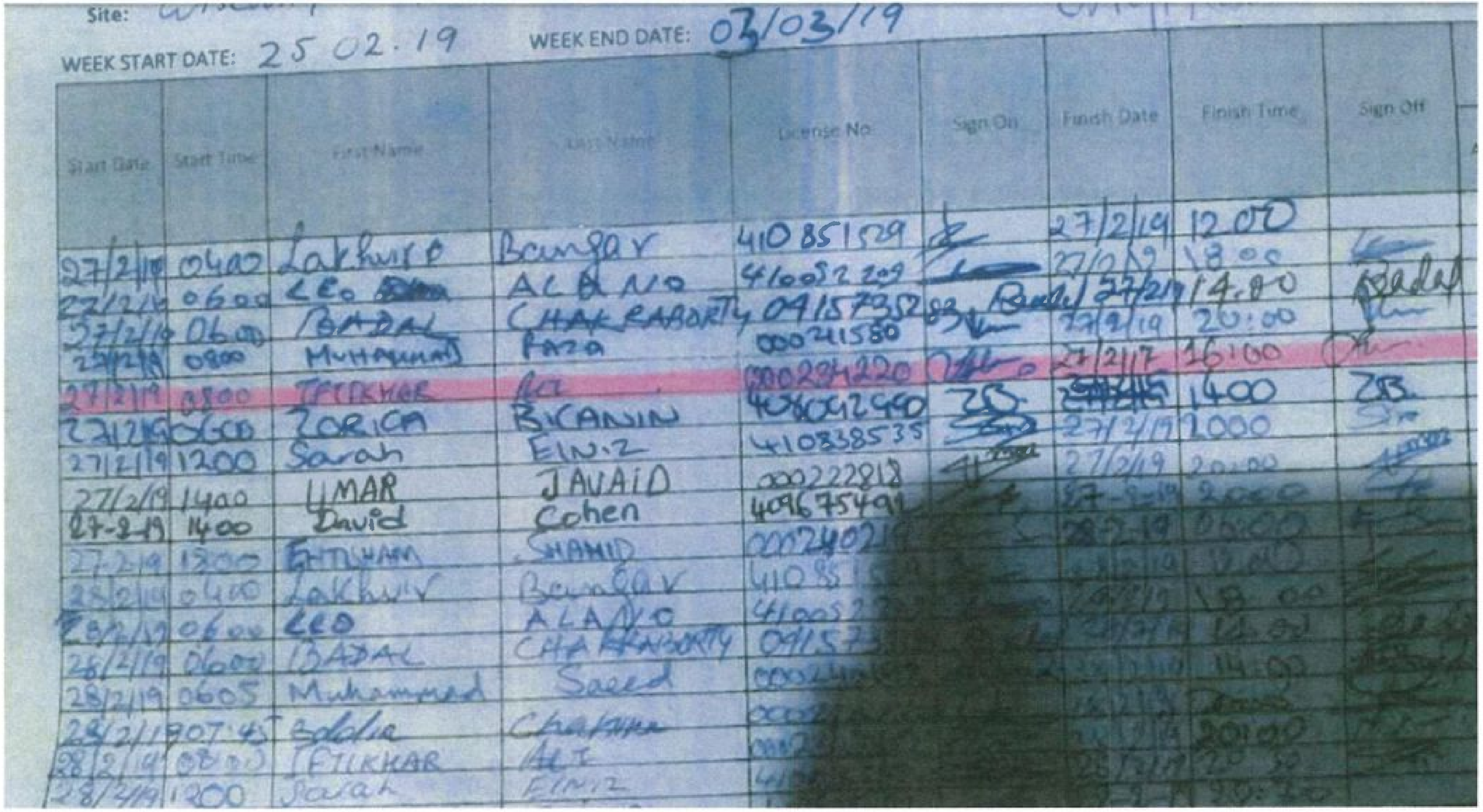


Employee Name:	Allan Timms	**Phone:**	1300 663 365
Employee Number:		**Fax:**	02 8762 9143
Client / Site:	ABC Darwin	**Email:**	nationaloperations@snpsecurity.com.au
Pay week commencing:	08 /04 /2019	**Pay week ending:**	14/04 /2019

Employee's ordinary hours: 37 hours 30 minutes per week / ~~fortnight / other~~ ______ (circle appropriate option and insert information if required)							Overtime					Leave	
Day/date (e.g. Day: Mon; Date: 21/3)	Start time (e.g. 8:30am)	Start time of unpaid break (e.g. 12:30pm)	Restart time (e.g. 1:30pm)	Finish time (e.g. 5:00pm)	Other times/ Breaks (e.g. time of other unpaid breaks)	Total (Hours minus unpaid breaks)	Start time (e.g. 8:30am)	Start time of unpaid break (e.g. 12:30pm)	Restart time (e.g. 1:30pm)	Finish time (e.g. 5:00pm)	Total (Hours minus unpaid breaks)	Type (e.g. personal leave, etc.)	Hours (hours minus unpaid breaks)
08/04	08:00	13:00	14:00	16:30	N/A	7.5							
09/04	08:00	13:00	14:00	16:30	N/A	7.5							
10/04	08:00	13:00	14:00	16:30	N/A	7.5							
11/04	08:00	13:00	14:00	16:30	N/A	7.5							
12/04	08:00	13:00	14:00	16:30	N/A	7.5							
					Total:	37.5				Total:		Total:	

Section 3:
Fraud Detection - Group Activity 3

Question: What is wrong with this timesheet?



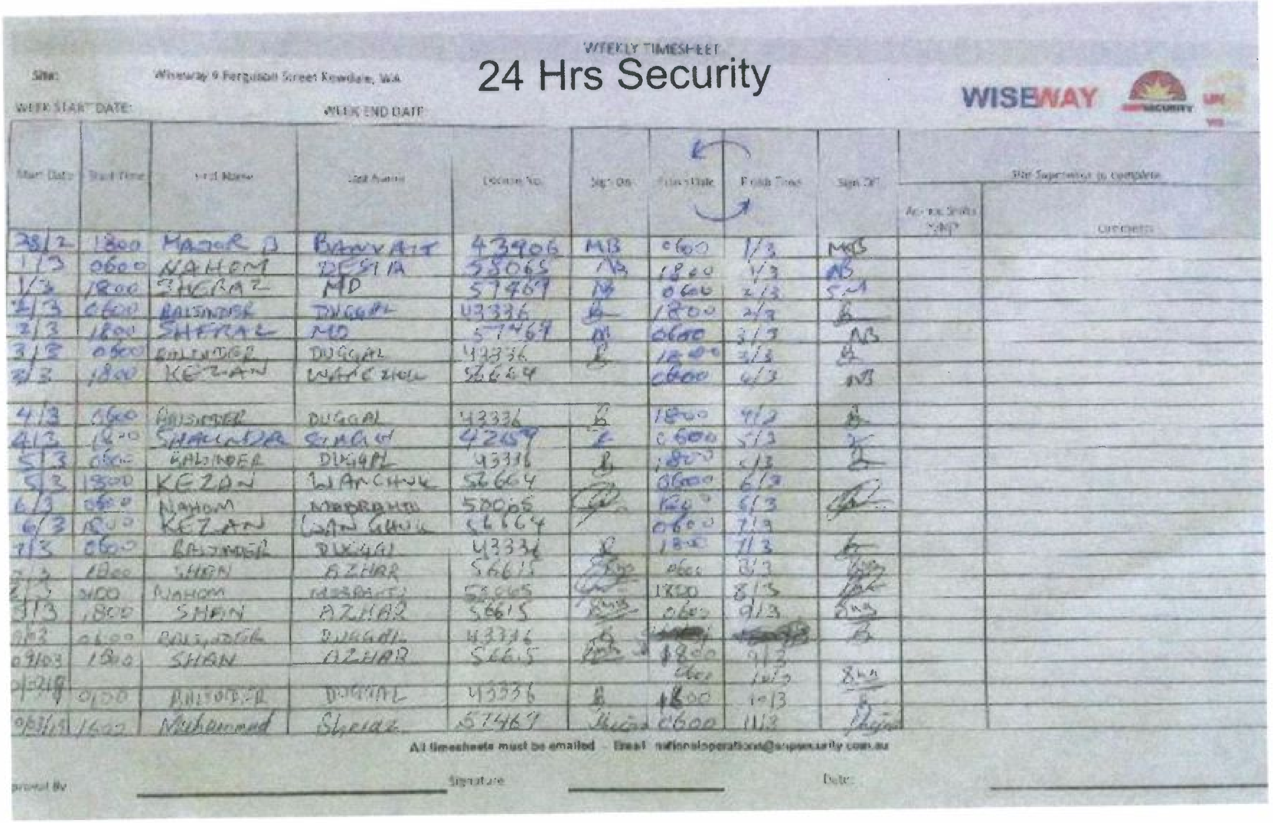
Site: [illegible]

WEEK START DATE: 25.02.19 WEEK END DATE: 03/03/19

Start Date	Start Time	First Name	Last Name	License No	Sign On	Finish Date	Finish Time	Sign Off
27/2/19	0400	Lakhvir	Bangar	410851529		27/2/19	12.00	
27/2/19	0600	LEO	ALANO	410052209		27/2/19	18.00	
27/2/19	0600	BADAL	CHAKRABORTY	0915735282	Badal	27/2/19	14.00	Badal
27/2/19	0800	MUHAMMAD	RAZA	000241580		27/2/19	20:00	
27/2/19	0800	IFTIKHAR	Ali	000284220		27/2/17	16:00	
27/2/19	0600	ZORICA	BICANIN	4080092990	ZB	[illegible]	1400	ZB
27/2/19	1200	Sarah	EINIZ	410838535		27/2/19	2000	
27/2/19	1400	UMAR	JAVAID	000222818		27/2/19	20:00	
27-2-19	1400	David	Cohen	409675491		27-2-19	2000	
27-2-19	1300	EHTISHAM	SHAHID	00024021[illegible]		28-2-19	06:00	
28/2/19	0400	Lakhvir	Bangar	41085[illegible]		[illegible]	12.00	
28/2/19	0600	LEO	ALANO	41005[illegible]		[illegible]	18.00	
26/2/19	0600	BADAL	CHAKRABORTY	09157[illegible]		[illegible]	14.00	
28/2/19	0605	Muhammad	Saeed	00024[illegible]		[illegible]	14.00	
28/2/19	07:45	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	
28/2/19	0800	IFTIKHAR	ALI	[illegible]		[illegible]	20:00	
28/2/19	1200	Sarah	EINIZ	[illegible]		28/2/19	20:30	
						[illegible]	20:00	

Section 3: Fraud Detection - Group Activity 4

Question: What is wrong with this timesheet?



WEEKLY TIMESHEET

24 Hrs Security

Site: Wiseway 9 Ferguson Street Kewdale, WA

WEEK START DATE: WEEK END DATE:

Start Date	Start Time	First Name	Last Name	Licence No.	Sign On	Finish Date	Finish Time	Sign Off	Actual Shifts Y/N?	Comments
28/2	1800	MAJOR B	BANYAIT	43906	MB	0600	1/3	MB		
1/3	0600	NAHOM	DESTA	58065	NB	1800	1/3	NB		
1/3	1800	SHERAZ	MD	57469		0600	2/3	SM		
2/3	0600	BALJINDER	DUGGAL	43336		1800	2/3			
2/3	1800	SHERAZ	MD	57469		0600	3/3	NB		
3/3	0600	BALJINDER	DUGGAL	43336		1800	3/3			
3/3	1800	KEZAN	WANGCHUK	56664		0600	4/3	NB		
4/3	0600	BALJINDER	DUGGAL	43336		1800	4/3			
4/3	1800	SHAMINDER	SINGH	42159		0600	5/3			
5/3	0600	BALJINDER	DUGGAL	43336		1800	5/3			
5/3	1800	KEZAN	WANGCHUK	56664		0600	6/3			
6/3	0600	NAHOM	MEBRAHTU	58065		1800	6/3			
6/3	1800	KEZAN	WANGCHUK	56664		0600	7/3			
7/3	0600	BALJINDER	DUGGAL	43336		1800	7/3			
7/3	1800	SHAN	AZHAR	56615		0600	8/3			
8/3	0600	NAHOM	MEBRAHTU	58065		1800	8/3			
8/3	1800	SHAN	AZHAR	56615		0600	9/3	Shan		
9/3	0600	BALJINDER	DUGGAL	43336						
09/03	1800	SHAN	AZHAR	56615		1800 0600	9/3 10/3	Shan		
10/3/19	0600	BALJINDER	DUGGAL	43336		1800	10/3			
10/3/19	1600	Muhammad	Sheraz	57469	Sheraz	0600	11/3	Sheraz		

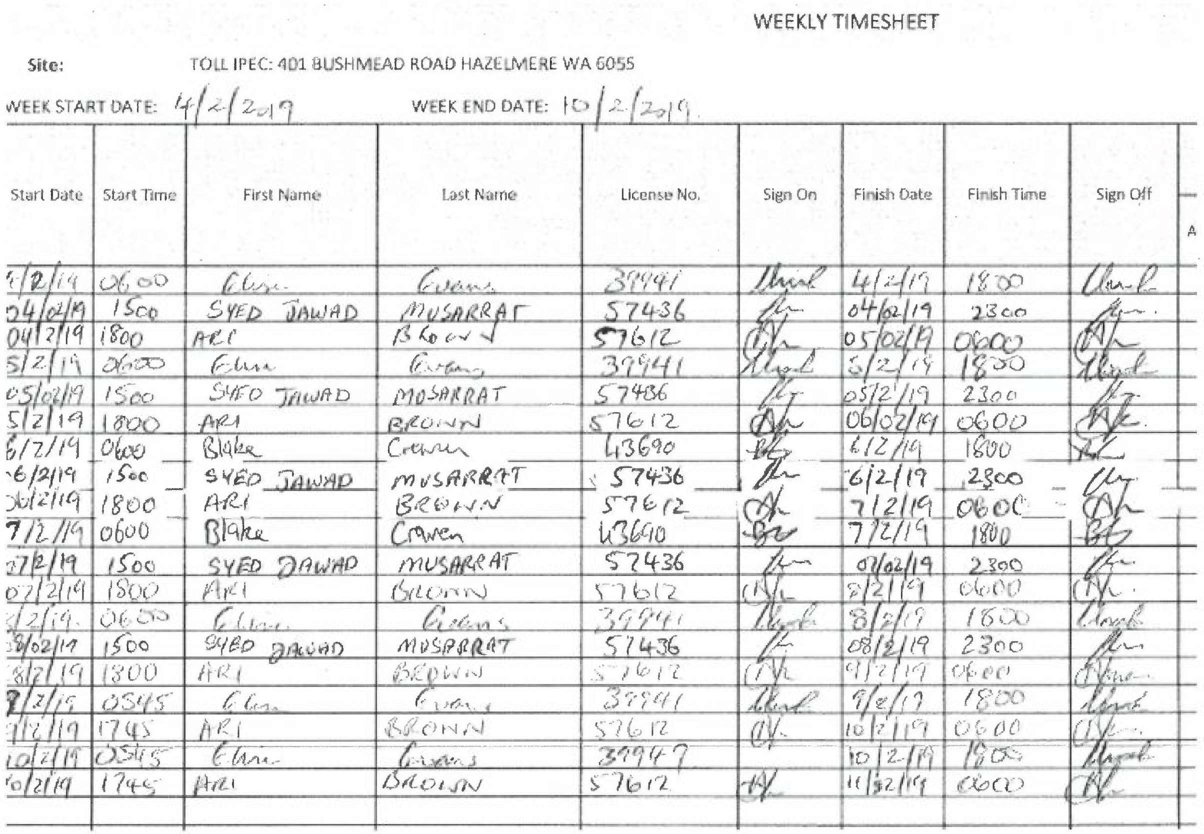
Site Supervisor to complete

All timesheets must be emailed - Email: nationaloperations@snpsecurity.com.au

Approved By ______ Signature ______ Date: ______

Section 3:
Fraud Detection - Group Activity 5

Question: What is wrong with this timesheet?



WEEKLY TIMESHEET

Site: TOLL IPEC: 401 BUSHMEAD ROAD HAZELMERE WA 6055

WEEK START DATE: 4/2/2019 WEEK END DATE: 10/2/2019.

Start Date	Start Time	First Name	Last Name	License No.	Sign On	Finish Date	Finish Time	Sign Off
4/2/19	0600	Elvin	Evans	39941		4/2/19	1800	
04/02/19	1500	SYED JAWAD	MUSARRAT	57436		04/02/19	2300	
04/2/19	1800	ARI	Brown ✓	57612		05/02/19	0600	
5/2/19	0600	Elvin	Evans	39941		5/2/19	1800	
05/02/19	1500	SYED JAWAD	MUSARRAT	57436		05/2/19	2300	
5/2/19	1800	ARI	BROWN	57612		06/02/19	0600	
6/2/19	0600	Blake	Craven	43690		6/2/19	1800	
6/2/19	1500	SYED JAWAD	MUSARRAT	57436		6/2/19	2300	
06/2/19	1800	ARI	BROWN	57612		7/2/19	0600	
7/2/19	0600	Blake	Craven	43690		7/2/19	1800	
07/2/19	1500	SYED JAWAD	MUSARRAT	57436		07/02/19	2300	
07/2/19	1800	ARI	BROWN	57612		8/2/19	0600	
8/2/19.	0600	Elvin	Evans	39941		8/2/19	1800	
08/02/19	1500	SYED JAWAD	MUSARRAT	57436		08/2/19	2300	
8/2/19	1800	ARI	BROWN	57612		9/2/19	0600	
9/2/19	0545	Elvin	Evans	39941		9/2/19	1800	
9/2/19	1745	ARI	BROWN	57612		10/2/19	0600	
10/2/19	0545	Elvin	Evans	39947		10/2/19	1800	
10/2/19	1745	ARI	BROWN	57612		11/2/19	0600	

CERTIS

Section 4:
Manage Fatigue - Fatigue Guidelines

These 2 limits have to be read in conjunction:
7days * 12hr shifts = 84hrs per week (Breach)
7 days * 6hr shifts = 42hrs per week (No Breach)

- Limit of 60 hours per worker per week **and**
- Limit of 7 days consecutive work
  - *In exceptional circumstances where consecutive days will be exceeded, complete a Risk Assessment form and seek approval from NOC Manager*
- Limit of 12 hours per **rostered** shift
- Limit of 14 hours total shift length after shift extensions
- Minimum of 8 hour gap between shifts

Section 4:
Manage Fatigue - Fatigue Breaches

Continued Fatigue breaches is not just a safety breach……

It may also be a sign of irregularities occurring on-site

CERTIS

Section 5:
Follow Escalation Process

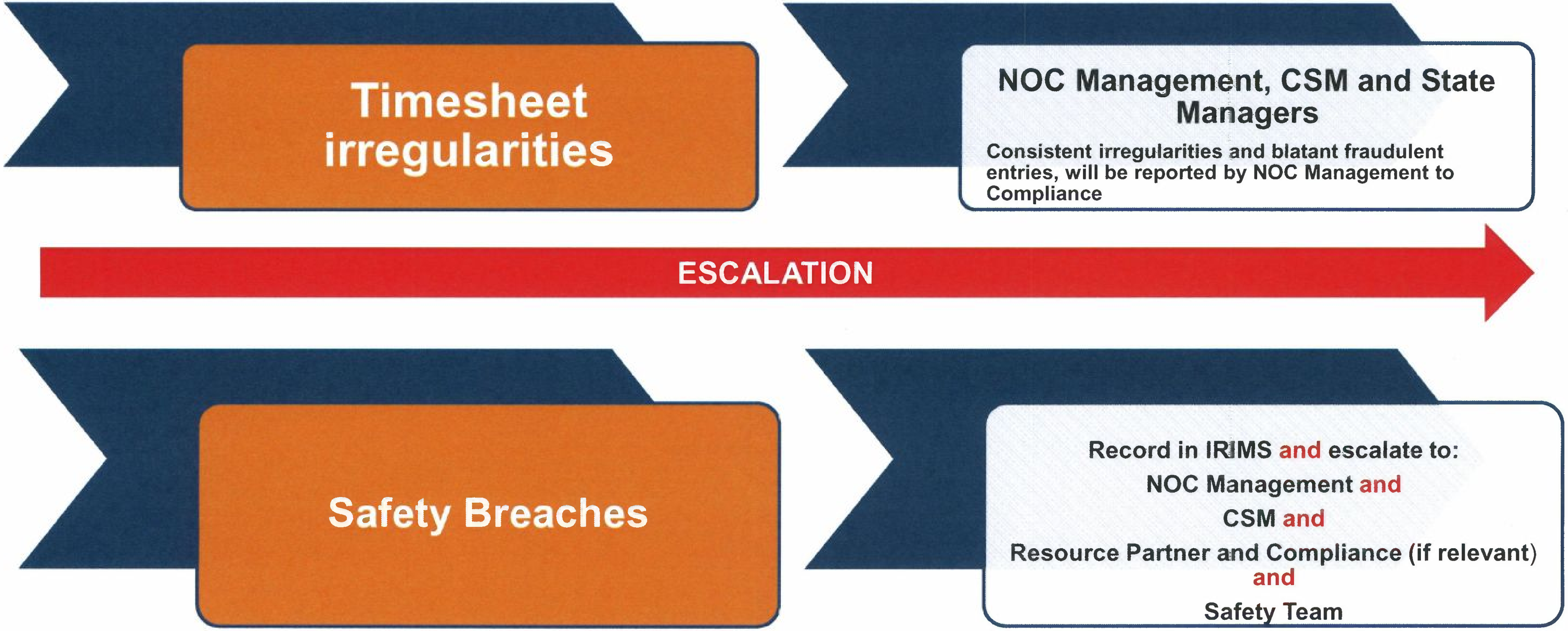
- ❖ IF IT DOES NOT LOOK RIGHT

- ❖ IF IT DOES NOT FEEL RIGHT

IT IS <u>NOT</u> RIGHT – REPORT IT

CERTIS

Section 5: Follow Escalation Process



Timesheet irregularities

NOC Management, CSM and State Managers

Consistent irregularities and blatant fraudulent entries, will be reported by NOC Management to Compliance

ESCALATION

Safety Breaches

Record in IRIMS and escalate to:

NOC Management and

CSM and

Resource Partner and Compliance (if relevant) and

Safety Team

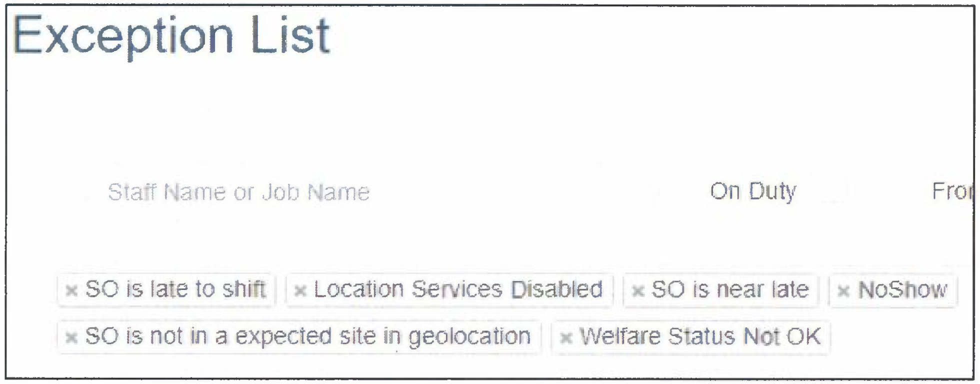
Section 6: Update
BOSS - Vision and Benefits

Certis Vision:
Aim is 100% roll out to all sites
BOSS Roll Out in stages

❑ Phase 1 – High Priority / High Risk (NSW Only)
❑ Phase 2 – Medium Priority (NSW Only)
❑ Phase 3 – All other States (not on this slide)

✓ BOSS communicates T&A in real time to the NOC
✓ BOSS supplies a geo-fenced location mark to ensure the guard is in the correct location
✓ BOSS will make all welfare checks, ensuring all guards get a check at the appropriate time
✓ BOSS is attached to compliance data, every guard has an individual account and password
✓ BOSS captures device and server time when clocking in/out to makes sure the correct time is always captured.

Section 6: Update BOSS demo



Exception List

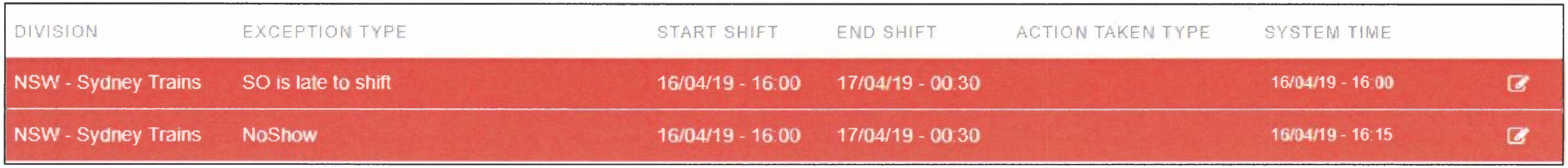
Staff Name or Job Name

On Duty

Fro

× SO is late to shift | × Location Services Disabled | × SO is near late | × NoShow

× SO is not in a expected site in geolocation | × Welfare Status Not OK



DIVISION	EXCEPTION TYPE	START SHIFT	END SHIFT	ACTION TAKEN TYPE	SYSTEM TIME	
NSW - Sydney Trains	SO is late to shift	16/04/19 - 16:00	17/04/19 - 00:30		16/04/19 - 16:00	✎
NSW - Sydney Trains	NoShow	16/04/19 - 16:00	17/04/19 - 00:30		16/04/19 - 16:15	✎

CERTIS

ATTENDANCE FORM

Training Session Name: NOC - Timesheet Processing Requirements.

First Name	Surname	Business Unit	Signature	Date
Tomas	Draper	Ops-Tech		17/4/19
Peter	DEAN	Nat ops		17/4/2019
PAUL	LIPSCOMB	NAT OPS.		17/4/19
HASHAM	JAMAL	NOC	Hasham	17/04/19
Shane	Moxham	NOC	S Moxham	17/4/19
Dee	Sluis	NCA Ops Admin		17.4.19
TASEEM Ahmed	Fateh	NOC		17.4.19.
Harris	Katsanis	NOC		"
Ilya	Baturin	NOC		17/4/19
OYTUN	GUNGOR		NOC.	17/4/19
MOSTAFA	HASSAN	NOC		17.04.19
Bill	Quadin	OPS		17.04.19
Saif	chahine	NOC		17.04.19
Kerryn	Frater -	NOC	KFrater.	17.04.19
William	Nixon	BRI Support		17 04 19
Peter	Hanna	NOC		17/4/19
Saila	Saipele	NOC		17.04.19

CERTIS

ATTENDANCE FORM

Training Session Name: REQUIREMENTS OF TIMESHEET PROCESSING (PAPER & ELECTRONIC)

First Name	Surname	Business Unit	Signature	Date
PAULA	BRUNO	MELB PSD		17/4/19
ROBERT	SYMONDS	"		18/04/19
Tony Pollard	POLLARD	'		17/4/19

CERTIS

ATTENDANCE FORM

Training Session Name: REQUIREMENTS OF TIMESHEET PROCESSING (PAPER & ELECTRONIC)

First Name	Surname	Business Unit	Signature	Date
PAULA	BRUNO	MELB PSO		17/4/19
ROBERT	SYMONDS	〃		18/04/19
Tony Pollard	POLLARD	〃		17/4/19

Re: NOC Training - PLEASE SIGN and send back to me

Phil Hart (AU)

Wed 17/04/2019 3:54 PM

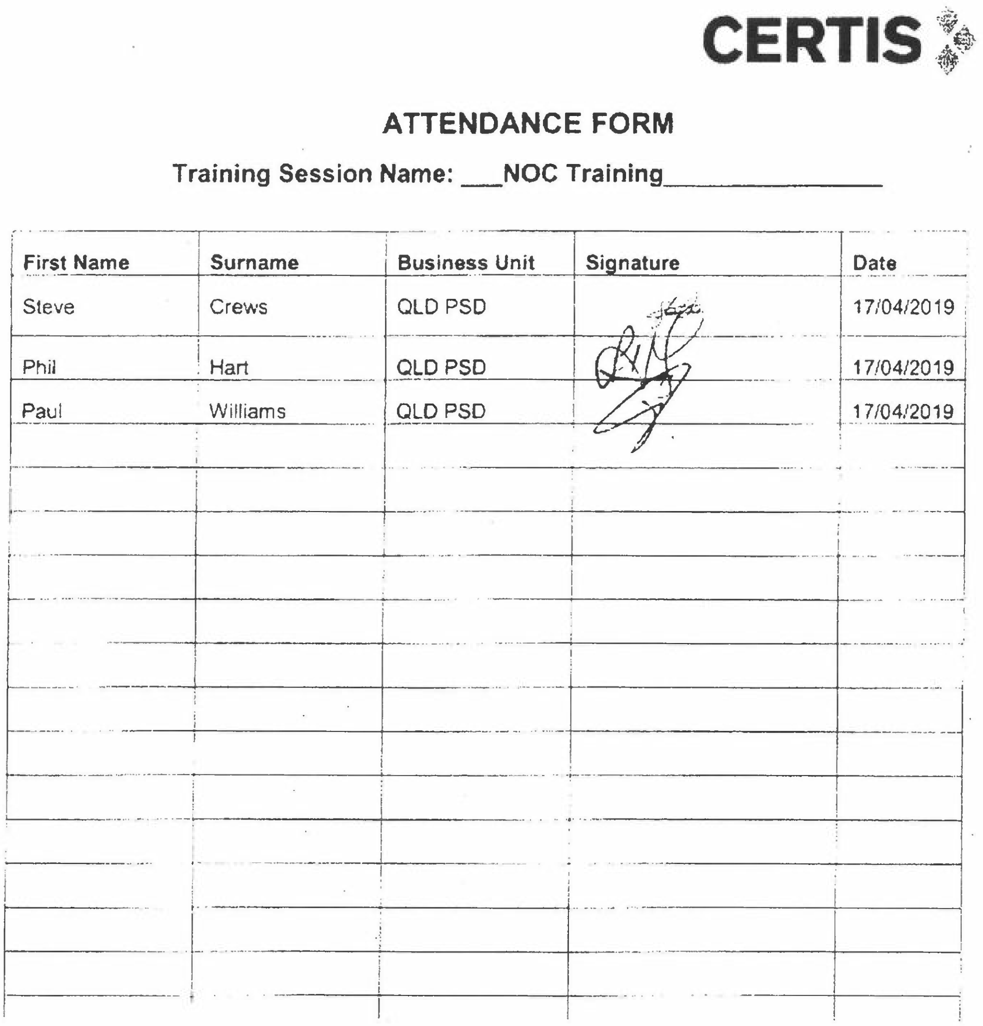
To: Linda Willard (AU) <lwillard@snpsecurity.com.au>; Stephen Mizzi (AU) <smizzi@brisecurity.com.au>; Paula Bruno (AU) <pbruno@snpsecurity.com.au>; Steven Crews (AU) <screws@snpsecurity.com.au>; Lisa Manning (AU) <LManning@snpsecurity.com.au>

Linda

Please see copied below, as requested

Regards

Phil



CERTIS

ATTENDANCE FORM

Training Session Name: ___NOC Training_______________

First Name	Surname	Business Unit	Signature	Date
Steve	Crews	QLD PSD		17/04/2019
Phil	Hart	QLD PSD		17/04/2019
Paul	Williams	QLD PSD		17/04/2019

CERTIS

Certis Australia operating companies

SNPSECURITY

BRISECURITY

Phillip Hart
Client Services Manager - Protective Services
Branch Office

D +61 7 3861 3652 | M +61 4 3940 2655

E phart@snpsecurity.com.au

W www.certisgroup.com, www.snpsecurity.com.au, www.brisecurity.com.au

CERTIS

ATTENDANCE FORM

Training Session Name: Timesheet Processing (paper/electronic)

First Name	Surname	Business Unit	Signature	Date
Lisa	Manning	PSD		17-4.19
MATTHEW	LEWSAM	PSD		17/4/19

CERTIS

ATTENDANCE FORM

Training Session Name: NOC Training (Timesheet)

First Name	Surname	Business Unit	Signature	Date
Belal	Abdelaal			23/4
Rob	Hensen			23/4
STEVE	NOLANI			23/4-
Soner	Inan			23/4.
Paul	Tamos			23/4/19
Moneer	Howari			23/4/19
Kamran	Mohammed			23/4/19

CERTIS

ATTENDANCE FORM

Training Session Name: NOC Training (Timesheets)

First Name	Surname	Business Unit	Signature	Date
Craig	Maher	PS		23/4
Jo	Dos Santos	PS		23/4
Craig	Car.	PS		23/4
Alexander	Rusa.	PS		23/4
Allan	Cooper	PS		23/4
Tyrone	Tipler.	PS		

Site managers
dial in remotely
from sites/home

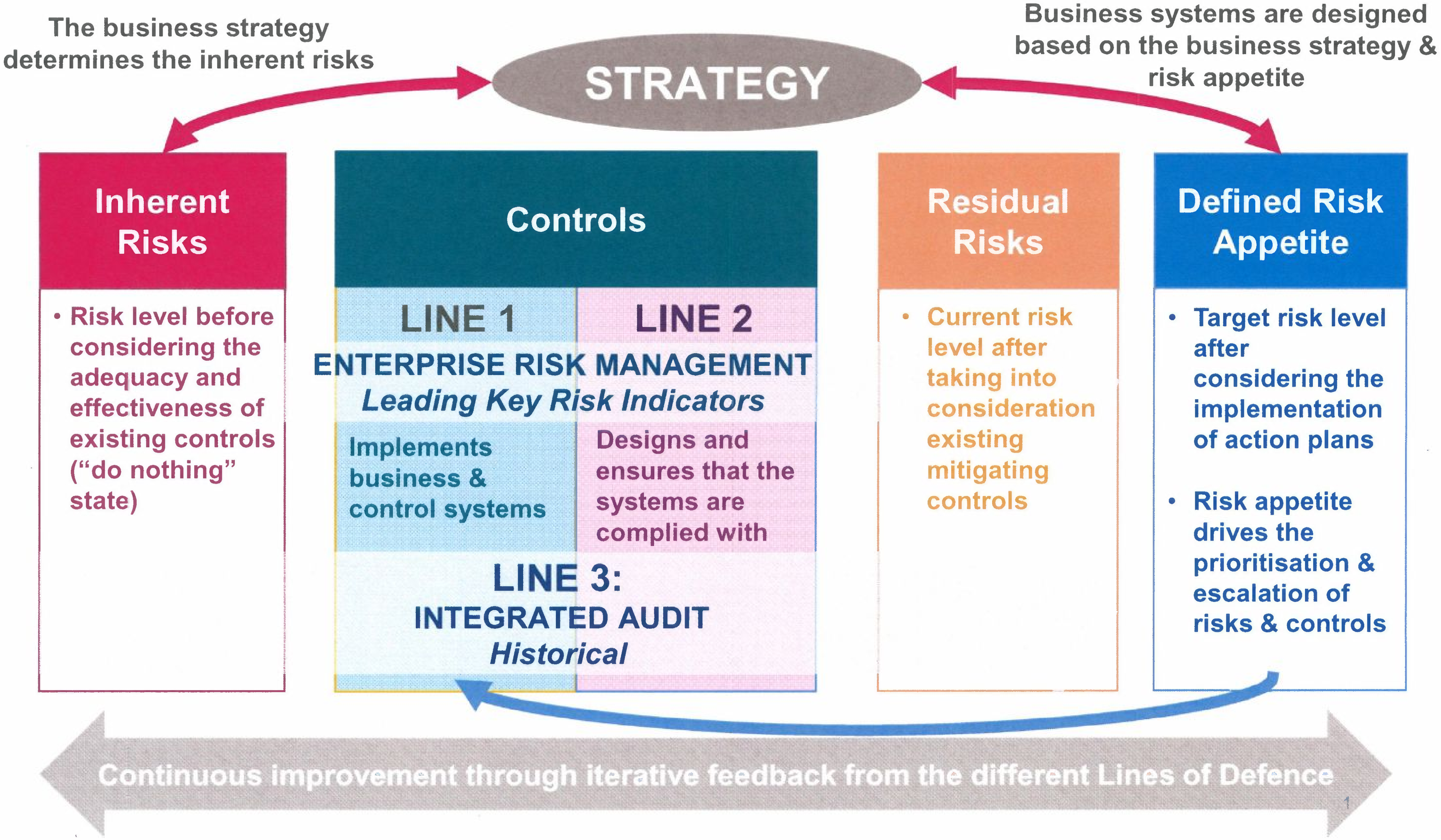
23/4/19

Linda Willard

Annexure D

Diagrammatic representation of the IAF

Integrated Assurance Framework



The business strategy determines the inherent risks

STRATEGY

Business systems are designed based on the business strategy & risk appetite

Inherent Risks

- Risk level before considering the adequacy and effectiveness of existing controls (“do nothing” state)

Controls

LINE 1

LINE 2

ENTERPRISE RISK MANAGEMENT

Leading Key Risk Indicators

Implements business & control systems

Designs and ensures that the systems are complied with

LINE 3:

INTEGRATED AUDIT

Historical

Residual Risks

- Current risk level after taking into consideration existing mitigating controls

Defined Risk Appetite

- Target risk level after considering the implementation of action plans
- Risk appetite drives the prioritisation & escalation of risks & controls

Continuous improvement through iterative feedback from the different Lines of Defence