APPENDICES

APPENDIX A: INITIAL VERSION OF UITCM/ COMPONENTS DESCRIPTION

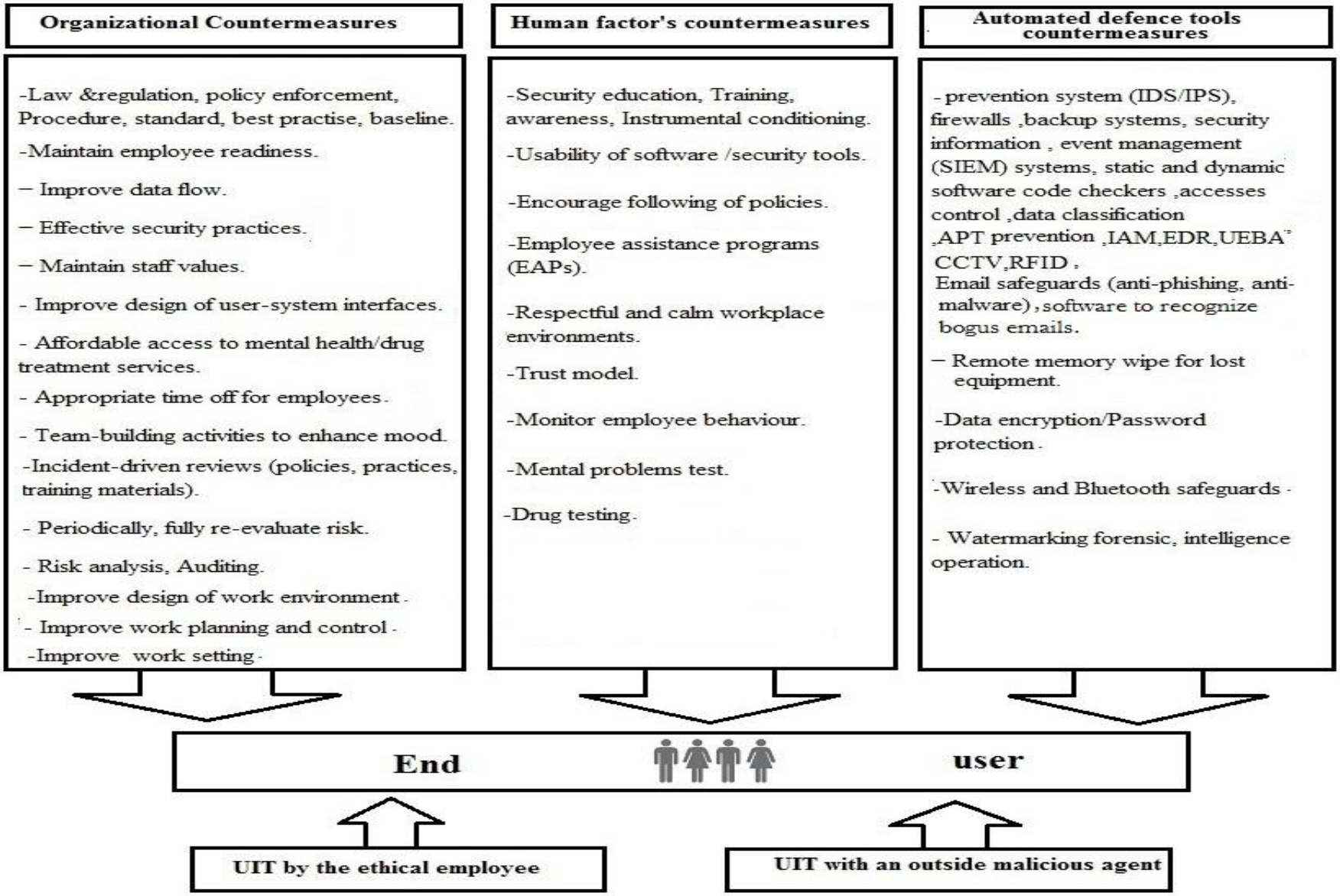


Figure 1: Initial Version of UIT Countermeasure Model (UITCM)

Table 1: The Organizational Countermeasures

UITCM		
The Organizational Countermeasures Components Group		
ID	**Component**	**Definition**
OC01	-Law &regulation, policy enforcement, Procedure, standard, best practice, baseline.	•Policies are the top tier of formalized security documents. These high-level documents offer a general statement about the organization's assets and what level of protection they should have. Well-written policies should spell out who's responsible for security, what needs to be protected, and what is an acceptable level of risk. They are much like a strategic plan because they outline what should be done but don't specifically dictate how to accomplish the stated goals. Those decisions are left for standards, baselines, and procedures, and implementing security best practices throughout the organization, as defined by widely tested and implemented security norms in the industry. Law &regulation, policy enforcement, Procedure, standard, best practice and baseline must take UITs in consideration.
OC02	-Maintain employee readiness.	• Implementing practices that reduceinattention, stress and anxiety, fatigue and boredom, and illness and injury and enhance awareness of drug and hormone side effects.
OC03	- Improve data flow.	• Improve data flow by enhancing communication and maintaining accurateprocedures and directions and the exchange of messages and data and ideas between people inside and outside of the organization, communication can be used to enhance information security awareness and motivate employees to comply with security policy. At the same time, if communication goes wrong or is misused, the outcome could damage the information security system. Management is required to communicate effectively with employees to ensure that they are aware of information security policy and understand thereasons for its effective implementation.
OC04	- Effective security practices.	• Provide effective security practices (e.g., two-way authentication for access).
OC05	- Maintain staff values.	• Maintain staff values and attitudes that align with organizational mission and ethics, establish good relationships in the workplace, encourage the development of positive relationships between managers and employees as well as amongst coworkers, setting clear goals, communicate effectively with employees, showing appreciation ,building a strong team, sending a clear message, improving the openness at work, improving the behaviour of the individuals in an organization, getting beyond the, negative with staff development and, creating open communication in the workplace.
OC06	- Improve design of user-system interfaces.	• Improve design of user-system interfaces to lower risk of errors, so that user interface design easy, putting users in control of the interface, and error prevention etc.
OC07	- Affordable access to mental health/drug treatment services.	• Ensure that employees have affordable accessto mental health services, including drugtreatment and provide adequate health insurance benefits for mental health care/Adequate health insurance for mental health care.

OC08	- Appropriate time off foremployees.	• Provide appropriate time off for employeesto find a balance between work and home life.
OC9	- Team-building activities toenhance mood.	• Promote team-building activities and social interactions among employees to enhancemood.
OC10	-Incident-driven reviews (policies, practices, training materials).	• Conduct incident-driven reviews of policies, practices, processes, and training materials, by reactive approach that focuses on quick response.
OC11	- Periodically, fully re-evaluate risk.	• Periodically, fully re-evaluating risk to avoid the effects of lowered perceived risk threshold accumulated over time, while many of the risks associated with information security are of a cumulative nature. This means that the likelihood of an event occurring on a given day or at a given time might be extremely small, but over time, this chance increases.
OC12	- Risk analysis, Auditing.	• Apply risk management and measurement and analysis concepts and approaches to critical business processes to ensure they are providing the intended results, with periodic and incident-driven review, maintain records of reviews.
OC13	- Improve design of workenvironment.	• Poor design and layout of workplaces must beseen as a causal factor to Physical discomfort which has been shown to be associated with human error, work environment includes such factors as noise, lighting and temperature, workspace arrangement, and facility layout and arrangement, , specifically in terms of how environmental factors contribute to human performance . The concerns for environmental interfaces are that they induce fatigue and/or distract attention from the primary task, resulting in increased potential for human error.
OC14	- Improve work planningand control.	• Job pressure, poor job rotation, time factors, task difficulty, change in routine, poor task planning or management practice, lack of knowledge ,skills and ability must be seen as a causal factor which has been shown to be associated with human error and must be improved.
OC15	-Improve work setting.	• Distractions, insufficient resources, poormanagement systems, inadequate security practices, and poor work flow must be seen as a causal factor which has been shown to be associated with human error and must be improved.

Table 2: The Human factor's countermeasures

UITCM		
The Human factor's countermeasures Components Group		
ID	**Component**	**Definition**
HC01	- Security education, Training, awareness, Instrumental conditioning.	• Enhance awareness of insider threat and unintentional insider threat, heighten motivation to be wary of insider threat risks, recognizing phishing and other social media threat vectors, Keep employees abreast of latest attack vectors and other threat-related news, train continuously to maintain proper level of knowledge, skills, and ability, conduct training and awareness on risk perception, and cognitive biases that affect decision making, conduct frequent training and awareness programs. • Instrumental conditioning refers to learning through consequences; the main idea of instrumental conditioning is that a system user's behaviour that produces theseresearchers used an imaginary case to demonstrate that designing good security policies can be enhanced by use of system dynamics.
HC02	-Usability of software /security tools.	• Improve usability of security tools; improve usability of software to reduce likelihoodof system-induced humanerror.
HC03	-Encourage following of policies.	• Reward and punishment policy, enforce penalties for non compliance, provide compliance incentives.
HC04	-Employee assistance programs (EAPs).	• Provide employee assistance programs (EAPs) to help employees reduce outsidestresses, which may cause mind wandering • An Employee Assistance Program (EAP) is a voluntary, work-based program that offers free and confidential assessments, short-term counseling, referrals, and follow-up services to employees who have personal and/or work-related problems. EAPs address a broad and complex body of issues affecting mental and emotional well-being, such as alcohol and other substance abuse, stress, grief, family problems, and psychological disorders. EAP counselors also work in a consultative role with managers and supervisors to address employee and organizational challenges and needs.
HC05	- Respectful and calm workplace environment.	• Provide workplace environment programs thatenhance respectful and calm environments.
HC06	-Trust model.	• Define specific tasks for each employee and segregate duties.
HC07	-Monitor employee behavior.	• The UIT factors might be recognized or inferred through monitoring and surveillance methods (perhaps including, in some cases, linguistic analysis performed on samples of monitored electronic communications), employee monitoring can be subject to a variety of laws and possible legal constraints or boundaries, for example, identifying perceived risk threshold under some circumstances may be considered mental health testing, laws would apply which could limit testing and responses.
HC08	-Mental problems test.	• Conduct mental problems test (within restrictions).
HC09	-Drug testing.	• Conduct drug testing (withinrestrictions).

Table 3: The Automated defence tools

UITCM		
The Automated Defence tools Countermeasures Components Group		
ID	**Component**	**Definition**
AC01	- Standard systems (antivirus ,anti-malware, intrusion detection and prevention system (IDS/IPS), firewalls ,backup systems, security information and event management (SIEM) systems, static and dynamic software code checkers ,accesses control ,data classification, APT prevention, IAM, EDR, UEBA,CCTV,RFID,DLP, Email safeguards anti-malware), software to recognize bogus emails.	• Employ automated tools to circumvent poor user decisions, such as developing software to better recognize threats in email messages, andDeploy data loss prevention (DLP)software to recognizepossible harmful sites,email practices, andother threats. • Use firewalls. • Use antivirus software. • Use anti-malware software. • Email safeguards (antiphishing, anti-malware) APT: advanced persistent threat prevention. •IAM :Identity AccessManagement •CCTV: Closed-circuittelevision. •RFID: Radio-frequencyidentification. •UEBA: User and entitybehaviour analytics. • EDR: Endpoint Detection and Response. • Intrusion detection andprevention system. (IDS/IPS), backup. • systems, securityinformation and event management (SIEM) systems, static anddynamic software code checkers, accessescontrol system and data classification etc.
AC02	- Remote memory wipe for lost equipment.	• Enable remote memory wipe for lost equipment.

AC03	-Data encryption/Password protection.	• Enable data encryptionon storage devices, Password protection onstorage devices.
AC04	-Wireless and Bluetooth safeguards.	•Enable wireless and Bluetooth safeguards(disable, protect).
AC05	-Watermarking forensic, intelligence operation.	• The main purpose of forensic watermarking is to protect the interests of content creators against illegal use and distribution of copyrighted digital works; they can make it easier for copyright holders to detect it and to identify people who engage in it. A forensic watermark can alert honest users when they have received illegitimate documents or programs. • Is the process by which organizations systematically collect and evaluate information for the purpose of discovering the potential threats to an organization in long-term. It relies on anticipating future behaviour and requires analysts with deep expertise, to understand and adapt to changes in the threats environment.
AC05	-Watermarking forensic, intelligence operation.	• The main purpose of forensic watermarking is to protect the interests of content creators against illegal use and distribution of copyrighted digital works; they can make it easier for copyright holders to detect it and to identify people who engage in it. A forensic watermark can alert honest users when they have received illegitimate documents or programs. • Is the process by which organizations systematically collect and evaluate information for the purpose of discovering the potential threats to an organization in long-term. It relies on anticipating future behaviour and requires analysts with deep expertise, to understand and adapt to changes in the threats environment.

APPENDIX B: UITs ONLINE QUESTIONNAIRE

Study of unintentional insider threats in Malaysian organizations

* Required Information

Participant's personal information: -

The goal of this section is to providing respondents' background information and experience

* 1.
1-Your gender

- ○ Male
- ○ Female

* 2.2- Your age

- ○ 20-30 years
- ○ 31-40 years
- ○ 41-50 years
- ○ 51-60 years
- ○ Above 60 years

* 3.3-How many total years of your Working experience in IT industry?

- ○ 1-5 years
- ○ 6-10 years
- ○ 11-15 years
- ○ 16-20 years
- ○ Above 20 years

* 4.4- Are you aware of unintentional insider threats?

- Yes
- No

* 5.5- Is your organization policy addressing the unintentional insider threats?

- Yes
- No

Identify the likelihood level of unintentional insider threats

The goal of this section of the questionnaire is investigating your opinions regarding the likelihood level of unintentional insider threats in your organization

Please determine ONLY one answer from the options that best describe your knowledge

* 6.1. How likely would the organization face unintentional insider threats?

Not likely Least likely Likely Very likely Most likely

0 1 2 3 4

* 7.2. How likely would employees accidentally jeopardizing security of organization through data leaks or similar errors?

Not likely Least likely Likely Very likely Most likely

0 1 2 3 4

* 8.3. How likely would similar organizations face unintentional insider threats?

Not likely Least likely Likely Very likely Most likely

0 1 2 3 4

✱ 9. 4. How likely would the organization not to face unintended insider threats?

Not likely Least likely Likely Very likely Most likely

0 1 2 3 4

✱ 10. 5. How likely would finding employees are not aware of unintended insider threats in the organization?

Not likely Least likely Likely Very likely Most likely

0 1 2 3 4

✱ 11. 6. How likely would employees unintentionally make mistakes affecting the information security of the organization?

Not likely Least likely Likely Very likely Most likely

0 1 2 3 4

Identify the Contributing Factors Of Unintentional Insider Threat

The goal of this section is to Identify the Contributing Factors Of Unintentional Insider Threat from the most significant to the least significant.

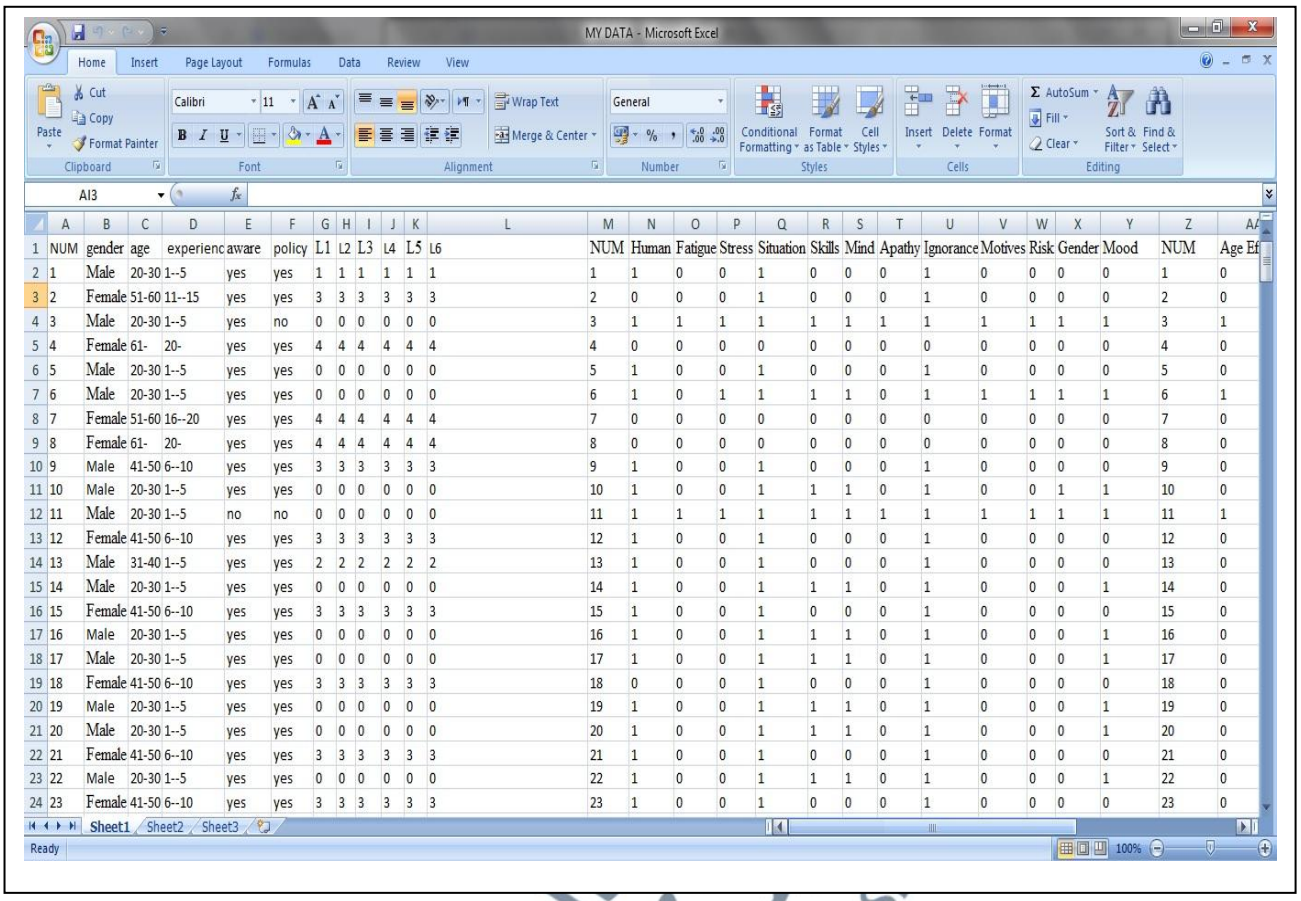
* 12.

Based on your knowledge ,which of the following options are the MOST Contributing factors of the Unintentional Insider Threat in Malaysian Organizations .

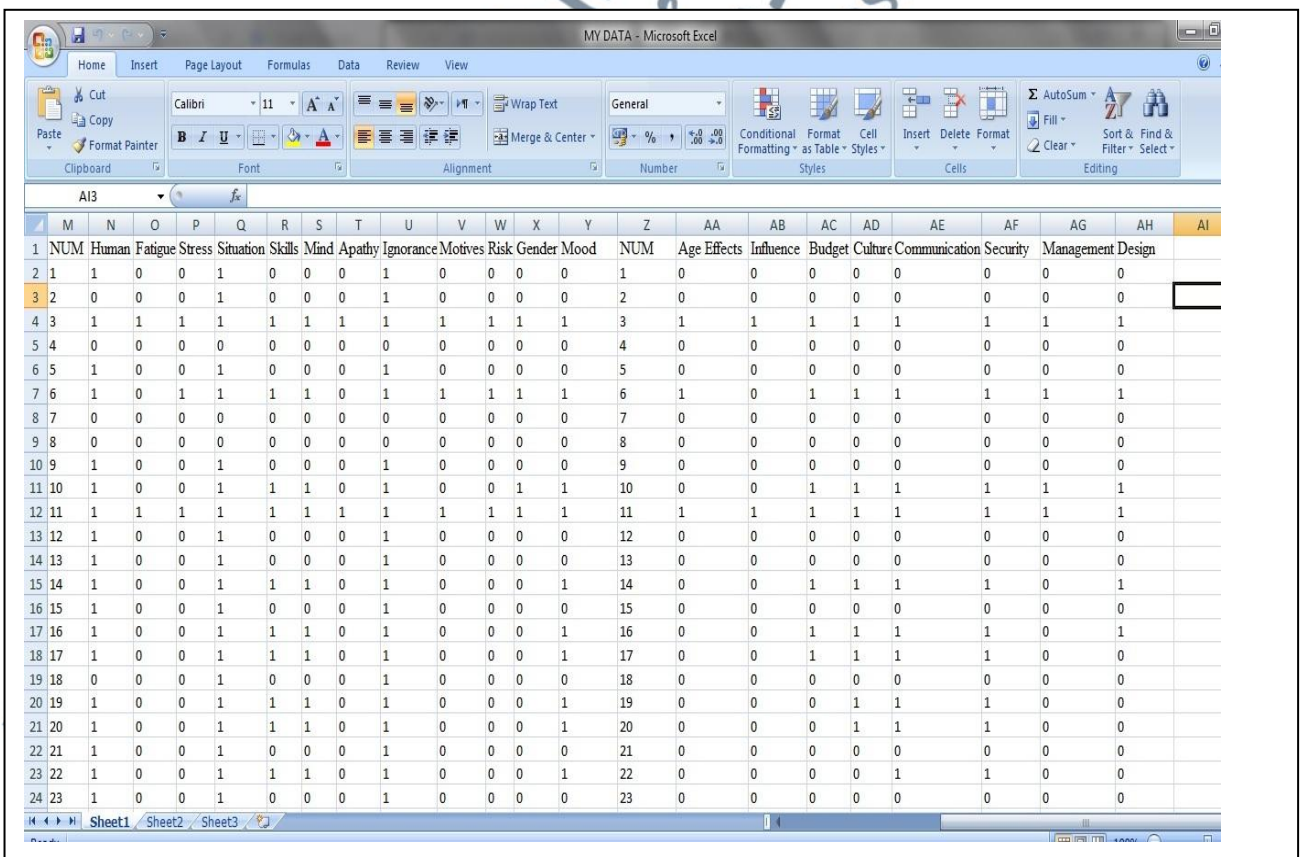
- [ ] Human Error ("I didn't mean to do that.")
- [ ] Fatigue And Sleepiness
- [ ] Stress And Subjective Mental Workload
- [ ] Situation Awareness ("I thought that's what I was supposed to do.")
- [ ] Skills And Experience of employees
- [ ] Mind Wandering ("I forgot to do that.")
- [ ] Apathy ("I don't care")
- [ ] Ignorance and negligence ("Nothing will happen")
- [ ] Motives and Incentive and Disincentive Policy
- [ ] Risk possibility as Personality feature (Recklessness)
- [ ] Gender (More likely to take risks, female/male)
- [ ] Mood (The influence of mood on making risky choices)
- [ ] Age Effects (More likely to take risks, young employees/ older employees)
- [ ] Influence of Drugs and Hormones
- [ ] Budget of organization
- [ ] Culture (Organizational culture)
- [ ] Communication (The exchange of messages and ideas between people inside and outside of the organisation)
- [ ] Security Policy Enforcement
- [ ] Management Support (job pressure, insufficient resources, poor management systems, inadequate security practices ,and work planning /control)
- [ ] Design of work environment (illumination, noise, temperature, vibration, the technology and equipment they use is poorly designed and confusing to use, etc.)

Clear answers on page | Submit

APPENDIX C: DATASET OF THE UITs QUESTIONNAIRE



NUM	gender	age	experienc	aware	policy	L1	L2	L3	L4	L5	L6	NUM	Human	Fatigue	Stress	Situation	Skills	Mind	Apathy	Ignorance	Motives	Risk	Gender	Mood	NUM	Age Ef
1	Male	20-30	1--5	yes	yes	1	1	1	1	1	1	1	1	0	0	1	0	0	0	1	0	0	0	0	1	0
2	Female	51-60	11--15	yes	yes	3	3	3	3	3	3	2	0	0	0	1	0	0	0	1	0	0	0	0	2	0
3	Male	20-30	1--5	yes	no	0	0	0	0	0	0	3	1	1	1	1	1	1	1	1	1	1	1	1	3	1
4	Female	61-	20-	yes	yes	4	4	4	4	4	4	4	0	0	0	0	0	0	0	0	0	0	0	0	4	0
5	Male	20-30	1--5	yes	yes	0	0	0	0	0	0	5	1	0	0	1	0	0	0	1	0	0	0	0	5	0
6	Male	20-30	1--5	yes	yes	0	0	0	0	0	0	6	1	0	1	1	1	1	0	1	1	1	1	1	6	1
7	Female	51-60	16--20	yes	yes	4	4	4	4	4	4	7	0	0	0	0	0	0	0	0	0	0	0	0	7	0
8	Female	61-	20-	yes	yes	4	4	4	4	4	4	8	0	0	0	0	0	0	0	0	0	0	0	0	8	0
9	Male	41-50	6--10	yes	yes	3	3	3	3	3	3	9	1	0	0	1	0	0	0	1	0	0	0	0	9	0
10	Male	20-30	1--5	yes	yes	0	0	0	0	0	0	10	1	0	0	1	1	1	0	1	0	0	1	1	10	0
11	Male	20-30	1--5	no	no	0	0	0	0	0	0	11	1	1	1	1	1	1	1	1	1	1	1	1	11	1
12	Female	41-50	6--10	yes	yes	3	3	3	3	3	3	12	1	0	0	1	0	0	0	1	0	0	0	0	12	0
13	Male	31-40	1--5	yes	yes	2	2	2	2	2	2	13	1	0	0	1	0	0	0	1	0	0	0	0	13	0
14	Male	20-30	1--5	yes	yes	0	0	0	0	0	0	14	1	0	0	1	1	1	0	1	0	0	0	1	14	0
15	Female	41-50	6--10	yes	yes	3	3	3	3	3	3	15	1	0	0	1	0	0	0	1	0	0	0	0	15	0
16	Male	20-30	1--5	yes	yes	0	0	0	0	0	0	16	1	0	0	1	1	1	0	1	0	0	0	1	16	0
17	Male	20-30	1--5	yes	yes	0	0	0	0	0	0	17	1	0	0	1	1	1	0	1	0	0	0	1	17	0
18	Female	41-50	6--10	yes	yes	3	3	3	3	3	3	18	0	0	0	1	0	0	0	1	0	0	0	0	18	0
19	Male	20-30	1--5	yes	yes	0	0	0	0	0	0	19	1	0	0	1	1	1	0	1	0	0	0	1	19	0
20	Male	20-30	1--5	yes	yes	0	0	0	0	0	0	20	1	0	0	1	1	1	0	1	0	0	0	1	20	0
21	Female	41-50	6--10	yes	yes	3	3	3	3	3	3	21	1	0	0	1	0	0	0	1	0	0	0	0	21	0
22	Male	20-30	1--5	yes	yes	0	0	0	0	0	0	22	1	0	0	1	1	1	0	1	0	0	0	1	22	0
23	Female	41-50	6--10	yes	yes	3	3	3	3	3	3	23	1	0	0	1	0	0	0	1	0	0	0	0	23	0



NUM	Human	Fatigue	Stress	Situation	Skills	Mind	Apathy	Ignorance	Motives	Risk	Gender	Mood	NUM	Age Effects	Influence	Budget	Culture	Communication	Security	Management	Design
1	1	0	0	1	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0
2	0	0	0	1	0	0	0	1	0	0	0	0	2	0	0	0	0	0	0	0	0
3	1	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1
4	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0
5	1	0	0	1	0	0	0	1	0	0	0	0	5	0	0	0	0	0	0	0	0
6	1	0	1	1	1	1	0	1	1	1	1	1	6	1	0	1	1	1	1	1	1
7	0	0	0	0	0	0	0	0	0	0	0	0	7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0
9	1	0	0	1	0	0	0	1	0	0	0	0	9	0	0	0	0	0	0	0	0
10	1	0	0	1	1	1	0	1	0	0	1	1	10	0	0	1	1	1	1	1	1
11	1	1	1	1	1	1	1	1	1	1	1	1	11	1	1	1	1	1	1	1	1
12	1	0	0	1	0	0	0	1	0	0	0	0	12	0	0	0	0	0	0	0	0
13	1	0	0	1	0	0	0	1	0	0	0	0	13	0	0	0	0	0	0	0	0
14	1	0	0	1	1	1	0	1	0	0	0	1	14	0	0	1	1	1	1	0	1
15	1	0	0	1	0	0	0	1	0	0	0	0	15	0	0	0	0	0	0	0	0
16	1	0	0	1	1	1	0	1	0	0	0	1	16	0	0	1	1	1	1	0	1
17	1	0	0	1	1	1	0	1	0	0	0	1	17	0	0	1	1	1	1	0	0
18	0	0	0	1	0	0	0	1	0	0	0	0	18	0	0	0	0	0	0	0	0
19	1	0	0	1	1	1	0	1	0	0	0	1	19	0	0	0	1	1	1	0	0
20	1	0	0	1	1	1	0	1	0	0	0	1	20	0	0	0	1	1	1	0	0
21	1	0	0	1	0	0	0	1	0	0	0	0	21	0	0	0	0	0	0	0	0
22	1	0	0	1	1	1	0	1	0	0	0	1	22	0	0	0	0	1	1	0	0
23	1	0	0	1	0	0	0	1	0	0	0	0	23	0	0	0	0	0	0	0	0

APPENDIX D: TABLES

Table 1: Cronbach Alpha Reliability Test (Pilot Study)

Variables	Number of items	Cronbach Alpha	Type
Likelihood of UIT	6	0.950	Excellent reliability
UIT Contributing factors	20	0.892	High reliability

Table 2: Correlations of the likelihood question's Items (Pilot Study)

Likelihood items	Likelihood 2	Likelihood 3	Likelihood 4	Likelihood 5	Likelihood 6
Likelihood 1	.964** .000 50	.945** .000 50	.982** .000 50	.977** .000 50	.890** .000 50
Likelihood 2		.969** .000 50	.986** .000 50	.986** .000 50	.991** .000 50
Likelihood 3			.978** .000 50	.975** .000 50	.969** .000 50
Likelihood 4				.992** .000 50	.990** .000 50
Likelihood 5					.983** .000 50

** Correlation is significant at the 0.01 level (2-tailed)

Table 3: Correlations of Contributing Factors of UIT (Pilot Study)

	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6	Factor 7	Factor 8	Factor 9	Factor 10	Factor 11	Factor 12	Factor 13	Factor 14	Factor 15	Factor 16	Factor 17	Factor 18	Factor 19	Factor 20
Factor 1	.142 .325 50	.187 .193 50	.657** .000 50	.403 .114 50	.333 .118 50	.115 .428 50	.657** .000 50	.187 .193 50	.166 .250 50	.208 .148 50	.316 .125 50	.187 .193 50	.142 .325 50	.263 .065 50	.298 .135 50	.421 .182 50	.333 .118 50	.208 .148 50	.245 .086 50
Factor 2		.758** .000 50	.093 .519 50	.352 .312 50	.426 .102 50	.808** .000 50	.093 .519 50	.758** .000 50	.857** .000 50	.684** .000 50	.450 .341 50	.758** .000 50	1.000** .000 50	.539** .000 50	.476 .401 50	.337 .117 50	.426 .272 50	.684** .000 50	.579** .000 50
Factor 3			.123 .394 50	.464 .401 50	.562** .000 50	.612** .000 50	.123 .394 50	1.000** .000 50	.885** .000 50	.903** .000 50	.593** .000 50	1.000** .000 50	.758** .000 50	.711** .000 50	.628** .000 50	.444 .111 50	.562** .000 50	.903** .000 50	.764** .000 50
Factor 4				.265 .063 50	.219 .127 50	.075 .603 50	1.000** .000 50	.123 .394 50	.109 .452 50	.136 .345 50	.208 .148 50	.123 .394 50	.093 .519 50	.173 .230 50	.196 .172 50	.277 .052 50	.219 .127 50	.136 .345 50	.161 .264 50
Factor 5					.826** .000 50	.284 .345 50	.265 .063 50	.464 .501 50	.411 .213 50	.514** .000 50	.783** .000 50	.464 .901 50	.352 .112 50	.653** .000 50	.740** .000 50	.957** .000 50	.826** .000 50	.514** .000 50	.608** .000 50
Factor 6						.344 .114 50	.219 .127 50	.562** .000 50	.497 .100 50	.623** .000 50	.948** .000 50	.562** .000 50	.426 .312 50	.790** .000 50	.896** .000 50	.790** .000 50	1.000** .000 50	.623** .000 50	.736** .000 50
Factor 7							.075 .603 50	.612** .000 50	.692** .000 50	.553** .000 50	.363 .110 50	.612** .000 50	.808** .000 50	.436 .122 50	.384 .716 50	.272 .056 50	.344 .214 50	.553** .000 50	.468 .121 50
Factor 8								.123 .394 50	.109 .452 50	.136 .345 50	.208 .148 50	.123 .394 50	.093 .519 50	.173 .230 50	.196 .172 50	.277 .052 50	.219 .127 50	.136 .345 50	.161 .264 50
Factor 9									.885** .000 50	.903** .000 50	.593** .000 50	1.000** .000 50	.758** .000 50	.711** .000 50	.628** .000 50	.444 .111 50	.562** .000 50	.903** .000 50	.764** .000 50
Factor 10										.799** .000 50	.525** .000 50	.885** .000 50	.857** .000 50	.629** .000 50	.555** .000 50	.393* 201 50	.497 .123 50	.799** .000 50	.676** .000 50
Factor 11											.657** .000	.903** .000	.684** .000	.788** .000	.695** .000	.492 .124	.623** .000	1.000** .000	.846** .000

											50	50	50	50	50	50	50	50	50
Factor 12												.593** .000 50	.450* .401 50	.834** .000 50	.945** .000 50	.749** .000 50	.948** .000 50	.657** .000 50	.777** .000 50
Factor 13													.758** .000 50	.711** .000 50	.628** .000 50	.444 .231 50	.562** .000 50	.903** .000 50	.764** .000 50
Factor 14														.539** .000 50	.476 .213 50	.337 .217 50	.426 .112 50	.684** .000 50	.579** .000 50
Factor 15															.882** .000 50	.625** .000 50	.790** .000 50	.788** .000 50	.932** .000 50
Factor 16																.708** .000 50	.896** .000 50	.695** .000 50	.822** .000 50
Factor 17																	.790** .000 50	.492 .220 50	.582** .000 50
Factor 18																		.623** .000 50	.736** .000 50
Factor 19																			.846** .000 50

Table 4: The Likelihood1 of UITs

Status	Frequency	Percentage (%)
Not likely	54	17.4
Least likely	45	14.5
Likely	75	24.1
Very likely	105	33.8
Most likely	31	10.0

Table 5: The Likelihood 2 of UITs

Status	Frequency	Percentage (%)
Not likely	57	18.3
Least likely	45	14.5
Likely	74	23.8
Very likely	106	34.1
Most likely	29	9.3

Table 6: The Likelihood 3 of UITs

Status	Frequency	Percentage (%)
Not likely	56	18.0
Least likely	56	18.0
Likely	66	21.2
Very likely	105	33.8
Most likely	28	9.0

Table 7: The Likelihood 4 of UITs

Status	Frequency	Percentage (%)
Not likely	54	17.4
Least likely	45	14.5
Likely	78	25.1
Very likely	103	33.1
Most likely	31	10.0

Table 8: The Likelihood 5 of UITs

Status	Frequency	Percentage (%)
Not likely	55	55
Least likely	47	47
Likely	73	73
Very likely	109	109
Most likely	27	27

Table 9: The Likelihood 6 of UITs

Status	Frequency	Percentage (%)
Not likely	56	18.0
Least likely	44	14.1
Likely	76	24.4
Very likely	106	34.1
Most likely	29	9.3

APPENDIX E: SECOND VERSION OF UITCM/ COMPONENTS DESCRIPTION AND RELATIONS

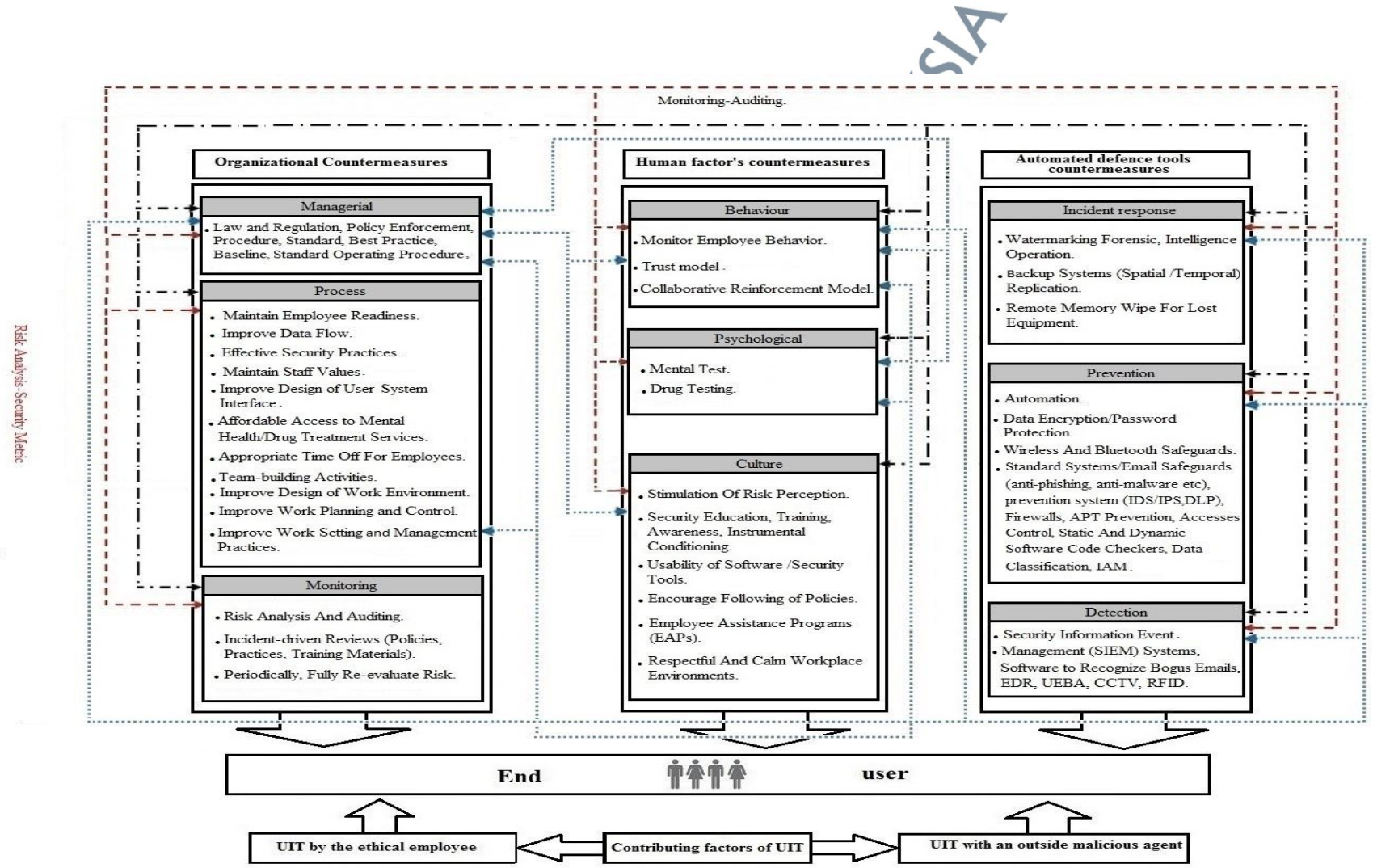


Figure 1: Second Version of UIT Countermeasure Model (UITCM)

Table 1: The Organizational Countermeasures.

UITCM		
The Organizational Countermeasures Components		
Component	**Element**	**Description**
Managerial	OC01-Law and Regulation, Policy Enforcement, Procedure, Standard, Best practise, Baseline, Standard Operating Procedure (SOP).	• Organizations should adopt a security program that deals with unintentional insider threats and takes them into consideration. Security program is a documented set of ***organization's information security policies, procedures, regulations***, ***and standards***. Organization should has law ,***regulations, policy , procedures, standards, best practice, baselines and standard operating procedure*** that deals with all aspects of unintentional insider threats. • ***Information security law*** is the body of legal rules, codes, and standards that require organization to protect information and the information systems that process it from threats including UIT. • ***A regulation*** is the process, or body, responsible for ensuring that the law is put into effect. A regulation explains the details necessary, whether technical, operational or legal, to put the law into effect, for example it is mandatory for businesses to dispose and destroy of customer information in its custody when the records are no longer related to the business. Civil criminal and monetary penalties would be levied on anyone browsing, selling or unlawfully accepting customer's records by law. To prevent occurrence of such failures, regulations should be created to require employees to dispose customer's data in an appropriate manner. • ***Policies*** are the top tier of formalized security documents. These high-level documents offer a general statement about the organization's assets and what level of protection they should have, and it is a set of rules that guide individuals who work with IT assets Well-written policies should spell out who's responsible for security, what needs to be protected, and what is an acceptable level of risk. They are much like a strategic plan because they outline what should be done but don't specifically dictate how to accomplish the stated goals. Those decisions are left for standards, baselines, and procedures, and implementing security best practices throughout the organization, as defined by widely tested and implemented security norms in the industry. The difference between policy and procedures is that they are generic, the policy are there to serve as a guide but do not provide detailed specifics in implementation. An effective information security procedure must include identify and remediate UIT. • ***Information Security Best Practices*** are a set of guidelines, ethics, or ideas that represent the most efficient of action in a given task. To decrease UIT encompass being cautious when engaging in online activities, abiding by organization rules, and reaching out for help when encounter something suspicious. • ***A Standard Operating Procedure*** (SOP) is a document that consists of a set of instructions or steps on how to execute a task step-by-step. (SOP) serves as a tool to ensure that activities are performed properly. Though it follows the ISO format, the document and the process belong to the organization. They are unique to a company or organization. Using SOP reduces the possibility of

		human error. • Organizations should adopt ***standards*** that supposed to reduce the feasibility and likelihood of the unauthorized release of classified information and addresses gaps in policy for information systems security, including characterization and detection of UITs, for examples :- ° The ISO 9001:2015 standard on human errors. ° The ISO 9001:2015, 8.5.1.g, requires organizations to carry out service provision under controlled conditions, which include taking actions to prevent human error. ° According to ISO/TS 9002:2016, the actions to prevent human error may include: ▪ Limiting excessive working hours. ▪ Putting in place a more suitable working environment. ▪ Providing appropriate training and instructions. ▪ Automating processes. ▪ Requiring double electronic entry of critical information. ▪ Making available devices to avoid incorrect tooling. ▪ Avoiding distractions (such as personal electronic devices). ▪ Rotating jobs. ▪ Requiring completion of information before submission. ▪ Planning of Changes. ° The intent of ISO 9001:2015, 6.3, Planning of changes, is to determine the need for changes to the organization's quality management system in order to adapt to changes in its business environment, as well as, to ensure that any proposed changes are planned, introduced, and implemented in a controlled manner. Properly planning a change can help to avoid negative consequences. It can also result in positive outcomes, such as the reduction of nonconforming outputs or reduced incidents of human error. ° The intent of ISO 9001:2015, 7.1.4, Environment for the operation of processes, is to ensure the organization determines and

		provides the necessary environment for the operation of its processes and to facilitate provision of conforming services. Whereas, human factors can be critical in a process; therefore, they should be considered when determining the environment for the operation of the processes, e.g., by avoiding high workloads and stress for employees (to prevent potential errors, burn-out).
Process	OC02-Maintain Employee Readiness.	•***Employee readiness*** is the extent to which having the personal characteristics such ability, attitudes, awareness, belief, activity, calm and motivation. These characteristics are necessary in order for them to perform the work tasks as they should. •To maintain employee readiness organizations should implement practices that reduce inattention, stress and anxiety, fatigue and boredom, and effects of illness and injury such as giving breaks, use automated reminder tools to change passwords periodically, material and moral incentives, granting sick leave, boost employees' confidence and enhance awareness of drug and hormone side effects and cognitive factors.
Process	OC03- Improve Data Flow.	• For an organization to get conquer a handle on its own data, it must have a coherent picture of how data flows through organization from beginning to end during data collection and creation, data storage, data use and transfer, data destruction and retention. • Organization must be concerned with: ▪ Who has sensitive data, what kind of sensitive data are they, where are the data stored, where did they come from, why were they collected, are they used for that purpose, are they used for other purposes, are the data transferred to other departments, third parties, clients, abroad? Who has access, how long are the data retained? ° How data are stored and transferred, which connections are secure or encrypted? ° What are data sources (data analysts, vendors, suppliers, partners, other departments)? ° How the data are obtained (hard-copy forms, telephone, mobile, email, online, web application, mobile application, desktop application, fax)? ° What are the places in which data are stored, both physically and digitally (e.g. databases, filing cabinets, tapes, network share drive, external hard-drive, personal laptop) and identify where these physically are? ° Where are the data processed and where they are transferred to (manual processing, digital processing, other departments, agencies, clients, vendors, regulators and authorities? ° Are data retained and destroyed in accordance with organizational policies and standards? (Hardcopy documents getting scanned for archiving purposes, system backup tapes, physical file archives, files held on laptops, when you end a

		relationship with a client or fieldwork agency, what happens with the data?) ° Are the means of transfer secure, is the transfer automated or manual? Is the form of the data secure (Excel, SPSS, PDF, audio/video, emails and attachments)? ▪ What is required by law? And how well are organization's processes in line with national laws ,local requirements or the data privacy laws in the country or in all countries concerned if the organization has established cross-border data transfers? •Organization should improve data flow by enhancing communication and maintaining accurate procedures and directions in the exchange of messages and data and ideas between people inside and outside of the organization, enhance information security awareness and motivate employees to comply with security policy, and communicate effectively with employees to ensure that they are aware of information security policy and understand the reasons for its effective implementation. For example, an organization could be storing sensitive data in the most secure cloud you could find, but if the data are transferred to this cloud unencrypted, they are still vulnerable.
Process	OC04- Effective Security Practices.	• Security program are implemented by several means: ° Technical: software, hardware, or firmware. ° Physical: physical barriers, locks, etc. ° Administrative: the actions and practices of people. • Security technology is important to security (firewalls, intrusion detection software, virus scanners), but the practices of the people who develop, integrate, evaluate, configure, maintain, and use that technology are more important; indeed, these practices are the foundation of technical (as well as physical and personnel) security. It is crucially important, therefore, that security practices be good ones; when feasible, best security practices should be used. • Security practices is a human practice; that is, a repeated or customary method used by people to perform some process and not an IT security mechanism, which is implemented by hardware, software, or firmware. • Some examples of security practices ° Plan for mobile devices (it is essential that organizations have a documented mobile devices policy and include these devices in a policy such as smart watches and fitness trackers with wireless capability). ° Document organization's security policies.

		° Educate all employees. ° Enforce safe password practices. ° Back up all data regularly. ° Install anti-malware software.
Process	OC05- Maintain Staff Values.	• ***Organizations' values*** are the fundamental beliefs of an organization, the guiding principles that dictate how people should behave and act. Organization must maintain staff values and attitudes that align with organizational mission and ethics. The values statement, also called the code of ethics, differs from both the vision and mission statements. The vision and mission state where the organization is going (vision) and what it will do to get there (mission). They direct the efforts of people in the organization toward common goals. The values statement defines what the organization believes in and how people in the organization are expected to behave with each other, with customers and suppliers, and with other stakeholders. It provides a moral direction for the organization that guides decision making and establishes a standard for assessing actions. It also provides a standard for employees to judge violations. Together, the vision, mission, and values statements provide direction for everything that happens in an organization. They keep everyone focused on where the organization is going and what it is trying to achieve. And they define the core values of the organization and how people are expected to behave. They are not intended to be a straitjacket that restricts or inhibits initiative and innovation, but they are intended to guide decisions and behaviours to achieve common ends. • An organization's values help people know the difference between right and wrong, and they help organizations determine if they are on the right path to fulfilling their business goals. The values statement defines how people in the organization should behave. It provides a guideline for decision making. Organization's workplace values set the tone for an organization's culture, and they identify what organization, as a whole, cares about. It's important that values of area's people align with organization's values. When this happens, people understand one another, everyone does the right things for the right reasons, and this common purpose and understanding helps people build great working relationships. Values alignment helps the organization as a whole to achieve its core mission. • Some examples of organization's values : ° Making a difference, respecting company policy and rules, and respecting others, focusing on detail, delivering quality, being positive, being completely honest, being a great team member, keeping promises, helping others, showing tolerance, being reliable and caring about deadlines. ° A problem solver: Solving one problem after the next will lead to building a great organization and that required people that are excited to hop from one problem to problem. ° Ambitious: Not just wanting things to happen, not watching things to happen but making things happen. Ambition can be a

		really powerful value if it leads to people being the change they want to see. ° Transparent: That if people are honest, open and direct in all conversations organization saves a lot of time. ° Empathetic: The ability to understand the challenges that others deal with, and how can help them thrives to hit their goals and maximize their potential. ° Adaptable: means how well does a person handle with vary conditions and to improve is to change, how well we adapt to change will determine how our success will be. ° Focused: If one is focused on doing too many things he won't do anything really well. ° Integrable: Integrity is the quality of being honest and having strong moral principles; moral uprightness. Organization should surround itself with people who care deeply about integrity. ° Accountable: The obligation of an individual to account for his or her activities, accept responsibility for them and to disclose their results in a transparent manner. • However, managers cannot just create a values statement and expect it to be followed. •Maintain staff values and attitudes that align with organizational mission and ethics can be achieved via establish good relationships in the workplace, encourage the development of positive relationships between managers and employees as well as amongst co-workers, setting clear goals, communicate effectively with employees, showing appreciation, building a strong team, sending a clear message, improving the openness at work, improving the behaviour of the individuals in an organization, getting beyond the, negative with staff development and, creating open communication in the workplace. Senior management shall act as role models in the visible promulgation of these values and expectations. Avoiding a culture of disloyalty and distrust within the organization and voiding authoritarian leadership such as (the use of one-way communication from top to bottom with an emphasis only on work progress, and final decisions usually made by the upper-level of management). Instead, another leadership should be adopted such as paternalistic leadership, or belief in reciprocity (e.g., work hard and the organization will offer a person more bonuses), participative leadership (e.g., authority is greatly decentralized), servant leadership (i.e., the perception that a leader's primary duty is to help subordinates to fulfil their desires, or interests), or leadership that has the capability to inspire organizational success and influence followers' beliefs and leading by example for example if one of an organization's values is to give more. The organization can do this by giving employees hours of paid time off each year to volunteer, or having its own charitable foundation based on service learning, social investments, donations and awards. • Keeping the organization's moral values at the forefront of everyone's mind by making it prominent within the workplace. In addition to featuring it on the company website and in the employee handbook, post it where employees often gather (conference rooms, snack rooms, etc.). , painting them on the walls throughout the office, to serve as a daily reminder for organization's

		employees. Reminding employees of values doesn't stop after crafting, laminating and posting posters throughout the office, however. They need to convert into specific, behavioural examples. By modelling and rewarding behaviours that demonstrate each value, employees are constantly reminded of what their organization stands for and how to better work by those principles. The best way to maintain staff values and attitudes is to model them. In other words, don't just let them sit on the wall and call it a day. Live, work and play by them on a daily basis. Most important, leading by example. Showing employees how it's done by using organization character to guide business decisions and empowering employees to do the same. Promote organizational values by rewarding behaviours that demonstrate them. Don't hesitate to publicly reward someone for exhibiting behaviours that are in line with the organization's character. Not only does this make the individual feel good, it also pushes the rest of the organization to follow suit. To hire based on values, for each of the organization's values, should developing a list of questions designed to assess a candidate's character and potential fit. For instance, if one of an organization values is that they are team entrepreneurial. Asking interview questions related to a candidate's ability to be enterprising is essential to finding talent that shares and fulfils the organization's values.
Process	OC06- Improve Design of User-System Interface.	• ***User interface*** is the features of a computer system which allows the user to interact with it. A user interface, also sometimes called a human-computer interface, comprises both hardware and software components. It handles the interaction between the user and the system. Interfaces include organizational factors and operational factors that manage the flow of information throughout the system, and maximize the accuracy, timeliness, and usability of information as set out in a company's Management Systems. Human operators are one of the biggest sources of errors in any complex system. Many operator errors are attributed to a poorly designed human-computer interface. System design and human interaction both play a role in how often human error occurs particularly when there is a slight mismatch between the system design and the person operating it, the ease and complexity of systems and software design , font colour and font size that cause optical dispersion can affect the user of information systems. A poorly designed system interface make errors more likely .When the system interface is poorly designed and confusing to use, the users will make similar types of mistakes. Security may be compromised when humans make mistakes at the user interface. Certain user-interface design drives users toward error, while other facilitate success and encourage the operator to perform correctly and protect the system from common operator errors. • Examples of features of a good user interface: ° The user interface must give appropriate feedback to the operator to allow him to make well informed decisions based on the most up to date information on the state of the system. If the user must operate the system to perform a task, the interface should guide the user to take the appropriate actions and provide feedback to the user when operations succeed or fail. ° High false alarm rates will make the operator ignore a real alarm condition. If an operator gets an alarm for nearly every action, most of which are false, he or she will ignore the alarm when there is a real emergency.

° System designers must insure that the user interface is easy and intuitive for human operators to use, but not so simple that it lulls the operator into a state of complacency and lowers his or her responsiveness to emergency situations. The interface must be relatively simple and easy to use without sacrificing system safety. One major problem with systems design is that they are designed for simplicity which can lead a normally privacy conscious person to make bad security decisions.

° In safety critical systems, the main goal when of the user interface is to prevent the operator from making a mistake and causing a hazard. In most cases usability is a complementary goal in that a highly usable interface will make the operator more comfortable and reduce anxiety. However, there are some trade-offs between characteristics that make the interface usable and characteristics that make it safe. For example, a system that allows the user to commit a procedure by simply pressing the enter key a series of times may make it extremely usable, but allow the operator to bypass important safety checks or easily confirm an action without assessing the consequences.

° The user interface must provide intuitive controls and appropriate feedback to the user. Many user interfaces' can cause information overload. For example, if an operator must watch several displays to observe the state of a system, he or she may be overwhelmed and not be able to process the data to gain an appropriate view of the system. This may also cause the operator to ignore displays that are perceived as having very low information content.

° The user interface must be designed so that it provides enough novelty to keep the user alert and interested in his or her job, but not so extremely complicated that the user will find it difficult to operate. Automated systems are extremely good at repetitive tasks. However, if an unusual situation occurs and corrective action must be taken, the system usually cannot react well. In this situation, a human operator is needed handle an emergency. Humans are much better than machines at handling novel occurrences, but cannot perform repetitive tasks well. Thus the operator is left to passively monitor the system when there is no problem, and is only a fail-safe in an emergency. This is a major problem in user interface design, because when the user is not routinely involved in the control of the system, they will tend to become bored and be lulled into complacency. This is known as operator drop-out. Since the user's responsiveness is dulled, in a real emergency situation, he or she may not be able to recover as quickly and will tend to make more mistakes.

• Improving design of user interface, putting users in control of the interface and correcting for human errors and lower its risk is a key part of designing a safety critical system. In order for a user interface to be well -designed and as many flaws as possible to be caught, several inspection methods should be applied. There are several heuristics for judging a well- designed user interface, but there is no systematic method for designing safe, usable user interfaces. It is also difficult to quantitatively measure the safety and usability of an interface, as well as find and correct for defects. Empirical methods can also be applied at the prototype stage to actually observe the performance of the user interface in action.

• Examples of inspection methods for judging a good designed user interface.

° ***Heuristic Evaluation***

Heuristic evaluation involves having a set of people (the evaluators) inspect a user interface design and judge it based on a set

of usability guidelines. These guidelines are qualitative and cannot be concretely measured, but the evaluators can make relative judgments about how well the user interface adheres to the guidelines.

This technique is usually applied early in the life cycle of a system, since a working user interface is not necessary to carry it out. Each individual evaluator can inspect the user interface on his or her own, judging it according to the set of heuristics without actually having to operate the interface. Heuristic evaluation is good at uncovering errors and explaining why there are usability problems in the interface. Once the causes are known, it is fairly easy to implement a solution to fix the interface. This can be extremely time and cost saving since things can be corrected before the user interface is actually built. However, the merits of heuristic evaluation are very dependent on the merits of the evaluators. Skilled evaluators who are trained in the domain of the system and can recognize interface problems are necessary for very domain specific applications.

A sample set of usability heuristics :

- Simple and natural dialog.
- Speak the users' language.
- Minimize the users memory load.
- Consistency.
- Feedback.
- Clearly marked exits.
- Shortcuts.
- Precise and constructive error messages.
- Prevent errors.
- Help and documentation.

° ***Cognitive Walkthrough***

Another usability inspection method is the cognitive walkthrough. Like the heuristic evaluation, the cognitive walkthrough can be applied to a user interface design without actually operating a constructed interface. However, the cognitive walkthrough evaluates the system by focusing on how a theoretical user would go about performing a task or goal using the interface. Each step the user would take is examined, and the interface is judged based on how well it will guide the user to

		perform the correct action at each stage. The interface should also provide an appropriate level of feedback to ensure to the user that progress is being made on his or her goal. Since the cognitive walkthrough focuses on steps necessary to complete a specific task, it can uncover disparities in how the system users and designers view these tasks. It can also uncover poor labelling and inadequate feedback for certain actions. However, the method's tight focus loses sight of some other important usability aspects. This method cannot evaluate global consistency or extensiveness of features. It may also judge an interface that is designed to be comprehensive poorly because it provides too many choices to the user. • Case example: Two security-sensitive user interfaces were evaluated in a laboratory user study: the Windows XP file-permissions interface and an alternative interface, called Salmon, designed in accordance with an error-avoiding principle to counteract the misleading constructs in the XP interface. The alternative interface was found to be more dependable; it increased successful task completion by up to 300%, reduced commission of a class of errors by up to 94%, and provided a nearly 3× speed-up in task completion time (Maxion& Reeder,2005).
Process	OC07- Affordable Access to Mental Health/Drug Treatment Services.	• ***Affordable access*** to mental health and drug treatment services means ensuring that employees have affordable access to mental health services, including drug treatment and provide adequate health insurance benefits for mental health care (adequate health insurance for mental health care). • Health insurance plan must covering mental health or substance use disorder services in parity with medical and surgical benefits, so that organizations' employees be protected by Mental Health and Substance Use Disorder Coverage Parity laws as defined under the health care laws. •The Drug Dependents (Treatment and Rehabilitation) Act 1983 The Act provides for both mandatory treatment and rehabilitation of any person who have been certified as drug dependent as well as for voluntary treatment and rehabilitation. •The Malaysian Mental Health Act 2001 The Act provides a framework for the delivery of comprehensive care, treatment, control, protection and rehabilitation of those with mental disorders.
Process	OC08- Appropriate Time Off For Employees.	• *Appropriate time off for employee's* means, providing appropriate time off for employees to find a balance between work and home life. • Working world poses many challenges to employees. While some careers allow a relaxed relationship between work and private

		life, many others demand significant reductions in the area of leisure and family. To reduce human error in workplace it's essential for organizations should considering how to achieve a work-life balance and implementing targeted measures to promote this and providing appropriate time off for employees. The goal is not only to make employees more productive, but also happier and more balanced.
Process	OC9- Team-building Activities.	• Promote team-building activities and social interactions among employees to enhance mood and building a strong team by encouraging teamwork through formal and informal team-building activities. For example arranging an organization-oriented outing, such as bowling or mini-golf, or involve the office in a team-based charitable activity. Good relationships in the workplace thrive when individuals feel part of a team and comfortable with their teammates. According to a 2008 study published by the University of Florida Institute of Food and Agricultural Sciences, respect and trust amongst co-workers and between supervisors and staff leads to greater collaboration, innovation and efficiency in the workplace.
Process	OC10- Improve Design of Work Environment.	• ***The work environment*** is the place where the employee is located and the physical conditions surrounding him during the performance of his work. • ***Design of work environment*** is a factor that makes errors more or less likely. Organizations must view poor design and layout of workplaces as a causal factor to physical discomfort which has been shown to be associated with human error, work environment includes such factors as noise, lighting and temperature, vibration, chaos in files and documents, workspace arrangement, and facility layout and arrangement, environmental controls, glare, noisy environment where alarms cannot be heard, too tight workspace to adequate remove or work on equipment and the uncomfortable offices, specifically in terms of how environmental factors contribute to human performance and safety and health .The concerns for design of work environment are that they induce fatigue and/or distract attention from the primary task, resulting in increased potential for human error. Design of work environment also includes the ease and complexity of systems and software design , font colour and font size that cause optical dispersion and can affect the user of information systems, and when the technology and equipment the user use is poorly designed and confusing to use, they get frustrated and make mistakes. • Organizations must improve design of work environment by providing quiet environment, arranged workplace, comfortable offices, easy-to-use and perfectly designed software, systems and equipment and avoiding design factors that cause confusion get frustrated, fatigue, distract attention and lead to mistakes.
Process	OC11- Improve Work Planning and Control.	• ***Work planning and control*** is the use of formal, documented processes for identifying and mitigating risks when planning, authorizing, releasing, and performing work. The purpose of work planning and control is to ensure adequate protection of employees, the public, and the environment, which would otherwise be put at risk by inconsistent and inadequate planning, authorization, and control. • Job pressure, poor job rotation, time factors, task difficulty, change in routine, poor task planning or management practice, lack of knowledge ,skills , capability , capacity and ability must be seen as a causal factor which has been shown to be associated with human error and impact employee performance and must be improved. For example, job stress and time pressure negatively affect

		performance; heavy and prolonged workload can cause fatigue, which adversely affects performance and in the presence of high email loads, users are more likely to respond to phishing email.
Process	OC12-Improve Work Setting and Management Practices.	• ***Work setting*** is the employee's ways and tools to perform his work. • ***Management practices*** are the working methods and innovations that managers use to make the organization more efficient. • Distractions, insufficient resources, poor management systems, inadequate security practices, and poor work flow must be seen as a causal factor which associated with human error and impact employee performance, and must be improved, as well as the working methods and innovations that managers use to make the organization more efficient. In addition to distributive, procedural, interpersonal, and informational justice in the relationships that employees have with their work organization and its members, which can promote employees' motivation to support the organization's interests and their ability to choose where, how and when they do their work in the office, a s they different types of tasks throughout the day, people need access to different types of work settings that relieves the physical and psychological stress that comes from working in a space that doesn't fit the task. For example: poor communication can cause several problems during a workflow lifecycle: information can become outdated, employees do not know that, and expectations and deliverables can be unclear.
Monitoring	OC13- Risk Analysis And Auditing.	• ***Risk analysis*** is the process of identifying and analysing potential issues that could negatively impact key business initiatives or projects. This process is done in order to help organizations avoid or mitigate those risks. Performing a risk analysis includes considering the possibility of adverse events caused by either natural processes, like severe storms, earthquakes or floods, or adverse events caused by malicious or inadvertent human activities. An important part of risk analysis is identifying the potential for harm from these events, as well as the likelihood that they will occur. • Risk analysis is necessary in many cases such as planning projects, to help anticipate and neutralize possible problems, deciding whether or not to move forward with a project, and improving safety and managing potential risks in the workplace. • To carry out a risk analysis, organization should follow these steps: 1- Identifying threats Identifying the existing and possible threats that organization might face in the systems, processes, or structures that organization use, and analysing risks to any part of these. What vulnerabilities can you spot within them? These can come from many different sources. For example(loss of a key individual by Illness, death or injury, disruption to supplies and operations or loss of access to essential assets, loss of customer confidence, or damage to market reputation, business failure, stock market fluctuations, interest rate changes, or non-availability of funding. 2- Estimate Risk Once organization has identified the threats you're facing, need to calculate out both the likelihood of these threats being

		realized, and their possible impact.(Risk Value = Probability of Event x Cost of Event).In addition the organization employs automated tools to support analysis of events. Once organization has identified the value of the risks it faces, organization can start to look at ways of managing them. Such as avoid the risk, share the risk with other parties, accepting the risk, or control the risk. • ***Auditing*** :The information systems auditing is the process of conducting analytical test and evaluating evidence to be determine in monitoring and evaluating computer system, maintain data integrity, achieve the organizational goals effectively, and use resources efficiently. The information system auditing is conducted to evaluate the readiness level of organization in managing information technology The process of information system audit involves four steps: 1. Measuring vulnerability of information system. 2. Identification of sources of threat. 3. Identification of high risk points. 4. Checking for computer abuse. • Organizations must apply risk management and measurement and analysis concepts and approaches to critical business processes to ensure they are providing the intended results, with periodic and incident-driven review, maintain records of reviews.
Monitoring	OC14-Incident-driven Reviews (Policies, Practices, Training Materials).	• Every organization that develops policies needs a review process. The organization's policies and procedures need to be periodically reviewed to ensure that they continue to be relevant to the work of the organization and aligned with applicable standards and security requirements .The policy shall be reviewed every year or at the time of any major change in existing IT environment affecting policy and procedures. • ***Incident-driven review*** is a review in which the review of the policies, practices, and training materials conduct after occurrence of incidents to determining the weaknesses in the policy that led to the accident and trying to develop it based on the causes of the accident, rather than periodic normal review. • Organization must conduct incident-driven reviews of policies, practices, processes, and training materials, by reactive approach that focuses on quick response.
Monitoring	OC15- Periodically, Fully Re-evaluate Risk.	• ***Risk evaluation*** is a systematic process of identifying hazards and evaluating any associated risks within an organization, then implementing reasonable control measures to remove or reduce them.

		• To carrying out a risk evaluation: ° Identifying potential risks. ° Identifying who and what might be harmed by those risks. ° Evaluating risk (severity and likelihood) and establishing suitable precautions ° Implementing controls and recording findings ° Reviewing the evaluation and re-evaluating if necessary. • A suitable and sufficient risk evaluation must be carried out prior to a particular activity or task being carried out in order to eliminate, reduce or suitably control any associated risk to information security. Once completed a risk evaluation should be reviewed periodically (proportionate to the level of risk involved) and in any case when either the current evaluation is no longer valid and/or if at any stage there has been significant changes to the specific activity or task. Relevant risk evaluation should be reviewed following an incident in order to verify if the control measures and level of evaluated risk where appropriate or require amendment. • Organization must treats the evaluation of risk as a continuous process and periodically fully re-evaluate risk to avoid the effects of lowered perceived risk threshold accumulated over time while many of the risks associated with information security are of a cumulative nature. This means that the likelihood of an event occurring on a given day or at a given time might be extremely small, but over time, this chance increases and risk tolerance varies over time in individuals They might come to accept or adapt to the surrounding risk and no longer perceive it the same way they perceived before and they might have a lower perception of risk than before.

Table 2: The Human Factor's Countermeasures

UITCM		
The Human Factor's Countermeasures Components		
Component	**Element**	**Description**
Behaviour	HC01-Monitor	•The UIT factors might be recognized or inferred through monitoring and surveillance methods. Monitoring the activity of

	Employee Behaviour.	employees is essential for risk management resulting from UITs .Monitoring is a tool to maintain the security of an organization by discovering employee involvement and participation, making certain that employees are properly matched in their jobs and fully aware of the extent of their authority, and make sure there is no policy violation or compliance .Employees who are resistant to change and training and who comply with policies only when management is tightly observing , employees who are unaware and employees who may causes damage accidentally, their interests and practices are being monitored automatically and routinely. Motives behind employee monitoring are, to prevent inappropriate actions of employees; monitoring careless behaviour and to protect employees' personnel information from becoming accessible to hackers who are likely to use the information. •Employee behavioural patterns could be tracked with the help of employee monitoring software reports that capture the data on employees' computer use style, visited websites orientation, and the software and documents used as well as relevant activities' duration. These programs running on their computers or a connected server. Employee monitoring acts involve monitoring Internet links, review of e-mails, telephone use, video surveillance for security purposes, storage and review of computer files, video recording of employee job performance, recording and review of telephone conversations, and storage and review of voicemail messages. Detection is achieved by automated tools that can detect employee's activity to reduce and stop data loss. Monitoring processes can includes examining and retrieving employees' e-mails that related to the work, records, and information about, employees' access to Internet websites, monitoring computer used by employee, knowing where the employee is, authorized personnel files, the possibility to proscribe all small electronic devices in the workplace that to prevent using it in work place and time spent outside the workplace. Perhaps including, in some cases, linguistic analysis performed on samples of monitored electronic communications. In addition to reporting policy violation by co-workers. •Organization's management must find a balance between monitoring gains and the costs of invading employee privacy. • Monitoring must be performed in accordance with privacy and civil liberties laws and protecting employee rights. Employee monitoring can be subject to a variety of laws and possible legal constraints or boundaries, for example, identifying perceived risk threshold under some circumstances may be considered mental health testing, laws would apply which could limit testing and responses. •Employees should be aware of the devices that will be used to monitor them, how the data will be used, and when exactly they will be monitored; and employees and customers should be notified when telephonic monitoring is taking place through the use of a specific tone that can be heard by both employee and customer.
Behaviour	HC02- Trust model.	•In the ***Trust model***, only certain people are given permission to certain rooms, open certain cabinet files, or sign cheques and the person who has the physical possession of the cheques does not have the machine that embosses the signatures. Someone might be trusted to make changes in the personnel records but not the engineering specifications. This segregation of duties can be used to minimize human error. The assumption is that one person can only make an error only in the area they are designated to be working on. • Applying the segregation of duties for all roles is essential for insider risk management and to mitigate insider threats by the

		principle of least privilege where strict organizational rules let employees have access only to resources that are required for their job role. •There needs to be shared responsibility at senior management level for the creation, dissemination and enforcing of a robust security policy that every employee has a copy of and familiar with the parts that pertain particularly to them ,that means segregation of duties, so that , only certain people are given permission to certain tasks. Physical controls are also well-founded in assigning the least privilege, i.e. only enough access to perform the required job, and in implementing a segregation of duty when more than one person is required to complete a critical function. Physical controls are also used to control and minimize the risk of unauthorized access to physical assets and information systems. For example, two people at least are needed with the privileged users to alter modifications on the system.
Behaviour	HC03- Collaborative Reinforcement Model.	•Employees work collaboratively to ensure that information security policy is adhered to by every member in the group. Certain rewards and punishments are then awarded to individuals, depending on their actions, and then monitoring and reporting for doing harmful mistakes so by the associated team members, who have probably better knowledge of it or can better detect it than the centrally administered monitoring mechanisms. Furthermore, policies regarding the reporting of careless behaviour of a co-worker can help in defending against the unintentional insider threat.
Psychological	HC04- Mental Problem Test.	•Psychological testing is a tool used for employment-screening. Many employers require job applicants to take psychological tests as a condition of employment, within specific skills tests that have relevance to the position of interest to determine if the candidate is well-suited to the job. Testing is sometimes used as a condition of continued employment. Testing of employees before and after employment is commonplace in the business world. Psychological tests are used to measure a person's mental abilities, talents, intelligence, or personality. There are deferent types of psychological tests available to help employers in making decisions. Organization must choose the right one. A psychological test for a job, often called a psychometric test, is a standard, scientific method used to measure a person's mental capabilities and behavioural style. These tests are designed to measure candidates' suitability for a role based on the required personality characteristics and aptitude. The purpose of psychological testing is to make more informed hiring decisions. Human error can be minimized by tailoring the demands of the job to the characteristics of the person, and can help reduce the number of problem employees. All psychological tests require that job applicant perform some behaviour to measure personal attributes, traits, or characteristics or to predict outcomes, these tests can differ in various ways. For example, they can differ in terms of the behaviour they require job applicant to perform, what they measure, their content, how they are administered and formatted, how they are scored and interpreted, and their psychometric quality. Psychometrics is the quantitative and technical aspect of mental measurement. The mental test usually called psychological test. Mental match involves the individual's information and decision-making requirements, as well as their perception of the tasks and risks. Mismatches between job requirements and people's capabilities provide the potential for human error. • Psychological tests have limited validity like standard medical tests and are administered and interpreted by clinical and forensic psychologists. So psychological tests are not only used during the hiring process. Some organizations use these tests to monitor the continued suitability of employees who have been on the job for some time. The psychological tests required for the position can be preliminary, periodical or extraordinary. Preliminary psychological tests concerning suitability for sphere of activity shall be

		performed prior to the beginning of the working process. Periodical psychological tests is required on an annual basis, for example, for the employee who is employed in a position, where risks of accidents are highly increased, the frequency of periodical psychological tests is regulated by the policy of organization. Extraordinary psychological tests concerning suitability for sphere of activity shall be provided in the cases, for example, for the employee's behaviour condition highly changed, which may make him unable to hold the position complying with occupational security requirements. • Some organizations use games as a way to carry out psychological testing for employees, where job applicants have to perform tasks using skills that the organizations is looking for during playing these games. Such as Deloitte company which customized a "game" which places potential employees in real life work situations at the firm. The 20-minute online game incorporates videos and tasks from real Deloitte employees based on scenarios that occur regularly in the workplace. The game serves as the first round of the selection process and follows the same principals as traditional psychometric testing commonly used by large consulting and professional firms and allows employers to assess candidates' performances (Alloway & Cissel,2017).
Psychological	HC05-Drug Testing.	•The first line of defence to mitigate insider threat begins at the hiring stage. Potentially non-trustworthy candidates can be identified at the application stage by conducting specific tests as a condition of employment, that have relevance to the position of interest to determine if the candidate is well-suited to the job. Drug testing for drug in the workplace is an option that enables employers to find out if employees are using specific types of drugs, either currently or in the recent past. In situations where the employee has a responsibility for the security of information system; there is a strong argument for workplace drug testing being carried out, within the employment conditions. Special laboratories perform drug testing using methods include using samples of the employee's blood, urine, hair, saliva or sweat. Workplace drug testing has the potential to greatly enhance health and safety in the workplace. Testing discourages people from abusing substances and thereby reducing the likelihood of the incidents related to working under the influence and encourages greater responsibility among employees who may cause harm to information system. •Drug testing may be used either as a condition of employment or to identify drug use in current employees. The organizations might require all job candidates to submit to a drug test before being hired. Other organizations perform drug tests on current employees to ensure that no one is misusing drugs. Some organizations test all employees at particular times throughout the year. Others test individual employees if the employer has a reasonable suspicion of drug use or after an accident in the workplace to determine if drugs played a role in the incident. Random testing is another method of drug testing. This method involves selecting random employees for testing. To ensure a truly random pool of tested employees, organizations sometimes use a computer program to determine who is tested. •If organization plan to use drug testing as a part of a workplace substance abuse policy, must take in consideration some legal issues such as the civil liberties, emphasizing individual freedom, the right to privacy and protection from discrimination and make sure the policy adheres to the state's laws and is accompanied by a carefully written policy, which is understood by employees and supervisors alike and respects the rights of all. When caring out drug testing in the workplace, there are some ethical principles that need to be in place to avoid violation of the rights of the employee. For example: ° The employee needs to know, prior to taking the job that drug testing is an expectation, and the workplace drug testing is

		planned. ° Workplace drug testing should be a justifiable course of action rather than a routine screen used to discriminate against alcohol or drug-using employees and there should be a clear justification of the relevance of workplace drug testing to the situation. ° The employee's privacy must be respected, including whether workplace drug testing has taken place as well as the result and consequences and must keep the confidentiality. ° Repeat tests should be conducted when a workplace drug test is positive, and employees should be given the opportunity to explain a positive drug test result. ° People with positive results must be treated with dignity and respect, and be supported rather than shamed; this is the only way that leads to avoid the misuse of workplace drug testing to discriminate.
Culture	HC06- Stimulation Of Risk Perception.	• ***Risk perception is*** an individual's assessment of risk, and the individual's risk assessment is reliant on the risk information that individual has and on the previous experiences. If one experiences long period characterized by absence of accidents. In the event that an accident occurs, expectations are grounded on previous experiences, meaning that users perceive this accident more as a rare occasion. On the other hand, if one experiences attacks consecutively for a long period of time, one will expect a similar attack in the near future. Consequently such a person becomes more careful and is cautious with the security measures. There is association among risk perceptions and security behaviour, and the risk perception has an effect on decision-making. Thus risk perception might play an important role for motivating people to improve their security behaviour. • Organizations must consider stimulation of risk perception a key component of security behaviour change. To stimulate employees' risk perception: ° Organization must keep employees abreast of latest attack news and statistics in Malaysia and international threat-related statistics. ° Employees who have a good knowledge should have more ability to assess risks. Organization must ensure that employees obtained security education and awareness program. ° Sharing of employees personal previous experiences on the threats if an employee experiences attacks in the past. ° Organization must keep employees abreast of threats effect on the organization and consequences to employees.
Culture	HC07-Security Education, Training, Awareness, Instrumental	• ***Enhance awareness*** of unintentional insider threat, heighten motivation to be wary of insider threat risks, recognizing phishing and other social media threat vectors, Keep employees abreast of latest attack vectors and other threat-related news, train continuously to maintain proper level of knowledge, skills, and ability, conduct training and awareness on risk perception, and

	Conditioning.	cognitive biases that affect decision making, conduct frequent training and awareness programs. • ***Instrumental conditioning*** refers to learning through consequences, so that a system user's behaviour that produces positive results is reinforced while behaviour that produces negative effects is weakened (strategy of reward and punishment). This strategy can be used by organization to improve security behaviour of employees.
Culture	HC08-Usability of Software /Security Tools.	• ***Usability*** is the degree to which a software or security tool can be used by users to achieve task objectives with effectiveness, efficiency, and satisfaction. Usability is a controlled aspect of User Experience design that ensures the end-user doesn't strain or encounter problems with the use of software or security tool. A user experience designer can control accessibility, user interface, information architecture and usability to suit the goals of users. Security needs to motivate a positive experience, and this is what usable software does. Difficult to use or confusing security systems often are less likely to be used .If a security tool is easy to use employees will choose to work securely over choosing not to. The highest levels of security can be achieved only with an equally high level of usability. Because usability of security tools help overcome user errors during using it and reduces the possibility of ignoring or skipping it. • Organization must improve usability of security tools and software to reduce likelihood of system-induced human error, hold usability as a fundamental element of security and must take into account some characteristics and properties when developing or selecting software and security tools, such as: ° It's important to ensure that software /security tools have interfaced is easy to navigate with little thought and should be as flexible as possible. It should be logical and practical to use. If options are permitted, the more secure routes or choices should be encouraged by making them the default or the most natural path for a user to follow. If users are presented with the appropriate security solutions to match their tasks, in a way that makes sense to them and requires uncomplicated but obvious use to achieve the security intended by the solutions, it will require little effort for users to work more securely and effective security and usability can be accomplished together. ° A solution should be intuitive, so that users do not need to decide on how to use a software /security tool to ensure security. Instead, a software / security tool should work to remove security decisions from users as much as possible. If it is less dependent on user action to work, will be more effective as the room for error is significantly reduced. A good interface design elevates security as it lessens the liability on users. ° Security tools and software should be practical and work in real-world applications and scenarios with real people who make mistakes. It is useless if it only looks good on paper, but does not apply to real-world situations. ° Organization does not need to choose between security and usability as organization must implementing systems that improve security and usability concurrently. Usability should not outweigh security. On other hand if a priority was placed on security without consideration for usability, this will result in the human errors. Because cumbersome solutions cause users to default from using them as they obstruct their tasks and negatively impact workflows. Organization must achieve effective

		security through uncomplicated easy-to-use systems that provide convenience for employees. ° Software and security tools must have considerations for multiple means of authentication to provide choice and varied levels of security, risk-based features whereby security can be heightened or reduced depending on circumstances and requirements and usable verification so that verification does not become an obstacle to usability, which it can if not appropriately balanced, are all important security and usability considerations. User-friendly controls that make use of technology advancements like biometrics (fingerprints, facial recognition, etc.) for better user experience should also be considered.
Culture	HC09-Encourage Following of Policies.	•***Policies and procedures*** are an essential part of any organization. Together, policies and procedures provide a roadmap for day-to-day operations. They give guidance for decision-making, and streamline internal processes. Organizations set rules and a policy for reasons whether that reasons is security, ethics, quality, or efficiency. • Some of the outcomes of policies and procedures: ° Policies and procedures keep operations from devolving into complete chaos. ° When employees are following policies and procedures, organization will use time and resources more efficiently. ° Consistency in practices is also right for employees individually. They know what they're responsible for, what's expected of them, and what they can expect from their supervisors and co-workers. ° When employees follow procedures, they perform tasks correctly and provide better quality customer service. ° When employees are following policies and procedures, workplace accidents and incidents are less likely to occur. • Policies and procedures won't do organization any good if employees don't follow them, and employees often break organization rules, because employees don't always like the idea of having to follow the rules. So organization must encourage following of policies rules. Encourage following of policies means the organization must create motivations for its employees to follow the policies by some steps such as: ° Employees can't follow policies they don't know. Organizations must have written policies and procedures, because verbal reminders don't work. Organizations' procedures must be written down in a way that's easy to understand and making them easily accessible for every employee, to create a reminder that removes the opportunity for excuses. Sometimes employees don't follow procedures, because they can't remember what employer told them. Many organizations still use paper-based policy manuals. This is problematic because employees need to be able to refer to policies at any time. If they don't have easy access to an up-to-date policy and procedure manual, they won't know the correct procedures to follow. Using a policy management software makes policies and procedures available to every employee member. Organization can quickly send out policy updates, and require employee signatures to make sure everyone has read the policy. With online policy management,

		employee can access procedures from anywhere, using any computer or mobile device. Instead of having to seek through pages, they can do a simple keyword search to pull up the procedure they need. This ensures they are actually following policies and procedures. Organization must keep a hard copy for their records or for anyone who wants the physical version, but must using digital documents to make sure all policies and procedures are easily accessible for every employee. ° Making sure that, employees read policies and procedures is the first step toward ensuring compliance, but it's not enough on its own. Employees may not entirely understand a policy or know how to put it into practice. Organization must train employees on the substance of policies as well as on how to perform procedures in real-life situations. Thorough training on policies and procedures should happen for every new hire during the on boarding process and should be ongoing for all employees. ° It's important to make sure employees understand why following policies and procedures are critical. Organization must help employees understand why procedures are necessary. If employees perceive organization's procedures as unnecessary, or superfluous to their real responsibilities, they won't take them seriously. Employees must know why you have them in place and why adhering to policies and procedures is an important part of their job. ° Employers must frequently monitor their employees' computer use for security reasons, to ensure compliance with organization policies, to ensure employees' productivity and to limit employee access to non-work-related internet sites. ° Provide compliance incentives and reward employees who comply with procedures. Recognizing and rewarding correct behaviour is a great motivator for employees. Bad behaviour should not be ignored and the negative consequences of not following policies and procedures should be clear. Organization must apply punishment policy, enforce penalties for non-compliance.
Culture	HC10-Employee Assistance Programs (EAPs).	• ***An Employee Assistance Program (EAP)*** is a voluntary, work-based program designed to help employees in resolving personal problems that may be adversely affecting the employee's performance and reduce outside stresses, which may cause mind wandering ,EAP offers free and confidential assessments, short-term counselling, referrals,, and follow-up services to employees who have personal or work-related problems. • EAP services are usually made available not only to the employee but also to the employee's family. They are most often associated with counselling services for troubled employees enduring difficult times affecting mental and emotional well-being such as illness and injury, minor medical emergencies, alcohol or substance abuse, marriage concerns and family problems ,child or elder care, grief and loss, stress ,psychological disorders, and financial and personal legal issues. EAP counsellors also work in a consultative role with managers and supervisors to address employee and organizational challenges and needs. • Some benefits of EAPs ° Reduced incidents and human errors.

		° Fewer workplace disputes. ° Significantly reduced medical costs arising from early identification and treatment of individual mental health and substance use issues. ° Decreased absenteeism. ° Greater employee retention. • EAP plans should be entirely subsidized by organization. Programs are delivered at no cost to employees as part of comprehensive health insurance plans. Services are often delivered via phone, video-based counselling, online chatting, e-mail interactions or face-to-face.
Culture	HC11-Respectful And Calm Workplace Environments.	• A respectful workplace is one where employees can expect to be treated fairly and courteously in an environment that promotes engagement and contributes towards the safe, effective and quality delivery of service. Respect is showing consideration for other employees, demonstrating compassion, treating others with dignity and fairness as well as valuing and honouring diversity and recognizing and affirming individual and team contributions. Employees can be expected to demonstrate polite and courteous behaviour towards each other (verbal and non-verbal), feel empowered to perform their roles and feel safe to suggest changes for improvements in a collaborative and constructive manner. For employees to be motivated and engaged, they must be in a respectful environment. Without respect, productivity, profits, health, and happiness dwindle. Employees want to feel appreciated and know they matter and treated with dignity and respect. Demonstrating respectful behaviour will ensure a desired and professional workplace as well as a highly productive environment. Respect is earned when employees act and react in considerate and professional ways. • Just as the physical work environment impacts the employee's performance (temperature and lighting, etc), non-respectful environment impacts the employee's performance as well. Respectful and calm workplace environments lead to motivate and encourage organization's employees to work better and with pleasure. Even small details can impact employees' productivity and performance, so everything, is significant for team-building and crafting a workplace and keeping employees' motivated and handle stress and create a positive work environment for organization's employees and reducing workplace disputes and incidents of human errors. • Organization must create a respectful positive environment through some steps such as: ° Organization must develop clear workplace instructions to employees that eliminates racism and discrimination harassment, bullying, intimidation, purposeful exclusion or ignoring, threats, belittling, yelling, rumours, coercion, gossiping, sarcasm, constant criticism, mobbing, using profane, disrespectful, abusive, demeaning language, using inappropriate labels or comments about others ,patronizing and insulting remarks, shaming others publicly ,exhibiting uncontrolled anger ,berating an individual in front of others or in private ,excessive and unreasonable monitoring of someone's work ,withholding information or resources needed to, escalating personal harassment ,threats of retribution and

		litigation or violence. ° Organization must develop clear instructions to employees that which supports and encourages responding to requests and information in a timely and professional manner ,acknowledging the contributions of others , including people in the communication and decisions that need to be involved , transparency in the evaluation processes used, treating people with respect, compassion, dignity and fairness ,acting ethically and upholding professional standards, taking responsibility for actions and expecting the same of others, being open , honest and no bully, respect confidentiality and privacy ,staying calm , kind, courteous and positive ,avoiding getting angry and emotional, asking for help when needed, listening to understand and practice empathy, following the boundaries that have been set, asking permission to use someone's stuff, keeping the environment clean for others to use, showing appreciation, respecting differ opinions ,communicating effectively with team members and resolve stressful situations, respecting co-worker's property and individual space, helping and cooperation, accepting criticism and knowledge from co-workers as well, apologizing when necessary, smiling and saying good morning and thank you, giving everyone a chance to share input and bring ideas to life in conversations, muting or turning off cell phone while in the workplace ,taking into account the voices as it can be distracting to others, expressing calmly without passing judgment or criticism and not to send text messages or receive calls etc. ° Organization must lead by example and model the behaviours that they expect of employees. ° Organization must implement educational courses so that employees understand the benefits of respectful work environment and enhancing the substance of engagement, cooperation and calm. ° If organization experience or observe disruptive behaviour in the workplace, it is important that they do not ignore the incident. Ignoring it can make the workplace feel unfriendly, impact morale and engagement. Problems must be resolved from the beginning when conflict arises and attempting to find a common ground and solution, to prevent and address violence in the workplace and response policy that sets out the processes for reporting and investigating workplace abuse and harassment claims to create a psychologically safe work environment. ° Organization can use different ways to provide rewards, including praise, recognition, money, prizes, gift cards, celebratory meals, trophies and certificates of achievement to create a positive atmosphere in the workplace. ° Organization can develops employees' relationships outside of work such as planning a charity campaign and encouraging employees to participate in fundraising events, having lunch together or event like a bowling day or day a ballpark.

Table 3: The Automated Defence Tools Countermeasures

UITCM		
Automated Defence Tools Countermeasures		
Component	**Element**	**Description**
Incident response.	AC01- Watermarking Forensic, Intelligence Operation.	• ***A forensic watermark*** is the process of embedding of a sequence of characters or code in a digital document, image, video or computer program to uniquely identify its originator and authorized user. In such a way that it is imperceptible to a human observer but easily detected by computer algorithm. A digital watermark is a transparent, invisible information pattern that is inserted into a suitable component of the data source by using a specific computer algorithm. Digital watermarks are signals added to digital data (audio, video, or still images) that can be detected or extracted later to make an assertion about the data. Forensic watermarks can be repeated at random locations within the content to make them difficult to detect and remove. •The main purpose of forensic watermarking is to protect the interests of content creators against illegal use and distribution of copyrighted digital works. While forensic watermarks cannot prevent such activity altogether, they can make it easier for copyright holders to detect it and to identify people who engage in it. A forensic watermark can alert honest users when they have received illegitimate documents or programs. Forensic watermarks are used in the software and digital video industries. Other applications in which the technology holds promise include digital music and electronic books (e-books). • ***Intelligence operation*** is the practice of collecting, evaluation, standardizing, analysing and response to data generated by networks, applications, and other IT infrastructure undergoing potential security threats in real-time. And that includes the processes, policies and tools designed to gather the information relevant to protecting an organization from external and inside threats .That information is used to assess and improve an organization's security posture. • ***Security intelligence's*** main goal is to protect the data an organization has by compiling and scrutinizing as much of the data as possible. • Elements of security intelligence include: ° Log management: The collective processes and policies used to administer and facilitate the generation, transmission, analysis, storage and ultimate disposal of the large volumes of log data created within an information system. ° Security information and event management (SIEM): An approach to security management that seeks to provide a holistic view of an organization's information technology (IT) security. Most SIEM systems deploy multiple collection agents to gather security-related events from end-user devices, servers, network equipment and specialized security equipment like

		firewalls, antivirus or intrusion prevention systems. The collectors forward events to a centralized management console, which performs inspections and flags anomalies. ° Network behaviour anomaly detection (NBAD): The continuous monitoring of a network for unusual events or trends. An NBAD program tracks critical network characteristics in real time and generates an alarm if a strange event or trend is detected that could indicate the presence of a threat. NBAD is an integral part of network behaviour analysis (NBA). ° Risk management: The process of identifying, assessing and controlling threats to an organization's capital and earnings. Such threats include financial uncertainty, legal liabilities, strategic management errors, accidents, natural disasters and information technology (IT) security threats ° Network forensics: The capture, recording, and analysis of network events for the purpose of discovering the source of security attacks or other problem incidents. "Catch-it-as-you-can" systems capture all packets passing through a certain traffic point, store the data and perform analysis subsequently in batch mode. "Stop, look and listen" systems perform a rudimentary analysis in memory and save only certain data for future analysis. • Key properties of security intelligence ° Real-Time Analysis: It is not enough to be able to view log records when dealing with exploits and immediate threats. Real-time monitoring is a crucial aspect of security intelligence gathering when identifying threats. Security Intelligence is able to evaluate potential present threats. IT organizations use technological tools such as SIEM software to gather security intelligence in real time. ° Pre-Exploit Analysis: Security intelligence blends pre-exploit vulnerability management with real-time analysis. By identifying risks before they become breaches, organizations may reduce and more easily detect attacks. ° Data collection, standardization and analysis: Collecting as much applicable data as possible from pertinent devices on the network, creating relations between those devices, and then analysing their behaviour to identify aberrant actions is the most relevant and complete method of identifying security incidents. Security intelligence is capable of fully understanding a situation, identifying the key components and surrounding information, and effectively notifying security analysts of potential threats. Data are aggregating from the IT infrastructure in the form of network, event and application logs. Security intelligence use complex machine learning, pattern recognition and big data analysis to sift through millions of logs from across applications, translate the aggregated data into a standardized format that is human readable, and analyse the data to detect attacks or vulnerabilities. ° Actionability: Genuine security intelligence must be actionable for the organization. The goal of security intelligence is not to collect, evaluate and store additional data and information, but to identify threats, and present potential threats to security analysts in a meaningful and comprehensive way and generate actionable data that drives the informed and targeted

		implementation of security controls and countermeasures. • Benefits of intelligence operation. ° Improved regulatory and standards compliance: Tools that collect standardize and analyse log data can help IT organizations demonstrate their compliance with a specified security standard. ° Enhanced threat detection and remediation: Detecting security threats is a core function of SIEM tools. These tools use machine learning and big data to correlate events that are buried in millions of log files from across the network. That leads to faster threat detection and better response times when indicators of a computer intrusion are detected. ° Simplified Security Operations: IT organizations today can automate many different types of security intelligence gathering tasks through cutting-edge SIEM tools, simplifying their operations and reducing the cost of gathering actionable and useful security intelligence.
Incident response.	AC02-Backup Systems (Spatial /Temporal) Replication.	• ***Backup*** is the process of creating and storing copies of data that can be used to protect organizations against data loss. Recovery from a backup typically involves restoring the data to the original location, or to an alternate location where it can be used in place of the lost or damaged data. A proper backup copy is stored in a separate system or medium, from the primary data to protect against the possibility of data loss due to primary hardware or software failure. The alternate medium can be an external drive or USB stick, a disk storage system, cloud storage container, or tape drive. The alternate medium can be in the same location as the primary data or at a remote location. The possibility of weather-related events may justify having copies of data at remote locations. The purpose of the backup is to create a copy of data that can be recovered in the event of a primary data failure. Primary data failures can be the result of hardware or software failure, data corruption, or a human-caused event, such as a malicious attack (virus or malware), or accidental deletion of data. Backup copies allow data to be restored from an earlier point in time to help the business recover from an unplanned event. A system backup is the process of backing up the operating system, files and system-specific useful/essential data. Backup is a process in which the state, files and data of a computer system are duplicated to be used as a backup or data substitute when the primary system data is corrupted, deleted or lost. The purpose of a systems backup is to provide a means to restore the integrity of a computer system in the event of a hardware/software failure, physical disaster, or human error. A system backup consists of either a full backup (copying everything that is considered important and that must not be lost), incremental backup (making copies of the files by taking into account the changes made in them since the previous backup) , or a combination of the two. For best results, backup copies are made on a consistent, regular basis to minimize the amount data lost between backups. The more time passes between backup copies, the more potential for data loss when recovering from a backup. Retaining multiple copies of data provides the insurance and flexibility to restore to a point in time not affected by data corruption or malicious attacks. • ***Replication*** is a process of copying and maintaining database objects. The replicated databases are monitored for changes and resynchronized when a change is made .Database replication makes a copy of data accessible from many various servers instead of accessing one central server, or enables many servers to behave like one (parallel query processing). Replication considered as a

		mechanism for creating data backups. • ***Spatial replication:*** The idea of this strategy is the creation of several copies of a system. Each replica of the system has its own duplicates of the system's important information, which is synchronized (Several copies in different places).This approach is most suitable in cases when only the minority of the replicas is affected by human error. Consequently the greater proportion of the replicas is accepted as the correct state of system. • ***Temporal replication:*** it keeps more than one copies of system, with each one having its own replica of state of the system. The replicas used in temporal replication are not synchronized (Several copies in different times). Temporal replication makes use of a current copy that represents the actual state of the system and several replicas (historical) will represent the situation of different states in the system's history. Requests to the system together with human operator input are only affected on the current replica. This approach works well for cases whereby human errors affect the system state.
Incident response.	AC03- Remote Memory Wipe For Lost Equipment.	• ***Remote Wipe*** is a system capability or software solution where an administrator has the ability to remotely delete and destroy data on a device or system (totally erase the device's memory, in case the device gets lost or stolen) . This feature is often present in the context of mobile device management, and comprehensive risk management systems usually have a remote erase function. Remote Wipe is an effective way to prevent data breaches, and it can address security concerns in Bring Your Own Device (BYOD) policies and security gaps in distributed company computing networks. Wiping a device is the best way to ensure sensitive data stays out of the wrong hands. When a device is lost, stolen, or otherwise compromised, the company must take action to prevent a data breach. So organization must enable remote memory wipe for lost equipment.
Prevention	AC04-Automation.	• ***Automation:*** The use of information technologies to make decisions on behalf of the user .Such as would be to have a popup menu appear on an employee's computer screen giving notification that it is time to change their password. Automation is highly commendable in cases where it is absolutely impossible for the system user to do the work. An example is where packets are checked by intrusion prevention systems at a speed that exceeds that of a human systems administrator. Since many security failures are attributed to humans, then it could be wise to use techniques that involve minimum human intervention. The major strength of automation is that it is more predictable and accurate that its' human counterparts. An example of automation is the old anti-virus program that required system users to decide on whether to clean quarantine or ignore a detected virus. With the modern versions of anti-virus programs, the viruses are automatically cleaned upon detection. The main purpose of automation is overcoming poor user decisions and choices. • Organization should adopt automation in the processes that can be automated to reduce human error.
Prevention	AC05-Data Encryption/Password Protection.	• A password is a series of characters containing alphabets, numbers and special characters. ***Password*** protection means only authorized users or the ones who know the password can access the desired information. Password protection is a security measure put in place to protect sensitive information accessible via computers from unauthorized access. • ***Encryption*** is process of concealing information in such a way that only authorized personnel can access the information encoded

		within files and unauthorized users cannot. Encryption means to hide information or data into something that is unreadable to anyone with no access to the information. To hide the information, two crucial pieces of data is required: the cipher and the key. Cipher is an algorithm and the special knowledge required to decrypt the encrypted data is called the key. So, a cipher is basically a key to the code. • Data encryption and password protection are using in order to protect sensitive information from falling into the wrong hands. Organization should enable data encryption and, Password protection on storage devices.
Prevention	AC06-Wireless And Bluetooth Safeguards.	• ***Bluetooth*** is a wireless technology standard used for exchanging data between fixed and mobile devices over short distances using radio waves. It is an open standard for short-range radio frequency (RF) communication. Bluetooth technology is used primarily to establish wireless personal area (WPAN), ad hoc or peer-to-peer (P2P) networks. Bluetooth technology has been integrated into many types of business and individuals devices, including cellular phones, personal digital assistants (PDA), laptops, automobiles, printers, and headsets. Bluetooth a technology for creating small personal networks between a wide variety of devices to transfer voice and data without the need for cables. Bluetooth devices easily connect to each other. This was the intent when the specification was developed. Consequently, many devices include Bluetooth in a manner that provides for easy connectivity while exposing the information assets of individuals and organizations to greater risk. • Any organization might have hundreds or thousands of Bluetooth enabled cell phones, smart phones, PDA's, keyboards, and mice in the workplace. The possibility of it interacting with organization's network also grows. This number of wireless devices is increasing the potential for information asset compromise and the potential security vulnerabilities that mobile devices present. The more that employees and contractors use mobile devices to access organizational systems, applications and data, the more important it is to protect such access. • Given that mobile devices are inherently moving targets used outside the organization , and thus also outside its firewalls, threat management, spam and content filtering, and other protection tools, it's important to apply a battery of best practices to use of mobile devices to keep exposure to risk and loss to a minimum. • Organization must take security measures that can implement to secure mobile devices, that Bluetooth-enabled. It's essential to prevent the mobile devices from opening unauthorized means of access to information and other assets. Organization must develop mobile security best practices that can help protect mobile devices and their users from unwanted exposure or unauthorized disclosure of organization information. Organization must enable Bluetooth safeguards (disable or protect these devices), either incorporate these devices into organization's security architecture, or ban their presence altogether. If organization can't secure it, it doesn't need to touch or interact with organization's network. • The following practices aim at securing the Bluetooth-enabled devices themselves. ° Create a policy: Organization must accept that Bluetooth technology is out there and has the potential to interact with their networks. It's important for organization to be proactive; doesn't wait for a Bluetooth-related security incident to occur.

		Instead, organization must develop an organization policy that discusses the use of Bluetooth-enabled devices and defines how these devices can interact with the network. The policy should address three main areas: 1-Support: Bluetooth-enabled devices are not a supported technology, and no one should connect them to the organization network. 2-Data: No one is allowed to store any organization data on any Bluetooth-enabled device specifically, passwords and usernames. 3-Repercussions: Discussing in detail the penalties for violating this policy. ▪ Scan for devices: After organization created and distributed the policy, it is recommended performing a wireless sweep to determine whether Bluetooth is active around organization's physical security boundaries. • The following practices aim to protect the data and applications used in the Bluetooth-enabled device. ° Mobile devices need antimalware software: Any employee who wants to use a mobile device for work should install and update antimalware software for his or her smart phone or tablet. ° Secure mobile communications: All mobile device communications must be encrypted, simply because wireless communications are so easy to intercept and snoop on. Any communications from employees who want to use a mobile device to access applications, services or remote desktops or systems should require use of a VPN for access to be allowed to occur. °Require strong authentication, and use Password controls: Employees should be instructed to enable and use passwords to access their mobile devices, beyond that, mobile devices should be used with multiple forms of authentication to make sure that possession of a mobile device doesn't automatically grant access to important information and systems. Organizations should consider whether the danger of loss and exposure means that some number of failed login attempts should cause the device to wipe its internal storage clean (ability to remotely wipe a smart phone or tablet). ° Control third-party software: Organizations that allow to employees to use mobile devices in work should establish policies to limit or block the use of third-party software. To prevent possible security breaches resulting from installation of rogue software, replete with backdoors, and require such employees to log into a remote virtual work environment. Then, the only information that goes to the mobile device is the screen output from work applications and systems; data therefore doesn't persist once the remote session ends. Since remote access invariably occurs through VPN connections, communications are secure as well, and organization should implement security policies that prevent download of files to mobile devices. ° Create separate, secured mobile gateways: It's important to understand what kinds of uses; systems and applications mobile

		users really need to access. Directing mobile traffic through special gateways with customized firewalls and security controls in place such as protocol and content filtering and data loss prevention tools keeps mobile workers focused on what they can and should be doing away from the office. This also adds protection to other, more valuable assets they don't need to access on a mobile device. ° Require secure mobile devices: Mobile devices should be configured to avoid unsecured wireless networks, and Bluetooth should be hidden from discovery. For examples, when headphones is not in use Bluetooth should be disabled. ° Perform regular mobile security audits, penetration testing: At least once a year, organizations should hire a security testing firm to audit their mobile security and conduct penetration testing on the mobile devices they use. • ***Wireless networking*** is a technology that allows devices such as computers (laptops and desktops), mobile devices (smart phones and wearables), and other equipment (printers and video cameras) to be connected and interface with the Internet without cables. Organizations created a good deal of flexibility with wireless for the employees to work wherever they wanted within an organization's. It will increases in agility, productivity, and morale. Users were no longer forced into working from their desk or conference rooms where network drops resided. But the wireless can be risky. Wireless networks connections can be vulnerable points of access for data or hackers may access employee's connection and compromise sensitive information stored on their devices and in online accounts. So it is important to fix organization security weaknesses before they're exposed, not after. • Wireless security is the prevention of unauthorized access or damage to computers or data using wireless networks, which include Wi-Fi networks. The most common type is Wi-Fi security, which includes Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). • Some security practices to prevent wireless risk: ° Wireless routers offer the option of encrypting data, it should be used. ° Using a secure password using current best practices to make sure it's not easily guessed or cracked. ° Not broadcasting organization SSID and when naming the network should making it not easy to guess and making sure that organization SSID doesn't call attention to organization. ° Organization should not allow any guests onto its private network, and create a separate network for organization's guests in organization wireless access points (WAPs) and then provide them a passphrase when they visit organization's offices. Organization would have a system that generates unique access for them. ° Organization should uniquely connect users to wireless network. Uniquely authenticate each user to organization's wireless network is an important item for wireless security. Providing authenticated access to the wireless network requires IT organizations to implement RADIUS servers and connect those to a central directory service. RADIUS server lets organization

		maintain user profiles in a central database. Hence, organization has control over who can connect with the organization's network. ° Organization should adopt per user (or group) network segmentation with VLANs. Network segmentation via VLANs is important step for improving organization wireless security. The organization can segment it's network so that only users assigned to specific network segments can access those segments. When you utilize a network that has not been segmented, all users are on the same network. That means different employees from different departments share the same network space. For example if computer of an employee in finance section had compromised. That means the entire network is open to that attacker. When organization segments the network, only the finance section would be compromised. This does limit the attack greatly.
Prevention	AC07- Standard Systems/Email Safeguards (anti-phishing, anti-malware etc), prevention system (IDS/IPS,DLP), Firewalls, APT Prevention, Accesses Control, Static And Dynamic Software Code Checkers, Data Classification, IAM.	• Organization should employ automated tools to circumvent poor user decisions, such as developing software to better recognize threats in email messages. • Organization should use anti-malware which includes anti (spyware, viruses, phishing, spam, and email attachments). • Organization should employ ***intrusion Detection system*** (IDS): is a software that automates the intrusion detection process by the process of monitoring the events occurring in a computer system or network and analysing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, accept- able use policies, or standard security practices. • Organization should employ ***intrusion prevention system*** (IPS): is software to detect and prevent identified threats. Intrusion prevention systems continuously monitor network, looking for possible malicious incidents and capturing information about them. The IPS reports these events to system administrators and takes preventative action, such as closing access points and configuring firewalls to prevent future attacks. IPS solutions can also be used to identify issues with corporate security policies, deterring employees and network guests from violating the rules these policies contain. • Organization should ***deploy data loss prevention*** (DLP) software to recognize possible harmful sites, email practices, and other threats it is a technology for the early detection of data exfiltration attempts by a malicious or unintentional insider. DLP monitors traffic and prevents sensitive data from leaving organization' network. It is performed in three steps: 1-system discovery. 2- Leaked confidential data identification. 3- Organization policy enforcement. • Organization should employ firewall: is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. A firewall can be hardware, software, or

		both. • Organization should employ ***advanced persistent threat's prevention*** system. (APT) is an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive data. • Organization should employ ***access control*** system: is a security technique that regulates who or what can view or use resources in a computing environment. • Organization should employ ***static and dynamic software code checkers***: is a software verification activity that analyses source code for quality, reliability, and security without executing the code. By using static analysis can identify defects and security vulnerabilities that can compromise the safety and security of an application. Just analysing the software without running (static), on other hand analysing software as it is running (dynamic). • Organization should employ ***data classification system:*** the process of organizing data by relevant categories so that it may be used and protected more efficiently. • Organization should employ (IAM)***Identity Access Management***: is a technology defining and managing the roles and access privileges of individual network users and the circumstances in which users are granted (or denied) those privileges. The core objective of IAM systems is one digital identity per individual. Once that digital identity has been established, it must be maintained, modified and monitored throughout each user's access lifecycle.
Detection	AC08-Security Information Event Management (SIEM) Systems, Software to Recognize Bogus Emails, EDR, UEBA, CCTV, RFID.	• Organization should employ ***(SIEM) system:*** is a tool that is responsible for centralizing and analysing logging in one management platform, it collects information through secure network channels from various security-related logs (ranging from client workstations and servers to application servers, antivirus software, network devices, honeypots, firewalls, IDSs), and any other sensors in the network, then correlating the events among them in a database by matching any related characteristics and events .This approach allows the information security administrator to quickly search for events and possibly identify malicious insider activity before it occurs, or as a data-mining tool and evidence for forensic investigations after the accident occurs , and safeguard that can detect and prevent data leakage • Organization should employ ***software to recognize bogus emails*** to avoid Phishing and scam emails. • Organization should employ (EDR) ***Endpoint Detection and Response***: is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities. The tools primarily focused on detecting and investigating suspicious activities and traces of such problems on hosts/endpoints.EDR is focused on providing the right endpoint visibility with the right insights to help security analysts discover, investigate and respond to very advanced threats and broader attack campaigns stretching across multiple endpoints. • Organization should employ (UEBA) ***User and Entity Behaviour Analytics***: is a security process that takes note of the normal conduct of users. In turn, they detect any anomalous behaviour or instances when there are deviations from these normal patterns.

		For example, if a particular user regularly downloads 10 MB of files every day but suddenly downloads gigabytes of files, the system would be able to detect this anomaly and alert them immediately .UEBA can analyse the behaviour across multiple users and ICT devices, such as routers, servers, and endpoints in order to detect complex attacks and to detect potential intrusions and malicious activity and to detect users and entities that might compromise your entire system. • Organization should employ (CCTV) ***Closed-circuit television*** for video recording of employee job performance and detect employee's activity to reduce and stop data loss. • Organization should employ (RFID) ***Radio-Frequency Identification:*** is a technology uses radio waves to identify people or objects. It can be found in car keys, employee identification, medical history/billing, highway toll tags and security access cards. It can used to track employee movements and help provide them access to secure locations. An example of tracking employees can be an organization's basic attendance system. Usually, companies give each employee an ID badge.

Table 4: The proposed relations in the Initial (UITCM)/Second Version

No	Relation	Description
1	Managerial□□Defence Tools (Detection, Prevention, Incident response) □Behaviour	Laws and regulations, policy enforcement, Procedure, Standard and Best practice fall under the administrative controls (Managerial group), they clearly show the acceptable use of an organization's system, network, and information and what is expected from employees and also the possible consequences of violations. Thus they are the documented theoretical side from the cyber security program that provides a roadmap for effective security. Whereas, Prevention, Detection and Incident response tools are the technical and operational side of a cyber security program to increase the chances of preventing, detecting and responding to insider threats (Detection, Prevention, Incident and response groups).Both the administrative controls side and technical controls side represent together an effective security program that is able to both, dealing with incidents proactively and can respond to incidents quickly, through control measures in place, rules and controls in order to detect and get alerted about the actions of its employees. Administrative controls and technical controls together produce deterrent measures that control employee behaviour and reduce or prevent their errors and reduce their consequences, to proactively protecting data and to ensure compliance with regulations, rules, laws, so that it prevents the occurrence of the accident or mitigate its potential risks. Managerial group has a direct influence on controlling the employees' behaviour. Laws and regulations, imposes using the technical controls and adopting control measures in place, rules and controls that leads to controlling employees' behaviour. Therefore, the UITCM proposed a relationship among managerial group, defence tools (incident response, prevention, and detection groups) and behaviour group. The managerial group is responsible to impose and adopt defence tools in an organization, (Detection, Prevention and Incident Response) which in turn constitute deterrent measures that control employee behaviour and reduce or prevent error and its consequences. For example law and regulations, imposes using (SIEM) systems and CCTV which detects negligent employee behaviour. Law and regulations, imposes using automation for password changing reminder to enforcing employees to change their devices passwords, and imposes adopting remote memory wipe In the case employee lost his device.
2	Managerial □□ Culture□□Behaviour.	Organizational culture consists of the beliefs, practices, attitudes, behaviour, reputation and ethics of an organization and its employees. Group norms influence individuals' security behaviour. Thus, perceptions of risks are influenced by the cultural context in which they are formed. What is perceived as a risk is shaped by cultural beliefs, social relationships, power relationships, hierarchies, knowledge, experience, discourse, and practice in organization. People generally follow group norms, and therefore if the group considers information security to be an important and serious problem, then it is more likely that the individuals within that group will value and follow the security policies. Conversely, if risk-taking is accepted within the group, then it is likely that greater risks will be taken. Organizational policies, practices, laws, regulations, procedure, standards, processes, and written values inform and shape organizational cultural knowledge, actions, and, ultimately, perceived risks. They also provide guidance on what behaviours are deemed appropriate, ideal, or inappropriate; they establish expectations and inform cultural knowledge.

		It is important to make all employees all employees receive and sign a copy of organization's policies. Through this, the employees are made aware of what is expected from their job roles and the penalties for violation of these policies are clearly agreed upon and having security awareness training, with a specific chapter dedicated to unintentional insider threat in order to explain what is expected from them and which threats they might be exposed to. Laws and regulations should set strict organizational rules, provide for penalty against any person who exceeds organization's policy or violates it's rules ,then enforce policy and procedures to ensure compliance with regulations, rules, laws, to deliver a clear message of information security policy to the rest of the organization and develop individual values, institutional values and behavioural expectations for the organization to support the implementation of the management system and deploy security culture to mitigate risks. Based on the above. The UITCM proposed a relationship among culture, behaviour and managerial groups. The Managerial group is responsible for spreading the security culture in organizations and the organizational culture greatly influences employee behaviour. For instance, group norms can affect individuals' password behaviour. If organization's laws and regulations, provides for penalty against any person who exceeds policy of password sharing, therefore, refusing to share a password could be seen as a compliance with the organization's security policy and not a sign that people do not trust their colleagues. Furthermore, policies regarding the reporting of careless behaviour of a co-worker can help in defending against the unintentional insider threats.
3	Managerial □□Psychological□□ behaviour.	Psychological problems such as drug side effects and mental problems can negatively affect operator performance and can contribute to errors. Organization's laws and regulations should consider psychological problems of employees and thereby reducing the likelihood of the incidents related to working under the influence and encourages greater responsibility among employees who may cause harm to information system. Thus the UITCM proposed a relationship among psychological, behaviour, and managerial groups. Where physiological state affects employee behaviour and managerial group is responsible for mitigating risks of physiological employee state, by some procedures such as necessary tests and suitable work environments. For example if organization's laws and regulations impose mental abilities test and drug test as a condition of employment , potentially non-trustworthy candidates can be identified at the application stage and avoid those who may cause harm to information system.

4	Managerial □Process □Psychological □behaviour.	Problems in data flow and increased workload both can negatively affect operator performance and contribute to errors. Similarly, problems in work setting and management systems, such as lack of available qualified staff or inadequate or flawed policies, may lead to increased workload, increased stress, or other factors that affect information processing and decision making and lead to errors and failures. Problems with work planning and control, such as changes in routine, can affect performance through increased fatigue or stress. Deficiencies in employee readiness tends to negatively impact performance due to insufficient knowledge for correct task completion, as well as associated anxiety and stress that further affects judgment and decision making. Stress is a major contributing factor to human error. Stressful situations include unfamiliar or exceptional occurrences, incidents that may cause a high loss of money, data, or life, or time critical tasks. Human performance tends to degrade when stress levels are raised. Intensive training can reduce this affect by making unusual situations a familiar scenario with drills. However, the cases where human beings must perform at their best to avoid hazards are often the cases of most extreme stress and worst error rates. According to this the UITCM proposed a relationship among process, psychological, behaviour, and managerial groups. Where work processes affect physiological state of employee and physiological state affects employee behaviour and managerial group is responsible for controlling work processes and for its effects on employee behaviour. Therefore when determining the relationship between process and behaviour groups, physiological group must be taken into account. Likewise, when determining the relationship between process and physiological groups, behaviour group must be taken into account. Since they are related and managerial group can mitigating risks of physiological employee state. For example if organization's laws and regulations do not consider work planning and work setting, that can lead to increasing fatigue or stress. Thus, it affects employee readiness and then his performance and may contribute to human error.

APPENDIX F: MODEL VALIDATION QUESTIONNAIRES

ROUND 1 : Evaluation of the proposed Unintentional Insider Threats Countermeasures Model (UITCM)

1. Research Background

An unintentional action usually may lead to financial losses or affect the reputation of institutions. The actions can be due to activities such as sending an email containing sensitive information to wrong address, or accidentally publishing sensitive information to the public or by the loss of laptops or memory that contains important information, these actions known as an unintentional insider threat. These threats happen due to the employees unaware about the related IT security, procedure, or guideline in the organization. This study proposed a conceptual model as a countermeasure towards unintentional insider threats.

2. Objective

The objectives of the study are:

a. To analyze the issues related to an unintentional action made by employees who deal with sensitive information in Malaysian organizations.

b. To evaluate the relevancy of the proposed model against the unintentional insider threats to be used in organizations. This evaluation is to be achieved by asking experts of the field, questions about the components and design of the proposed model.

3. Participant

An expert who has relevant knowledge to the research area. Participant can assist in the development of a new countermeasure model to mitigate unintentional insider threats in the organizations. All personal details will not be included on any written materials in this questionnaire, in any publication and the research.

4. Questionnaire Process

Participant will be asked to read and evaluate the proposed model and answer questions about components, design of the proposed model. Participants are required to:

- Review the design of the proposed model and evaluate the relevancy of the components.
- Check whether the proposed model meets the use's requirements, theoretically valid, readable, and adaptable.

The study will use Delphi technique and the questionnaire will be in two rounds:

- Round One (Open-ended questions).
- Round two (Close-ended questions).

For each round participant will be given a minimum of one week to send the feedback.

QUESTIONS & ANSWERS (Please refer to UITCM Model.pdf which attached as a separate file).

Please answer all the following questions: -

Participant Information

Q1: Please fill the table.

Gender	
Position	
Total years of working experience	

Theoretical validity

Q2: In evaluating this model please identify any aspect that is not appropriate and relevant to be in the elements of the model.

Remove	Reason for removal

Q3: In evaluating this model please identify any countermeasures aspects of unintentional insider threats that are not covered in the model.

Add	Reason for Adding

Q4: Please identify any aspects of the model that can be improved.

Improve	Reason for Improving

Usability

Q5: Can the model be used in the organizations? How can it be used, and how can it be useful?

Readability and understandability

Q6: Are the terms used in the model clear and easy to understand? If no, what is your suggestion to improve it?

Q7: Are the relationships between components of the model are logical? If no, what is your suggestion to improve it?

Q8: Is the model readable and understood? If no, what is your suggestion to improve it?

**Thank you for your willingness to participate in this questionnaire and it is highly appreciated.

ROUND 2 : Evaluation of the Unintentional Insider Threats Countermeasures Model (UITCM): Revised Version

Questionnaire Title: Evaluation of the Revised Version of Unintentional Insider Threats Countermeasures Model (UITCM)

Round 1 Finding:

Delphi method was used in this research. Delphi required minimum of two rounds of evaluation. Round 1 findings should be shown in the beginning of Round 2 Questionnaire.

Round 1:

There are five participants took part in the Round 1 Questionnaire.

Five participants have completed the questionnaire. The summary of findings can be referred in Appendix A.

Round 2:

Participants are required to complete the questionnaire based on the updated/revised version of UITCM Model. The model has been revised and updated based on the comments in Round1.

Questionnaire Process

Participant will be asked to read and evaluate the revised version of the model and answer all questions related to the model. Participants are required to:

- Review the design of the revised model and evaluate the relevancy of the components.
- Check whether the revised model meets the use's requirements, theoretically valid, readable and adaptable.

The study will use Delphi technique and the questionnaire in Round 2 will be ***Close-Ended Questions.***

Participant will be given a minimum of one week to send back the feedback.

Thank you for your willingness to participate in this questionnaire and it is highly appreciated.

QUESTIONS & ANSWERS

(Please refer to UITCM Model.pdf which attached as a separate file.)

Please answer all of the following questions based on data gathered in round 1:-

Theoretical Validity

Objective: The objective of this section is to review relevancy of the components in the model.

Q1: Please rate the RELEVANCY of the components in the model. Rating Scales are from scores 1 to 3 with "Not Relevant, Relevant and Strongly Relevant" accordingly.

Element	Not Relevant (1)	Relevant (2)	Strongly relevant (3)
Law and Regulation, Policy Enforcement, Procedure, Standard, Best Practice, Baseline, Standard Operating Procedure (SOP), Guidelines.			
Maintain Employee Readiness.			
Improve Data Flow.			
Effective Security Practices.			
Maintain Staff Values.			
Improve Design of User-System Interface (UI).			
Affordable Access to Mental Health/Drug Treatment Services.			
Appropriate Time Off For Employees.			
Team-building Activities.			
Improve Design of Work Environment.			
Improve Work Planning and Control.			
Improve Work Setting and Management Practices.			
Command And Control Centre.			
Incident Logs.			
Advisories.			
Risk Analysis And Auditing.			

Incident-driven Reviews (Policies, Practices, Training Materials).			
Periodically, Fully Re-evaluate Risk.			
Ethical Hacking.			
Regular Vulnerability Scans.			
Developing Incident Response Plan.			
Monitor Employee Behaviour.			
Trust model With Permission Authentication From Higher Level Employee.			
Collaborative Reinforcement Model.			
Mental and IQ Test.			
Drug Testing.			
The Cognitive Reflection Test (CRT).			
Stimulation Of Risk Perception.			
Security Education, Training, Awareness, Instrumental Conditioning.			
Usability of Software /Security Tools.			
Encourage Following of Policies.			
Employee Assistance Programs (EAPs).			
Respectful And Calm Workplace Environments.			
Watermarking Forensic, Intelligence Operation.			
Backup Systems (Spatial /Temporal) Replication.			
Remote Memory Wipe For Lost Equipment.			
Automation.			
Data Encryption/Password Protection.			
Wireless And Bluetooth Safeguards.			
Standard Systems/Email Safeguards (anti-phishing, anti-malware etc), prevention system (IDS/IPS,DLP), Firewalls, APT Prevention, Accesses Control, Static And Dynamic Software Code Checkers, Data Classification, IAM, Website Controls.			
Security Information Event Management (SIEM) Systems, Software to Recognize Bogus Emails, EDR, UEBA, CCTV, RFID.			

Usability

Objective: The goal objective of this section is to review the usability of the model.

Q2: The model can be used and adopted in organizations.

Yes	No

Q3: The model can be used in organizations that deal with confidential information. It can be used as a guidelines and a checklist that help organizations assess the status of their UIT mitigation measures. In addition it can be used to guide all the employees of the organization in being safe online.

Yes	No

Readability And Understandability

Objective: The objective of this section is to review the terms, connections, flows, design, and readability of the conceptual model.

Q4: The terms used are clear and easy to understand.

Yes	No

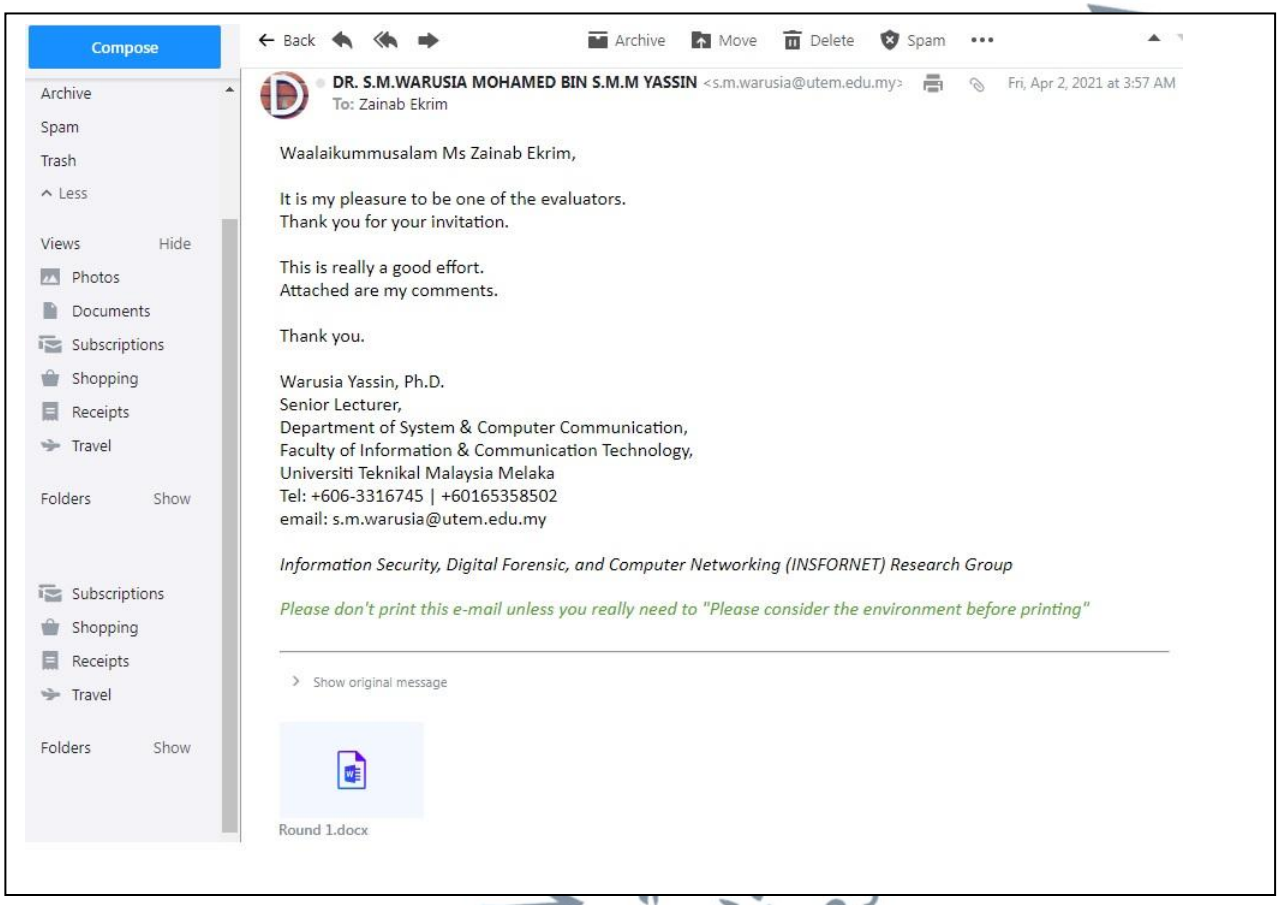
Q5: The connections and flows of all of the components are logical.

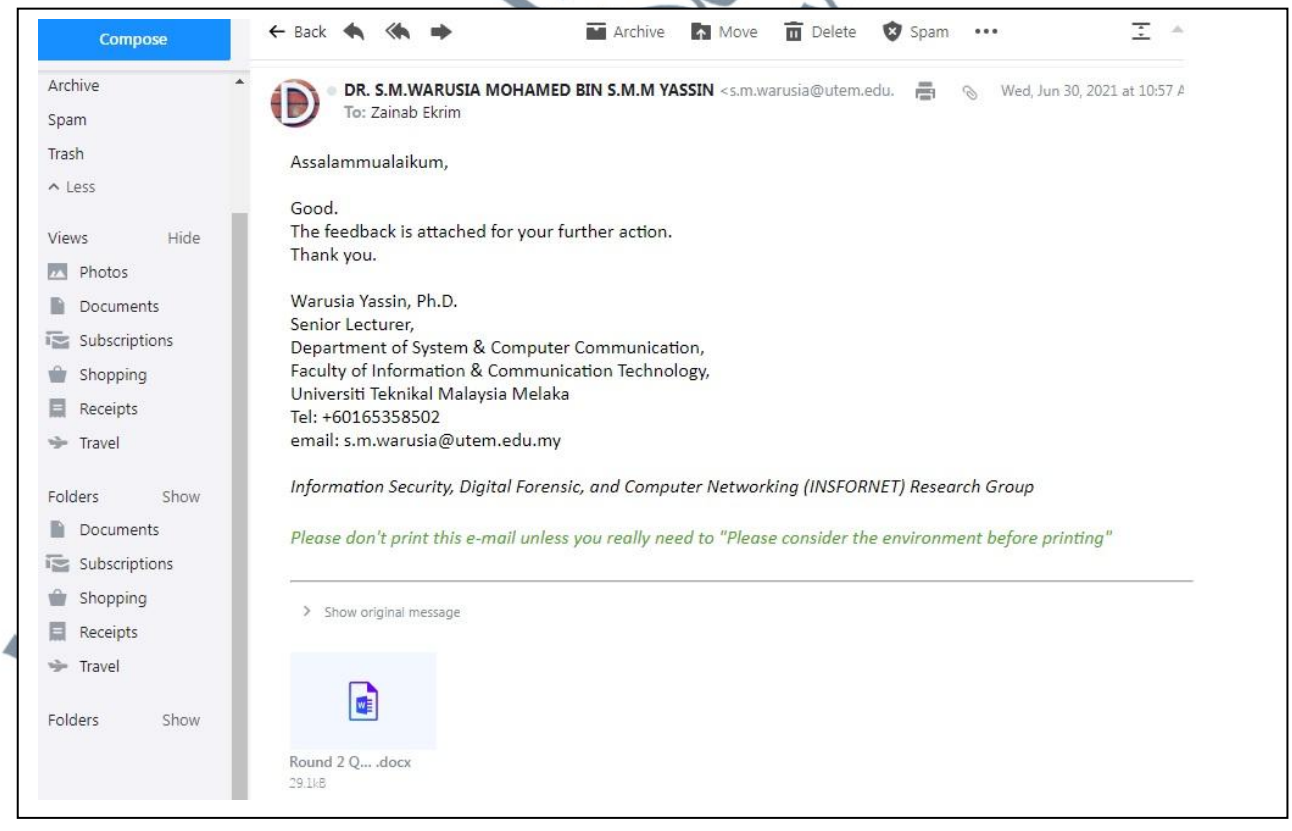
Yes	No

Q6: Overall, the design of the conceptual model is readable.

Yes	No

APPENDIX G: SAMPLES OF EXPERT RESPONSE VIA EMAIL





APPENDIX H: QUESTIONNAIRES RESPONSE SAMPLES

ROUND 1 : Evaluation of the proposed Unintentional Insider Threats Countermeasures Model (UITCM)

Participant Information

Q1: Please fill the table.

Gender	Male
Position	Lecturer
Total years of working experience	21 Years

Theoretical validity

Q2: In evaluating this model please identify any aspect that is not appropriate and relevant to be in the elements of the model.

Remove	Reason for removal
None	

Q3: In evaluating this model please identify any countermeasures aspects of unintentional insider threats that are not covered in the model.

Add	Reason for Adding
IQ testing	Adding IQ testing separate from mental problems testing can improve psychological evaluation and monitoring.
Ethical hacking	Ethical hacking can be added improve employee response to different types of security

Q4: Please identify any aspects of the model that can be improved.

Improve	Reason for Improving
Behaviour : Trust model Drug testing	Can be improved by adding permission authentication from higher level employee. Must be described clearly to distinguish between legal and illegal drugs. Also it must be related to a good health insurance system that manage drug usage.

Usability

Q5: Can the model be used in the organizations? How can it be used, and how can it be useful?

It can be used in organizations that deal with confidential information related to their type of work or employee.

Readability and understandability

Q6: Are the terms used in the model clear and easy to understand? If no what is your suggestion to improve it?

The terms used in the model are clear an easy to understand. Abbreviations can be added to some will known terms like user system interface etc.

Q7: Are the relationships between components of the model are logical? If no, what is your suggestion to improve it?

The relationships between the model components logical. But the source and destination of the relation arrows are not clear.

Q8: Is the model readable and understood? If no what is your suggestion to improve it?

The model is readable and understood easily.

**Thank you for your willingness to participate in this questionnaire and it is highly appreciated.

ROUND 2 : Evaluation of the Unintentional Insider Threats Countermeasures Model (UITCM): Revised Version

(Please refer to UITCM Model.pdf which attached as a separate file).

Please answer all of the following questions based on data gathered in round 1:-

Theoretical Validity

Objective: The objective of this section is to review relevancy of the components in the model.

Q1: Please rate the RELEVANCY of the components in the model. Rating Scales are from scores 1 to 3 with "Not Relevant, Relevant and Strongly Relevant" accordingly.

Element	Not Relevant (1)	Relevant (2)	Strongly relevant (3)
Law and Regulation, Policy Enforcement, Procedure, Standard, Best Practice, Baseline, Standard Operating Procedure (SOP), Guidelines.			/
Maintain Employee Readiness.		/	
Improve Data Flow.		/	
Effective Security Practices.			/

Maintain Staff Values.		/	
Improve Design of User-System Interface (UI).		/	
Affordable Access to Mental Health/Drug Treatment Services.		/	
Appropriate Time Off For Employees.		/	
Team-building Activities.		/	
Improve Design of Work Environment.		/	
Improve Work Planning and Control.		/	
Improve Work Setting and Management Practices.		/	
Command And Control Centre.		/	
Incident Logs.		/	
Advisories.		/	
Risk Analysis And Auditing.		/	
Incident-driven Reviews (Policies, Practices, Training Materials).			/
Periodically, Fully Re-evaluate Risk.			/
Ethical Hacking.		/	
Regular Vulnerability Scans.			/
Developing Incident Response Plan.			/
Monitor Employee Behaviour .		/	
Trust model With Permission Authentication From Higher Level Employee.			/
Collaborative Reinforcement Model.		/	
Mental and IQ Test.		/	
Drug Testing.		/	
The Cognitive Reflection Test (CRT).		/	
Stimulation Of Risk Perception.		/	
Security Education, Training, Awareness, Instrumental Conditioning.			/
Usability of Software /Security Tools.			/
Encourage Following of Policies.		/	
Employee Assistance Programs (EAPs).		/	
Respectful And Calm Workplace Environments.		/	

Watermarking Forensic, Intelligence Operation.		/	
Backup Systems (Spatial /Temporal) Replication.		/	
Remote Memory Wipe For Lost Equipment.		/	
Automation.		/	
Data Encryption/Password Protection.			/
Wireless And Bluetooth Safeguards.		/	
Standard Systems/Email Safeguards (anti-phishing, anti-malware etc), prevention system (IDS/IPS,DLP), Firewalls, APT Prevention, Accesses Control, Static And Dynamic Software Code Checkers, Data Classification, IAM, Website Controls.			/
Security Information Event Management (SIEM) Systems, Software to Recognize Bogus Emails, EDR, UEBA, CCTV, RFID.		/	

Usability

Objective: The goal objective of this section is to review the usability of the model.

Q2: The model can be used and adapted in organizations.

Yes	No
/	

Q3: The model can be used in organizations that deal with confidential information. It can be used as a guidelines and a checklist that help organizations assess the status of their UIT mitigation measures. In addition it can be used to guide all the employees of the organization in being safe online.

Yes	No
/	

Readability And Understandability

Objective: The objective of this section is to review the terms, connections, flows, design, and readability of the conceptual model.

Q4: The terms used are clear and easy to understand.

Yes	No
/	

Q5: The connections and flows of all of the components are logical.

Yes	No
/	

Q6: Overall, the conceptual design model is readable.

Yes	No
/	

APPENDIX I: FINAL VERSION OF UITCM /COMPONENTS DESCRIPTION AND RELATIONS

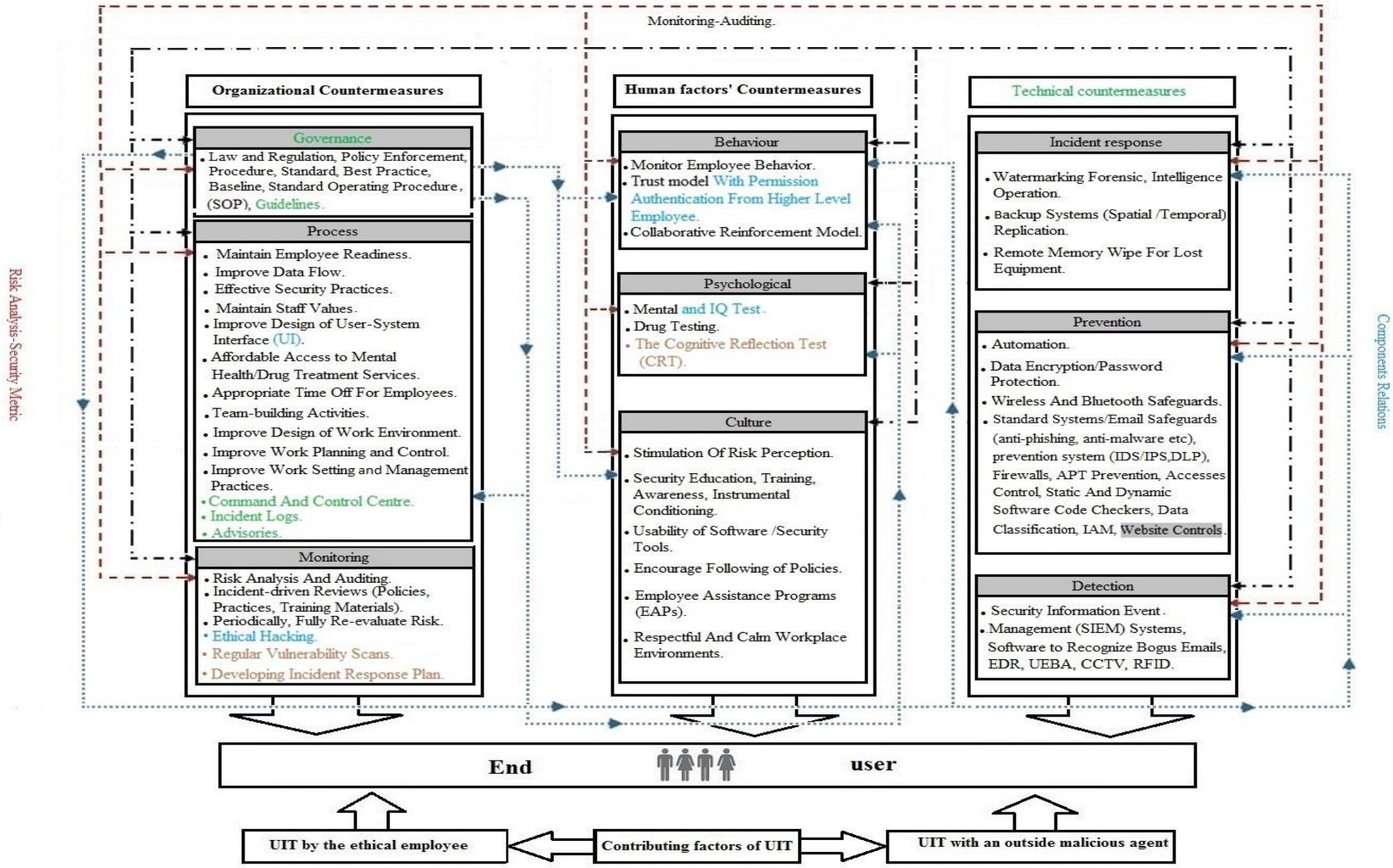


Figure 1: The Final Version of unintentional insider threats countermeasures model (UITCM)/ Validated Model

Table 1: Abbreviations of Final Model Components

Abbreviations	Description
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
DLP	Data Loss Prevention
APT prevention	Advanced Persistent Threat
SIEM	Security Information Event Management Systems
EDR	Endpoint Detection and Response
UEBA	User and Entity Behaviour Analytics
CCTV	Closed-circuit television
RFID	Radio-Frequency Identification
IAM	Identity Access Management

Table 2: Organizational Countermeasures Components.

UITCM		
The Organizational Countermeasures Components		
Component	**Element**	**Description**
Governance	OC01-Law and Regulation, Policy Enforcement, Procedure, Standard, Best practise, Baseline, Standard Operating Procedure (SOP), Guidelines.	• Organizations should adopt a security program that deals with unintentional insider threats and takes them into consideration. Security program is a documented set of ***organization's information security policies, procedures, regulations***, ***and standards***. Organization should has law ,***regulations, policy , Procedures, standards, best practice, baselines and standard operating procedure*** that deals with all aspects of unintentional insider threats. • ***Information security law*** is the body of legal rules, codes, and standards that require organization to protect information and the information systems that process it from threats including UIT. • ***A regulation*** is the process, or body, responsible for ensuring that the law is put into effect. A regulation explains the details necessary, whether technical, operational or legal, to put the law into effect, for example it is mandatory for businesses to dispose and destroy of customer information in its custody when the records are no longer related to the business. Civil criminal and monetary penalties would be levied on anyone browsing, selling or unlawfully accepting customer's records by law. To prevent occurrence of such failures, regulations should be created to require employees to dispose customer's data in an appropriate manner.

		•***Policies*** are the top tier of formalized security documents. These high-level documents offer a general statement about the organization's assets and what level of protection they should have, and it is a set of rules that guide individuals who work with IT assets Well-written policies should spell out who's responsible for security, what needs to be protected, and what is an acceptable level of risk. They are much like a strategic plan because they outline what should be done but don't specifically dictate how to accomplish the stated goals. Those decisions are left for standards, baselines, and procedures, and implementing security best practices throughout the organization, as defined by widely tested and implemented security norms in the industry. The difference between policy and procedures is that they are generic, the policy are there to serve as a guide but do not provide detailed specifics in implementation. An effective information security procedure must include identify and remediate UIT. • ***Information Security Best Practices*** are a set of guidelines, ethics, or ideas that represent the most efficient of action in a given task. To decrease UIT encompass being cautious when engaging in online activities, abiding by organization rules, and reaching out for help when encounter something suspicious. • ***A Standard Operating Procedure(SOP)*** is a document that consists of a set of instructions or steps on how to execute a task step-by-step.(SOP) serves as a tool to ensure that activities are performed properly. Though it follows the ISO format, the document and the process belong to the organization. They are unique to a company or organization. Using SOP reduces the possibility of human error. • Organizations should adopt ***standards*** that supposed to reduce the feasibility and likelihood of the unauthorized release of classified information and addresses gaps in policy for information systems security, including characterization and detection of UITs, for examples :- ° The ISO/IEC 27001: Information Security Management System is a standard for information security that is highly considered in any cybersecurity policies and guidelines. ° ISO/IEC15408: This is the Common Criteria Standard with regards to certified security function of the ICT product. One of the way for organization to minimize cyber threats is to procure Common Criteria certified ICT products. ° The ISO 9001:2015 standard on human errors. ° The ISO 9001:2015, 8.5.1.g, requires organizations to carry out service provision under controlled conditions, which include taking actions to prevent human error. ° According to ISO/TS 9002:2016, the actions to prevent human error may include: ▪ Limiting excessive working hours. ▪ Putting in place a more suitable working environment.

		▪ Providing appropriate training and instructions. ▪ Automating processes. ▪ Requiring double electronic entry of critical information. ▪ Making available devices to avoid incorrect tooling. ▪ Avoiding distractions (such as personal electronic devices). ▪ Rotating jobs. ▪ Requiring completion of information before submission. ▪ Planning of Changes. ° The intent of ISO 9001:2015, 6.3, Planning of changes, is to determine the need for changes to the organization's quality management system in order to adapt to changes in its business environment, as well as, to ensure that any proposed changes are planned, introduced, and implemented in a controlled manner. Properly planning a change can help to avoid negative consequences. It can also result in positive outcomes, such as the reduction of nonconforming outputs or reduced incidents of human error. ° The intent of ISO 9001:2015, 7.1.4, Environment for the operation of processes, is to ensure the organization determines and provides the necessary environment for the operation of its processes and to facilitate provision of conforming services. Whereas, human factors can be critical in a process; therefore, they should be considered when determining the environment for the operation of the processes, e.g., by avoiding high workloads and stress for employees (to prevent potential errors, burn-out). • ***Guidelines***: Guidelines offer general recommendations or instructions that provide a framework for achieving compliance with standards. They are more technical in nature and are updated on a more frequent basis to account for changes in technology.
Process	OC02-Maintain Employee Readiness.	•***Employee readiness*** is the extent to which having the personal characteristics such ability, attitudes, awareness, belief, activity, calm and motivation. These characteristics are necessary in order for them to perform the work tasks as they should. •To maintain employee readiness organizations should implement practices that reduce inattention, stress and anxiety, fatigue and boredom, and effects of illness and injury such as giving breaks, use automated reminder tools to change passwords periodically, material and moral incentives, granting sick leave, boost employees' confidence and enhance awareness of drug and hormone side effects and cognitive factors.

Process	OC03- Improve Data Flow.	For an organization to get conquer a handle on its own data, it must have a coherent picture of how data flows through organization from beginning to end during data collection and creation, data storage, data use and transfer, data destruction and retention. • Organization must be concerned with: ° Who has sensitive data, what kind of sensitive data are they, where are the data stored, where did they come from, why were they collected, are they used for that purpose, are they used for other purposes, are the data transferred to other departments, third parties, clients, abroad? Who has access, how long are the data retained? ° How data are stored and transferred, which connections are secure or encrypted? ° What are data sources (data analysts, vendors, suppliers, partners, other departments)? ° How the data are obtained (hard-copy forms, telephone, mobile, email, online, web application, mobile application, desktop application, fax)? ° What are the places in which data are stored, both physically and digitally (e.g. databases, filing cabinets, tapes, network share drive, external hard-drive, personal laptop) and identify where these physically are? ° Where are the data processed and where they are transferred to (manual processing, digital processing, other departments, agencies, clients, vendors, regulators and authorities? ° Are data retained and destroyed in accordance with organizational policies and standards? (Hardcopy documents getting scanned for archiving purposes, system backup tapes, physical file archives, files held on laptops, when you end a relationship with a client or fieldwork agency, what happens with the data?) ° Are the means of transfer secure, is the transfer automated or manual? Is the form of the data secure (Excel, SPSS, PDF, audio/video, emails and attachments). ° What is required by law? And how well are organization's processes in line with national laws ,local requirements or the data privacy laws in the country or in all countries concerned if the organization has established cross-border data transfers.? •Organization should improve data flow by enhancing communication and maintaining accurate procedures and directions in the exchange of messages and data and ideas between people inside and outside of the organization, enhance information security awareness and motivate employees to comply with security policy, and communicate effectively with employees to ensure that they are aware of information security policy and understand the reasons for its effective implementation. For example, an organization could be storing sensitive data in the most secure cloud you could find, but if the data are transferred to this cloud unencrypted, they are still vulnerable.

Process	OC04- Effective Security Practices.	• Security program are implemented by several means: ° Technical: software, hardware, or firmware. ° Physical: physical barriers, locks, etc. ° Administrative: the actions and practices of people. • Security technology is important to security (firewalls, intrusion detection software, virus scanners), but the practices of the people who develop, integrate, evaluate, configure, maintain, and use that technology are more important; indeed, these practices are the foundation of technical (as well as physical and personnel) security. It is crucially important, therefore, that security practices be good ones; when feasible, best security practices should be used. • Security practices is a human practice; that is, a repeated or customary method used by people to perform some process and not an IT security mechanism, which is implemented by hardware, software, or firmware. • Some examples of security practices ° Use multifactor authentication :using the multi-factor authentication (MFA)settings on most major network and email products is simple to do and provides an extra layer of protection to Increasing user account security. such as using employees' cell numbers as a second form, since it is unlikely a thief will have both the PIN and the password. (MFA) can employs biometric in addition to user passwords can prevent attackers from being able to use a stolen password. ° Plan for mobile devices (it is essential that organizations have a documented mobile devices policy and include these devices in a policy such as smart watches and fitness trackers with wireless capability). ° Document organization's security policies. ° Educate all employees. ° Enforce safe password practices: Organization should have a passwords security policy that includes password expiration and complexity(using a longer password and changing it regularly) ,this can further enhance security by rendering compromised passwords useless. ° Organization should install all the latest patches and updates to protect systems against vulnerabilities and security issues. ° Back up all data regularly.

		°Install anti-malware software. ° Turning off default settings: It's possible for default settings to open the way for cyber attacks. While these settings might promote operational efficiency, they can prove dangerous for system. It is recommended turning off legacy settings when possible. ° An important practice enterprises should implement is to put in systems where users can quickly and easily report a phishing attack, have it routed to IT, have it filtered and have it put in a system so that IT can quickly and easily add it to blacklists that will protect both internal employees and those that are remote or on mobile devices. ° Setting the responding rules: When an email, text, or phone message asks an employee to approve a fund transfer, share sensitive information, or take some other action that could result in a security breach, that employee should perform an independent verification of that communication. Instead of replying directly to the sender, the employee should reach out to higher level employee through pre-established channels.
Process	OC05- Maintain Staff Values.	• ***Organizations' values*** are the fundamental beliefs of an organization, the guiding principles that dictate how people should behave and act. Organization must maintain staff values and attitudes that align with organizational mission and ethics. The values statement, also called the code of ethics, differs from both the vision and mission statements. The vision and mission state where the organization is going (vision) and what it will do to get there (mission). They direct the efforts of people in the organization toward common goals. The values statement defines what the organization believes in and how people in the organization are expected to behave with each other, with customers and suppliers, and with other stakeholders. It provides a moral direction for the organization that guides decision making and establishes a standard for assessing actions. It also provides a standard for employees to judge violations. Together, the vision, mission, and values statements provide direction for everything that happens in an organization. They keep everyone focused on where the organization is going and what it is trying to achieve. And they define the core values of the organization and how people are expected to behave. They are not intended to be a straitjacket that restricts or inhibits initiative and innovation, but they are intended to guide decisions and behaviours to achieve common ends. • An organization's values help people know the difference between right and wrong, and they help organizations determine if they are on the right path to fulfilling their business goals. The values statement defines how people in the organization should behave. It provides a guideline for decision making. Organization's workplace values set the tone for an organization's culture, and they identify what organization, as a whole, cares about. It's important that values of area's people align with organization's values. When this happens, people understand one another, everyone does the right things for the right reasons, and this common purpose and understanding helps people build great working relationships. Values alignment helps the organization as a whole to achieve its core mission. • Some examples of organization's values : ° Making a difference, respecting company policy and rules, and respecting others, focusing on detail, delivering quality,

		being positive, being completely honest, being a great team member, keeping promises, helping others, showing tolerance, being reliable and caring about deadlines. ° A problem solver: Solving one problem after the next will lead to building a great organization and that required people that are excited to hop from one problem to problem. ° Ambitious: Not just wanting things to happen, not watching things to happen but making things happen. Ambition can be a really powerful value if it leads to people being the change they want to see. ° Transparent: That if people are honest, open and direct in all conversations organization saves a lot of time. ° Empathetic: The ability to understand the challenges that others deal with, and how can help them thrive to hit their goals and maximize their potential. ° Adaptable: means how well does a person handle with vary conditions and to improve is to change, how well we adapt to change will determine how our success will be. ° Focused: If one is focused on doing too many things he won't do anything really well. ° Integrable: Integrity is the quality of being honest and having strong moral principles; moral uprightness. Organization should surround itself with people who care deeply about integrity. ° Accountable: The obligation of an individual to account for his or her activities, accept responsibility for them and to disclose their results in a transparent manner. • However, managers cannot just create a values statement and expect it to be followed. •Maintain staff values and attitudes that align with organizational mission and ethics can be achieved via establish good relationships in the workplace, encourage the development of positive relationships between managers and employees as well as amongst co-workers, setting clear goals, communicate effectively with employees, showing appreciation, building a strong team, sending a clear message, improving the openness at work, improving the behaviour of the individuals in an organization, getting beyond the, negative with staff development and, creating open communication in the workplace. Senior management shall act as role models in the visible promulgation of these values and expectations. Avoiding a culture of disloyalty and distrust within the organization and voiding authoritarian leadership such as (the use of one-way communication from top to bottom with an emphasis only on work progress, and final decisions usually made by the upper-level of management). Instead, another leadership should be adopted such as paternalistic leadership, or belief in reciprocity (e.g., work hard and the organization will offer a person more bonuses), participative leadership (e.g., authority is greatly decentralized), servant leadership (i.e., the perception that a leader's primary duty is to help subordinates to fulfil their desires, or interests), or leadership that has the

		capability to inspire organizational success and influence followers' beliefs and leading by example for example if one of an organization's values is to give more. The organization can do this by giving employees hours of paid time off each year to volunteer, or having its own charitable foundation based on service learning, social investments, donations and awards. • Keeping the organization's moral values at the forefront of everyone's mind by making it prominent within the workplace. In addition to featuring it on the company website and in the employee handbook, post it where employees often gather (conference rooms, snack rooms, etc.). , painting them on the walls throughout the office, to serve as a daily reminder for organization's employees. Reminding employees of values doesn't stop after crafting, laminating and posting posters throughout the office, however. They need to convert into specific, behavioural examples. By modelling and rewarding behaviours that demonstrate each value, employees are constantly reminded of what their organization stands for and how to better work by those principles. The best way to maintain staff values and attitudes is to model them. In other words, don't just let them sit on the wall and call it a day. Live, work and play by them on a daily basis. Most important, leading by example. Showing employees how it's done by using organization character to guide business decisions and empowering employees to do the same. Promote organizational values by rewarding behaviours that demonstrate them. Don't hesitate to publicly reward someone for exhibiting behaviours that are in line with the organization's character. Not only does this make the individual feel good, it also pushes the rest of the organization to follow suit. To hire based on values, for each of the organization's values, should developing a list of questions designed to assess a candidate's character and potential fit. For instance, if one of an organization values is that they are team entrepreneurial. Asking interview questions related to a candidate's ability to be enterprising is essential to finding talent that shares and fulfils the organization's values.
Process	OC06- Improve Design of User-System Interface (UI).	• ***User interface*** is the features of a computer system which allows the user to interact with it. A user interface, also sometimes called a human-computer interface, comprises both hardware and software components. It handles the interaction between the user and the system. Interfaces include organizational factors and operational factors that manage the flow of information throughout the system, and maximize the accuracy, timeliness, and usability of information as set out in a company's Management Systems. Human operators are one of the biggest sources of errors in any complex system. Many operator errors are attributed to a poorly designed human-computer interface. System design and human interaction both play a role in how often human error occurs particularly when there is a slight mismatch between the system design and the person operating it, the ease and complexity of systems and software design , font colour and font size that cause optical dispersion can affect the user of information systems. A poorly designed system interface make errors more likely .When the system interface is poorly designed and confusing to use, the users will make similar types of mistakes. Security may be compromised when humans make mistakes at the user interface. Certain user-interface design drives users toward error, while other facilitate success and encourage the operator to perform correctly and protect the system from common operator errors. • Examples of features of a good user interface: ° The user interface must give appropriate feedback to the operator to allow him to make well informed decisions based on the most up to date information on the state of the system. If the user must operate the system to perform a task, the interface

		should guide the user to take the appropriate actions and provide feedback to the user when operations succeed or fail. ° High false alarm rates will make the operator ignore a real alarm condition. If an operator gets an alarm for nearly every action, most of which are false, he or she will ignore the alarm when there is a real emergency. ° System designers must insure that the user interface is easy and intuitive for human operators to use, but not so simple that it lulls the operator into a state of complacency and lowers his or her responsiveness to emergency situations. The interface must be relatively simple and easy to use without sacrificing system safety. One major problem with systems design is that they are designed for simplicity which can lead a normally privacy conscious person to make bad security decisions. ° In safety critical systems, the main goal when of the user interface is to prevent the operator from making a mistake and causing a hazard. In most cases usability is a complementary goal in that a highly usable interface will make the operator more comfortable and reduce anxiety. However, there are some trade-offs between characteristics that make the interface usable and characteristics that make it safe. For example, a system that allows the user to commit a procedure by simply pressing the enter key a series of times may make it extremely usable, but allow the operator to bypass important safety checks or easily confirm an action without assessing the consequences. ° The user interface must provide intuitive controls and appropriate feedback to the user. Many user interfaces' can cause information overload. For example, if an operator must watch several displays to observe the state of a system, he or she may be overwhelmed and not be able to process the data to gain an appropriate view of the system. This may also cause the operator to ignore displays that are perceived as having very low information content. ° The user interface must be designed so that it provides enough novelty to keep the user alert and interested in his or her job, but not so extremely complicated that the user will find it difficult to operate. Automated systems are extremely good at repetitive tasks. However, if an unusual situation occurs and corrective action must be taken, the system usually cannot react well. In this situation, a human operator is needed handle an emergency. Humans are much better than machines at handling novel occurrences, but cannot perform repetitive tasks well. Thus the operator is left to passively monitor the system when there is no problem, and is only a fail-safe in an emergency. This is a major problem in user interface design, because when the user is not routinely involved in the control of the system, they will tend to become bored and be lulled into complacency. This is known as operator drop-out. Since the user's responsiveness is dulled, in a real emergency situation, he or she may not be able to recover as quickly and will tend to make more mistakes. • Improving design of user interface, putting users in control of the interface and correcting for human errors and lower its risk is a key part of designing a safety critical system. In order for a user interface to be well -designed and as many flaws as possible to be caught, several inspection methods should be applied. There are several heuristics for judging a well designed user interface, but there is no systematic method for designing safe, usable user interfaces. It is also difficult to quantitatively measure the safety and usability of an interface, as well as find and correct for defects. Empirical methods can also be applied at the prototype stage to actually observe the performance of the user interface in action.

		• Examples of inspection methods for judging a good designed user interface. ° ***Heuristic Evaluation*** Heuristic evaluation involves having a set of people (the evaluators) inspect a user interface design and judge it based on a set of usability guidelines. These guidelines are qualitative and cannot be concretely measured, but the evaluators can make relative judgments about how well the user interface adheres to the guidelines. This technique is usually applied early in the life cycle of a system, since a working user interface is not necessary to carry it out. Each individual evaluator can inspect the user interface on his or her own, judging it according to the set of heuristics without actually having to operate the interface. Heuristic evaluation is good at uncovering errors and explaining why there are usability problems in the interface. Once the causes are known, it is fairly easy to implement a solution to fix the interface. This can be extremely time and cost saving since things can be corrected before the user interface is actually built. However, the merits of heuristic evaluation are very dependent on the merits of the evaluators. Skilled evaluators who are trained in the domain of the system and can recognize interface problems are necessary for very domain specific applications. A sample set of usability heuristics : ▪ Simple and natural dialog. ▪ Speak the users' language. ▪ Minimize the users' memory load. ▪ Consistency. ▪ Feedback. ▪ Clearly marked exits. ▪ Shortcuts. ▪ Precise and constructive error messages. ▪ Prevent errors. ▪ Help and documentation. ° ***Cognitive Walkthrough***

		Another usability inspection method is the cognitive walkthrough. Like the heuristic evaluation, the cognitive walkthrough can be applied to a user interface design without actually operating a constructed interface. However, the cognitive walkthrough evaluates the system by focusing on how a theoretical user would go about performing a task or goal using the interface. Each step the user would take is examined, and the interface is judged based on how well it will guide the user to perform the correct action at each stage. The interface should also provide an appropriate level of feedback to ensure to the user that progress is being made on his or her goal. Since the cognitive walkthrough focuses on steps necessary to complete a specific task, it can uncover disparities in how the system users and designers view these tasks. It can also uncover poor labelling and inadequate feedback for certain actions. However, the method's tight focus loses sight of some other important usability aspects. This method cannot evaluate global consistency or extensiveness of features. It may also judge an interface that is designed to be comprehensive poorly because it provides too many choices to the user. ▪ Case example: Two security-sensitive user interfaces were evaluated in a laboratory user study: the Windows XP file-permissions interface and an alternative interface, called Salmon, designed in accordance with an error-avoiding principle to counteract the misleading constructs in the XP interface. The alternative interface was found to be more dependable; it increased successful task completion by up to 300%, reduced commission of a class of errors by up to 94%, and provided a nearly 3× speed-up in task completion time(Maxion& Reeder,2005).
Process	OC07- Affordable Access to Mental Health/Drug Treatment Services.	• ***Affordable access*** to mental health and drug treatment services means ensuring that employees have affordable access to mental health services, including drug treatment and provide adequate health insurance benefits for mental health care (adequate health insurance for mental health care). • Health insurance plan must covering mental health or substance use disorder services in parity with medical and surgical benefits, so that organizations' employees be protected by Mental Health and Substance Use Disorder Coverage Parity laws as defined under the health care laws. ° The Drug Dependents (Treatment and Rehabilitation) Act 1983 The Act provides for both mandatory treatment and rehabilitation of any person who have been certified as drug dependent as well as for voluntary treatment and rehabilitation. ° The Malaysian Mental Health Act 2001 The Act provides a framework for the delivery of comprehensive care, treatment, control, protection and rehabilitation of those with mental disorders.

Process	OC08- Appropriate Time Off For Employees.	° *Appropriate time off for employee's* means, providing appropriate time off for employees to find a balance between work and home life. ° Working world poses many challenges to employees. While some careers allow a relaxed relationship between work and private life, many others demand significant reductions in the area of leisure and family. To reduce human error in workplace it's essential for organizations should considering how to achieve a work-life balance and implementing targeted measures to promote this and providing appropriate time off for employees. The goal is not only to make employees more productive, but also happier and more balanced.
Process	OC9- Team-building Activities.	• Promote team-building activities and social interactions among employees to enhance mood and building a strong team by encouraging teamwork through formal and informal team-building activities. For example arranging an organization-oriented outing, such as bowling or mini-golf, or involve the office in a team-based charitable activity. Good relationships in the workplace thrive when individuals feel part of a team and comfortable with their teammates. According to a 2008 study published by the University of Florida Institute of Food and Agricultural Sciences, respect and trust amongst co-workers and between supervisors and staff leads to greater collaboration, innovation and efficiency in the workplace.
Process	OC10- Improve Design of Work Environment.	• ***The work environment*** is the place where the employee is located and the physical conditions surrounding him during the performance of his work. • ***Design of work environment*** is a factor that makes errors more or less likely. Organizations must view poor design and layout of workplaces as a causal factor to physical discomfort which has been shown to be associated with human error, work environment includes such factors as noise, lighting and temperature, vibration, chaos in files and documents, workspace arrangement, and facility layout and arrangement, environmental controls, glare, noisy environment where alarms cannot be heard, too tight workspace to adequate remove or work on equipment and the uncomfortable offices, specifically in terms of how environmental factors contribute to human performance and safety and health .The concerns for design of work environment are that they induce fatigue and/or distract attention from the primary task, resulting in increased potential for human error. Design of work environment also includes the ease and complexity of systems and software design , font colour and font size that cause optical dispersion and can affect the user of information systems, and when the technology and equipment the user use is poorly designed and confusing to use, they get frustrated and make mistakes. • Organizations must improve design of work environment by providing quiet environment, arranged workplace, comfortable offices, easy-to-use and perfectly designed software, systems and equipment and avoiding design factors that cause confusion get frustrated, fatigue, distract attention and lead to mistakes.
Process	OC11- Improve Work Planning and Control.	• ***Work planning and control*** is the use of formal, documented processes for identifying and mitigating risks when planning, authorizing, releasing, and performing work. The purpose of work planning and control is to ensure adequate protection of employees, the public, and the environment, which would otherwise be put at risk by inconsistent and inadequate planning,

		authorization, and control. • Job pressure, poor job rotation, time factors, task difficulty, change in routine, poor task planning or management practice, lack of knowledge ,skills , capability , capacity and ability must be seen as a causal factor which has been shown to be associated with human error and impact employee performance and must be improved. For example, job stress and time pressure negatively affect performance; heavy and prolonged workload can cause fatigue, which adversely affects performance and in the presence of high email loads, users are more likely to respond to phishing email.
Process	OC12-Improve Work Setting and Management Practices.	• ***Work setting*** is the employee's ways and tools to perform his work. • ***Management practices*** are the working methods and innovations that managers use to make the organization more efficient. • Distractions, insufficient resources, poor management systems, inadequate security practices, and poor work flow must be seen as a causal factor which associated with human error and impact employee performance, and must be improved, as well as the working methods and innovations that managers use to make the organization more efficient. In addition to distributive, procedural, interpersonal, and informational justice in the relationships that employees have with their work organization and its members, which can promote employees' motivation to support the organization's interests and their ability to choose where, how and when they do their work in the office, a s they different types of tasks throughout the day, people need access to different types of work settings that relieves the physical and psychological stress that comes from working in a space that doesn't fit the task. For example: poor communication can cause several problems during a workflow lifecycle: information can become outdated, employees do not know that, and expectations and deliverables can be unclear.
Process	OC13-Command And Control Centre	• ***Command and control centre***: Organization must establish a team of information security professionals as command-and-control centre or a security operation centre for responding to cyber incidents. ° The team will provide advisories of potential threats or on how to mitigate threats being faced by the organization. Incident response team members should have skills and technical expertise. Having a command & control centre in place ensures effectively deal with a threat on the time to contain and remediate it. ° The command and control centre enables organization to identify threats and weakness. ° Monitoring and providing alarms, increase situation, awareness, advisories, logging of incidents and deliver a real-time response for any security incident. ° Conducting structured investigation to provide a targeted response to contain and remediate the threat with the right procedures.
Process	OC14- Incident	• When monitoring incidents the possibility that a questionable behaviour is not necessarily a true defect. These incidents should be log so that organization can keep the record of what they observed and they can follow up the incident and track what is done to

	Logs.	correct it. It will be a good idea to log, report, track, and manage incidents found during development and reviews because it gives useful information about the early and cheaper defect detection and removal activities. Incidents that are not logged may not be tracked and forgotten which can results in the incident occurring again. Documentation and Incident Reporting must be a regular part of the security's regular duties. Incident logs detail the actions taken to prevent or handle Incident -related problems .They serve as supporting documentation that may be needed in the future.
Process	OC15- Advisories.	***Advisories:*** Advisory is a document letting organization know, that is there security vulnerability in their system. It also tells organization how to fix the problem. A security vulnerability, which is a bug in the application that malicious users (hackers) could exploit to gain access to organization's data or network. In most cases, command and control centre would issue the security advisory at the same time as they provide the patch or upgrade that fixes the flaw. If necessary, they may issue the security advisory even before the patch is ready, and tell people how to minimise or prevent their exposure to attack until the fix is ready.
Monitoring	OC16- Risk Analysis And Auditing.	• ***Risk analysis*** is the process of identifying and analysing potential issues that could negatively impact key business initiatives or projects. This process is done in order to help organizations avoid or mitigate those risks. Performing a risk analysis includes considering the possibility of adverse events caused by either natural processes, like severe storms, earthquakes or floods, or adverse events caused by malicious or inadvertent human activities. An important part of risk analysis is identifying the potential for harm from these events, as well as the likelihood that they will occur. • Risk analysis is necessary in many cases such as planning projects, to help anticipate and neutralize possible problems, deciding whether or not to move forward with a project, and improving safety and managing potential risks in the workplace. • To carry out a risk analysis, organization should follow these steps: 1- Identifying threats Identifying the existing and possible threats that organization might face in the systems, processes, or structures that organization use, and analyse risks to any part of these. What vulnerabilities can you spot within them? These can come from many different sources. For example(loss of a key individual by Illness, death or injury, disruption to supplies and operations or loss of access to essential assets, loss of customer confidence, or damage to market reputation, business failure, stock market fluctuations, interest rate changes, or non-availability of funding. 2- Estimate Risk Once organization has identified the threats you're facing, need to calculate out both the likelihood of these threats being realized, and their possible impact.(Risk Value = Probability of Event x Cost of Event).In addition the organization employs automated tools to support analysis of events. Once organization has identified the value of the risks it faces, organization can start to look at ways of managing them. Such as avoid the risk, share the risk with other parties, accepting the risk, or control the risk.

		• ***Auditing*** :The information systems auditing is the process of conducting analytical test and evaluating evidence to be determine in monitoring and evaluating computer system, maintain data integrity, achieve the organizational goals effectively, and use resources efficiently. The information system auditing is conducted to evaluate the readiness level of organization in managing information technology The process of information system audit involves four steps: 1. Measuring vulnerability of information system. 2. Identification of sources of threat. 3. Identification of high risk points. 4. Checking for computer abuse. • Organizations must apply risk management and measurement and analysis concepts and approaches to critical business processes to ensure they are providing the intended results, with periodic and incident-driven review, maintain records of reviews.
Monitoring	OC17-Incident-driven Reviews (Policies, Practices, Training Materials).	• Every organization that develops policies needs a review process. The organization's policies and procedures need to be periodically reviewed to ensure that they continue to be relevant to the work of the organization and aligned with applicable standards and security requirements .The policy shall be reviewed every year or at the time of any major change in existing IT environment affecting policy and procedures. • ***Incident-driven review*** is a review in which the review of the policies, practices, and training materials conduct after occurrence of incidents to determining the weaknesses in the policy that led to the accident and trying to develop it based on the causes of the accident, rather than periodic normal review. • Organization must conduct incident-driven reviews of policies, practices, processes, and training materials, by reactive approach that focuses on quick response.
Monitoring	OC18-Periodically, Fully Re-evaluate Risk.	• ***Risk evaluation*** is a systematic process of identifying hazards and evaluating any associated risks within an organization, then implementing reasonable control measures to remove or reduce them. • To carrying out a risk evaluation: ° Identifying potential risks. ° Identifying who and what might be harmed by those risks.

		° Evaluating risk (severity and likelihood) and establishing suitable precautions ° Implementing controls and recording findings ° Reviewing the evaluation and re-evaluating if necessary. • A suitable and sufficient risk evaluation must be carried out prior to a particular activity or task being carried out in order to eliminate, reduce or suitably control any associated risk to information security. Once completed a risk evaluation should be reviewed periodically (proportionate to the level of risk involved) and in any case when either the current evaluation is no longer valid and/or if at any stage there has been significant changes to the specific activity or task. Relevant risk evaluation should be reviewed following an incident in order to verify if the control measures and level of evaluated risk where appropriate or require amendment. • Organization must treats the evaluation of risk as a continuous process and periodically fully re-evaluate risk to avoid the effects of lowered perceived risk threshold accumulated over time while many of the risks associated with information security are of a cumulative nature. This means that the likelihood of an event occurring on a given day or at a given time might be extremely small, but over time, this chance increases and risk tolerance varies over time in individuals They might come to accept or adapt to the surrounding risk and no longer perceive it the same way they perceived before and they might have a lower perception of risk than before.
Monitoring	OC19- Ethical Hacking.	***Ethical hacking*** involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them. Ethical hackers are security experts that perform these assessments. The proactive work they do helps to improve an organization's security posture. With prior approval from the organization or owner of the IT asset, the mission of ethical hacking is opposite from malicious hacking.
Monitoring	OC20- Regular Vulnerability Scans.	***Vulnerability scan*** is an inspection of the potential points of exploit on a computer or network to identify security holes. A vulnerability scan detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures. The role of vulnerability scan is to identify all existing and potential vulnerabilities to an organization's security. This can include finding loopholes in the company's firewall, servers, networks, applications, and routers. The scope of a vulnerability scan ends with identification itself. It can find all the vulnerabilities in an organization but cannot identify the ways in which these vulnerabilities can be exploited. This is where ethical hacking comes in. It uses all the identified vulnerabilities that were found in the vulnerability scan and creates simulated cyber attacks on the organization's servers, applications, firewalls, and more. Ethical hackers attempt to attack each and every vulnerability that has been detected to generate reports on how exposed the organization is to different types of risk.
Monitoring	OC21- Developing	***Developing incident response plan***: An incident response plan required having right employees with the right skills and experiences

	Incident Response Plan.	know what procedure to follow to contain and remediate an incident. An incident response plan ensures that in the event of a security breach, the right personnel and procedures are in place to effectively deal with a threat. Having an incident response plan in place ensures that a structured investigation can take place to provide a targeted response to contain and remediate the threat. ° Steps of Incident Response Plan 1. Preparation: Preparation for any potential security incident is a key to a successful response by giving clear instructions on how to prioritize an incident and when they should be escalated. These should be high level and focused on specific areas such as DDoS, Malware, Insider Threat, Unauthorized access, and Phishing. 2. Identification: the size and scope of an incident. 3. Containment: Once the scope of an incident has been successfully identified the containment process can then begin. The compromised devices within the estate are isolated from the rest of the network to stop the spread of an attack. 4. Eradication: Once the incident is successfully contained then the eradication of the threat can begin. This will vary depending on what caused a device to be compromised. Patching devices, disarming malware, disabling compromised accounts are all examples of what may be required in the eradication phase of an incident. 5. Recovery: The goal of the recovery phase of an incident is to restore normal service to the business. If clean backups are available, then these can be used to restore service. Alternatively, any compromised device will need rebuilding to ensure a clean recovery. Additional monitoring of affected devices may need to be implemented. 6. Lessons Learned Once the threat has been fully remediated the next step will involve a meeting known as a Post Incident Review (PIR) should take place and involve representatives from all teams involved in the incident. To discuss what went well during the incident and what can be improved and to prevent this incident from happening again.

Table 3: The Human Factor's Countermeasures Components.

UITCM
The Human Factor's Countermeasures Components

Component	Element	Description
Behaviour	HC01-Monitor Employee Behaviour.	•The UIT factors might be recognized or inferred through monitoring and surveillance methods. Monitoring the activity of employees is essential for risk management resulting from UITs .Monitoring is a tool to maintain the security of an organization by discovering employee involvement and participation, making certain that employees are properly matched in their jobs and fully aware of the extent of their authority, and make sure there is no policy violation or compliance .Employees who are resistant to change and training and who comply with policies only when management is tightly observing , employees who are unaware and employees who may causes damage accidentally, their interests and practices are being monitored automatically and routinely. Motives behind employee monitoring are, to prevent inappropriate actions of employees; monitoring careless behaviour and to protect employees' personnel information from becoming accessible to hackers who are likely to use the information. •Employee behavioural patterns could be tracked with the help of employee monitoring software reports that capture the data on employees' computer use style, visited websites orientation, and the software and documents used as well as relevant activities' duration. These programs running on their computers or a connected server. Employee monitoring acts involve monitoring Internet links, review of e-mails, telephone use, video surveillance for security purposes, storage and review of computer files, video recording of employee job performance, recording and review of telephone conversations, and storage and review of voicemail messages. Detection is achieved by automated tools that can detect employee's activity to reduce and stop data loss. Monitoring processes can includes examining and retrieving employees' e-mails that related to the work, records, and information about, employees' access to Internet websites, monitoring computer used by employee, knowing where the employee is, authorized personnel files, the possibility to proscribe all small electronic devices in the workplace that to prevent using it in work place and time spent outside the workplace. Perhaps including, in some cases, linguistic analysis performed on samples of monitored electronic communications. In addition to reporting policy violation by co-workers. •Organization's management must find a balance between monitoring gains and the costs of invading employee privacy. • Monitoring must be performed in accordance with privacy and civil liberties laws and protecting employee rights. •Employee monitoring can be subject to a variety of laws and possible legal constraints or boundaries, for example, identifying perceived risk threshold under some circumstances may be considered mental health testing, laws would apply which could limit testing and responses. •Employees should be aware of the devices that will be used to monitor them, how the data will be used, and when exactly they will be monitored; and employees and customers should be notified when telephonic monitoring is taking place through the use of a specific tone that can be heard by both employee and customer.
Behaviour	HC02- Trust model With Permission	•In the ***Trust model***, only certain people are given permission to certain rooms, open certain cabinet files, or sign cheques and the person who has the physical possession of the cheques does not have the machine that embosses the signatures. Someone might be trusted to make changes in the personnel records but not the engineering specifications. This segregation of duties can be used to

	Authentication From Higher Level Employee. .	minimize human error. The assumption is that one person can only make an error only in the area they are designated to be working on. The trust model can be improved by adding permission authentication from higher level employee. When an employee are implementing a critical task such as approving a fund transfer, share sensitive information, or take some other action that could result in a security breach, that employee should reach out to higher level employee to get a permission authentication. • Applying the segregation of duties for all roles is essential for insider risk management and to mitigate against insider threats by the principle of least privilege where strict organizational rules let employees have access only to resources that are required for their job role. •There needs to be shared responsibility at senior management level for the creation, dissemination and enforcing of a robust security policy that every employee has a copy of and familiar with the parts that pertain particularly to them ,that means segregation of duties, so that , only certain people are given permission to certain tasks. Physical controls are also well-founded in assigning the least privilege, i.e. only enough access to perform the required job, and in implementing a segregation of duty when more than one person is required to complete a critical function. Physical controls are also used to control and minimize the risk of unauthorized access to physical assets and information systems. For example, two people at least are needed with the privileged users to alter modifications on the system. Limit user access to high value data and systems can help protect high-value data from compromise. Only users who absolutely need access should have it ,which makes randomly-targeted phishing emails less likely to succeed. Even if account credentials are stolen, the damage caused can be limited to just those systems that the account had access to.
Behaviour	HC03- Collaborative Reinforcement Model.	•Employees work collaboratively to ensure that information security policy is adhered to by every member in the group. Certain rewards and punishments are then awarded to individuals, depending on their actions, and then monitoring and reporting for doing harmful mistakes so by the associated team members, who have probably better knowledge of it or can better detect it than the centrally administered monitoring mechanisms. Furthermore, policies regarding the reporting of careless behaviour of a co-worker can help in defending against the unintentional insider threat.
Psychological	HC04- Mental and IQ Test	•Psychological testing is a tool used for employment-screening. Many employers require job applicants to take psychological tests as a condition of employment, within specific skills tests that have relevance to the position of interest to determine if the candidate is well-suited to the job. Testing is sometimes used as a condition of continued employment. Testing of employees before and after employment is commonplace in the business world. Psychological tests are used to measure a person's mental abilities, talents, intelligence, or personality. There are deferent types of psychological tests available to help employers in making decisions. Organization must choose the right one. A psychological test for a job, often called a psychometric test, is a standard, scientific method used to measure a person's mental capabilities and behavioural style. Psychometric tests attempt to assess someone's ability to perform certain functions and tasks. Really, psychometric tests are a form of IQ test. An intelligence quotient is a total score derived from a set of standardized tests or subtests designed to assess human intelligence. These tests are designed to measure candidates' suitability for a role based on the required personality characteristics and aptitude. The purpose of psychological testing is to make more informed hiring decisions. Human error can be minimized by tailoring the demands of the job to the characteristics of the person, and can help reduce the number of problem employees. All psychological tests require that job applicant perform some

		behaviour to measure personal attributes, traits, or characteristics or to predict outcomes, these tests can differ in various ways. For example, they can differ in terms of the behaviour they require job applicant to perform, what they measure, their content, how they are administered and formatted, how they are scored and interpreted, and their psychometric quality. Psychometrics is the quantitative and technical aspect of mental measurement. The mental test usually called psychological test. Mental match involves the individual's information and decision-making requirements, as well as their perception of the tasks and risks. Mismatches between job requirements and people's capabilities provide the potential for human error. • Psychological tests have limited validity like standard medical tests and are administered and interpreted by clinical and forensic psychologists. So psychological tests are not only used during the hiring process. Some organizations use these tests to monitor the continued suitability of employees who have been on the job for some time. The psychological tests required for the position can be preliminary, periodical or extraordinary. Preliminary psychological tests concerning suitability for sphere of activity shall be performed prior to the beginning of the working process. Periodical psychological tests is required on an annual basis, for example, for the employee who is employed in a position, where risks of accidents are highly increased, the frequency of periodical psychological tests is regulated by the policy of organization. Extraordinary psychological tests concerning suitability for sphere of activity shall be provided in the cases, for example, for the employee's behaviour condition highly changed, which may make him unable to hold the position complying with occupational security requirements. • Some organizations use games as a way to carry out psychological testing for employees, where job applicants have to perform tasks using skills that the organizations is looking for during playing these games. Such as Deloitte company which customized a "game" which places potential employees in real life work situations at the firm. The 20-minute online game incorporates videos and tasks from real Deloitte employees based on scenarios that occur regularly in the workplace. The game serves as the first round of the selection process and follows the same principals as traditional psychometric testing commonly used by large consulting and professional firms and allows employers to assess candidates' performances (Alloway & Cissel,2017).
Psychological	HC05-Drug Testing.	•The first line of defence to mitigate insider threat begins at the hiring stage. Potentially non-trustworthy candidates can be identified at the application stage by conducting specific tests as a condition of employment, that have relevance to the position of interest to determine if the candidate is well-suited to the job. Drug testing for illegal drug in the workplace is an option that enables employers to find out if employees are using specific types of drugs, either currently or in the recent past. In situations where the employee has a responsibility for the security of information system; there is a strong argument for workplace drug testing being carried out, within the employment conditions. Special laboratories perform drug testing using methods include using samples of the employee's blood, urine, hair, saliva or sweat. Workplace drug testing has the potential to greatly enhance health and safety in the workplace. Testing discourages people from abusing substances and thereby reducing the likelihood of the incidents related to working under the influence and encourages greater responsibility among employees who may cause harm to information system. •Drug testing may be used either as a condition of employment or to identify drug use in current employees. The organizations might require all job candidates to submit to a drug test before being hired. Other organizations perform drug tests on current employees to ensure that no one is misusing drugs. Some organizations test all employees at particular times throughout the year. Others test individual employees if the employer has a reasonable suspicion of drug use or after an accident in the workplace to

		determine if drugs played a role in the incident. Random testing is another method of drug testing. This method involves selecting random employees for testing. To ensure a truly random pool of tested employees, organizations sometimes use a computer program to determine who is tested. •If organization plan to use drug testing as a part of a workplace substance abuse policy, must take in consideration some legal issues such as the civil liberties, emphasizing individual freedom, the right to privacy and protection from discrimination and make sure the policy adheres to the state's laws and is accompanied by a carefully written policy, which is understood by employees and supervisors alike and respects the rights of all. When caring out drug testing in the workplace, there are some ethical principles that need to be in place to avoid violation of the rights of the employee. For example: ° The employee needs to know, prior to taking the job that drug testing is an expectation, and the workplace drug testing is planned. ° Workplace drug testing should be a justifiable course of action rather than a routine screen used to discriminate against alcohol or drug-using employees and there should be a clear justification of the relevance of workplace drug testing to the situation. ° The employee's privacy must be respected, including whether workplace drug testing has taken place as well as the result and consequences and must keep the confidentiality. ° Repeat tests should be conducted when a workplace drug test is positive, and employees should be given the opportunity to explain a positive drug test result. ° People with positive results must be treated with dignity and respect, and be supported rather than shamed; this is the only way that leads to avoid the misuse of workplace drug testing to discriminate.
Psychological	HC06- The Cognitive Reflection Test (CRT).	***The Cognitive Reflection Test (CRT):*** measures the tendency to exceed an incorrect, intuitive answer and come to a more deliberate, correct answer by engage in further reflection that leads to the correct response. Users with higher Cognitive Reflection Test (CRT) scores in comparison to lower CRT scores are more likely to be phishing' victims due to their curiosity.
Culture	HC07- Stimulation Of Risk Perception.	• ***Risk perception is*** an individual's assessment of risk, and the individual's risk assessment is reliant on the risk information that individual has and on the previous experiences. If one experiences long period characterized by absence of accidents. In the event that an accident occurs, expectations are grounded on previous experiences, meaning that users perceive this accident more as a rare occasion. On the other hand, if one experiences attacks consecutively for a long period of time, one will expect a similar attack in the near future. Consequently such a person becomes more careful and is cautious with the security measures. There is association among risk perceptions and security behaviour, and the risk perception has an effect on decision-making. Thus risk perception might play an important role for motivating people to improve their security behaviour. • Organizations must consider stimulation of risk perception a key component of security behaviour change. To stimulate employees'

		risk perception: ° Organization must keep employees abreast of latest attack news and statistics in Malaysia and international threat-related statistics. ° Employees who have a good knowledge should have more ability to assess risks. Organization must ensure that employees obtained security education and awareness program. ° Sharing of employees personal previous experiences on the threats if an employee experiences attacks in the past. ° Organization must keep employees abreast of threats effect on the organization and consequences to employees.
Culture	HC08-Security Education, Training, Awareness, Instrumental Conditioning.	• ***Enhance awareness*** of unintentional insider threat, heighten motivation to be wary of insider threat risks, recognizing phishing and other social media threat vectors, Keep employees abreast of latest attack vectors and other threat-related news, train continuously to maintain proper level of knowledge, skills, and ability, conduct training and awareness on risk perception, and cognitive biases that affect decision making, conduct frequent training and awareness programs. ° Enhance awareness of phishing to spot phishing tactics , to identify phishing attacks and social engineering . Improve user's ability to identify phishing emails and spoofed websites with updated information on current trends and cybersecurity advice. ° Conducting regular simulated phishing attacks. It is necessary to test employees awareness. Regular simulated phishing attack tests can help in evaluating the effectiveness of security awareness training programs. • ***Instrumental conditioning*** refers to learning through consequences, so that a system user's behaviour that produces positive results is reinforced while behaviour that produces negative effects is weakened (strategy of reward and punishment). This strategy can be used by organization to improve security behaviour of employees.
Culture	HC08-Usability of Software /Security Tools.	• ***Usability*** is the degree to which a software or security tool can be used by users to achieve task objectives with effectiveness, efficiency, and satisfaction. Usability is a controlled aspect of User Experience design that ensures the end-user doesn't strain or encounter problems with the use of software or security tool. A user experience designer can control accessibility, user interface, information architecture and usability to suit the goals of users. Security needs to motivate a positive experience, and this is what usable software does. Difficult to use or confusing security systems often are less likely to be used .If a security tool is easy to use employees will choose to work securely over choosing not to. The highest levels of security can be achieved only with an equally high level of usability. Because usability of security tools help overcome user errors during using it and reduces the possibility of ignoring or skipping it. • Organization must improve usability of security tools and software to reduce likelihood of system-induced human error, hold usability as a fundamental element of security and must take into account some characteristics and properties when developing or

		selecting software and security tools, such as: ° It's important to ensure that software /security tools have interfaced is easy to navigate with little thought and should be as flexible as possible. It should be logical and practical to use. If options are permitted, the more secure routes or choices should be encouraged by making them the default or the most natural path for a user to follow. If users are presented with the appropriate security solutions to match their tasks, in a way that makes sense to them and requires uncomplicated but obvious use to achieve the security intended by the solutions, it will require little effort for users to work more securely and effective security and usability can be accomplished together. ° A solution should be intuitive, so that users do not need to decide on how to use a software /security tool to ensure security. Instead, a software / security tool should work to remove security decisions from users as much as possible. If it is less dependent on user action to work, will be more effective as the room for error is significantly reduced. A good interface design elevates security as it lessens the liability on users. ° Security tools and software should be practical and work in real-world applications and scenarios with real people who make mistakes. It is useless if it only looks good on paper, but does not apply to real-world situations. ° Organization does not need to choose between security and usability as organization must implementing systems that improve security and usability concurrently. Usability should not outweigh security. On other hand If a priority was placed on security without consideration for usability, this will result in the human errors. Because cumbersome solutions cause users to default from using them as they obstruct their tasks and negatively impact workflows. Organization must achieve effective security through uncomplicated easy-to-use systems that provide convenience for employees. ° Software and security tools must have considerations for multiple means of authentication to provide choice and varied levels of security, risk-based features whereby security can be heightened or reduced depending on circumstances and requirements and usable verification so that verification does not become an obstacle to usability, which it can if not appropriately balanced, are all important security and usability considerations. User-friendly controls that make use of technology advancements like biometrics (fingerprints, facial recognition, etc.) for better user experience should also be considered.
Culture	HC10-Encourage Following of Policies.	•***Policies and procedures*** are an essential part of any organization. Together, policies and procedures provide a roadmap for day-to-day operations. They give guidance for decision-making, and streamline internal processes. Organizations set rules and a policy for reasons whether that reasons is security, ethics, quality, or efficiency. • Some of the outcomes of policies and procedures: ° Policies and procedures keep operations from devolving into complete chaos.

		° When employees are following policies and procedures, organization will use time and resources more efficiently. ° Consistency in practices is also right for employees individually. They know what they're responsible for, what's expected of them, and what they can expect from their supervisors and co-workers. ° When employees follow procedures, they perform tasks correctly and provide better quality customer service. ° When employees are following policies and procedures, workplace accidents and incidents are less likely to occur. • Policies and procedures won't do organization any good if employees don't follow them, and employees often break organization rules, because employees don't always like the idea of having to follow the rules. So organization must encourage following of policies rules. Encourage following of policies means the organization must create motivations for its employees to follow the policies by some steps such as: ° Employees can't follow policies they don't know. Organizations must have written policies and procedures, because verbal reminders don't work. Organizations' procedures must be written down in a way that's easy to understand and making them easily accessible for every employee, to create a reminder that removes the opportunity for excuses. Sometimes employees don't follow procedures, because they can't remember what employer told them. Many organizations still use paper-based policy manuals. This is problematic because employees need to be able to refer to policies at any time. If they don't have easy access to an up-to-date policy and procedure manual, they won't know the correct procedures to follow. Using a policy management software makes policies and procedures available to every employee member. Organization can quickly send out policy updates, and require employee signatures to make sure everyone has read the policy. With online policy management, employee can access procedures from anywhere, using any computer or mobile device. Instead of having to seek through pages, they can do a simple keyword search to pull up the procedure they need. This ensures they are actually following policies and procedures. Organization must keep a hard copy for their records or for anyone who wants the physical version, but must using digital documents to make sure all policies and procedures are easily accessible for every employee. ° Making sure that, employees read policies and procedures is the first step toward ensuring compliance, but it's not enough on its own. Employees may not entirely understand a policy or know how to put it into practice. Organization must train employees on the substance of policies as well as on how to perform procedures in real-life situations. Thorough training on policies and procedures should happen for every new hire during the on boarding process and should be ongoing for all employees. ° It's important to make sure employees understand why following policies and procedures are critical. Organization must help employees understand why procedures are necessary. If employees perceive organization's procedures as unnecessary, or superfluous to their real responsibilities, they won't take them seriously. Employees must know why you have them in place and why adhering to policies and procedures is an important part of their job. ° Employers must frequently monitor their employees' computer use for security reasons, to ensure compliance with

		organization policies, to ensure employees' productivity and to limit employee access to non-work-related internet sites. ° Provide compliance incentives and reward employees who comply with procedures. Recognizing and rewarding correct behaviour is a great motivator for employees. Bad behaviour should not be ignored and the negative consequences of not following policies and procedures should be clear. Organization must apply punishment policy, enforce penalties for non-compliance.
Culture	HC11-Employee Assistance Programs (EAPs).	• ***An Employee Assistance Program (EAP)*** is a voluntary, work-based program designed to help employees in resolving personal problems that may be adversely affecting the employee's performance and reduce outside stresses, which may cause mind wandering ,EAP offers free and confidential assessments, short-term counselling, referrals,, and follow-up services to employees who have personal or work-related problems. • EAP services are usually made available not only to the employee but also to the employee's family. They are most often associated with counselling services for troubled employees enduring difficult times affecting mental and emotional well-being such as illness and injury, minor medical emergencies, alcohol or substance abuse, marriage concerns and family problems ,child or elder care, grief and loss, stress ,psychological disorders, and financial and personal legal issues. EAP counsellors also work in a consultative role with managers and supervisors to address employee and organizational challenges and needs. • Some benefits of EAPs ° Reduced incidents and human errors. ° Fewer workplace disputes. ° Significantly reduced medical costs arising from early identification and treatment of individual mental health and substance use issues. ° Decreased absenteeism. ° Greater employee retention. • EAP plans should be entirely subsidized by organization. Programs are delivered at no cost to employees as part of comprehensive health insurance plans. Services are often delivered via phone, video-based counselling, online chatting, e-mail interactions or face-to-face.
Culture	HC12-Respectful And Calm Workplace	• A respectful workplace is one where employees can expect to be treated fairly and courteously in an environment that promotes engagement and contributes towards the safe, effective and quality delivery of service. Respect is showing consideration for other employees, demonstrating compassion, treating others with dignity and fairness as well as valuing and honouring diversity and recognizing and affirming individual and team contributions. Employees can be expected to demonstrate polite and courteous

	Environments.	behaviour towards each other (verbal and non-verbal), feel empowered to perform their roles and feel safe to suggest changes for improvements in a collaborative and constructive manner. For employees to be motivated and engaged, they must be in a respectful environment. Without respect, productivity, profits, health, and happiness dwindle. Employees want to feel appreciated and know they matter and treated with dignity and respect. Demonstrating respectful behaviour will ensure a desired and professional workplace as well as a highly productive environment. Respect is earned when employees act and react in considerate and professional ways. • Just as the physical work environment impacts the employee's performance (temperature and lighting, etc), non-respectful environment impacts the employee's performance as well. Respectful and calm workplace environments lead to motivate and encourage organization's employees to work better and with pleasure. Even small details can impact employees' productivity and performance, so everything, is significant for team-building and crafting a workplace and keeping employees' motivated and handle stress and create a positive work environment for organization's employees and reducing workplace disputes and incidents of human errors. • Organization must create a respectful positive environment through some steps such as: ° Organization must develop clear workplace instructions to employees that eliminates racism and discrimination harassment, bullying, intimidation, purposeful exclusion or ignoring, threats, belittling, yelling, rumours, coercion, gossiping, sarcasm, constant criticism, mobbing, using profane, distrespectful, abusive, demeaning language, using inappropriate labels or comments about others ,patronizing and insulting remarks, shaming others publicly ,exhibiting uncontrolled anger ,berating an individual in front of others or in private ,excessive and unreasonable monitoring of someone's work ,withholding information or resources needed to, escalating personal harassment ,threats of retribution and litigation or violence. ° Organization must develop clear instructions to employees that which supports and encourages responding to requests and information in a timely and professional manner ,acknowledging the contributions of others , including people in the communication and decisions that need to be involved , transparency in the evaluation processes used, treating people with respect, compassion, dignity and fairness ,acting ethically and upholding professional standards, taking responsibility for actions and expecting the same of others, being open , honest and no bully, respect confidentiality and privacy ,staying calm , kind, courteous and positive ,avoiding getting angry and emotional, asking for help when needed, listening to understand and practice empathy, following the boundaries that have been set, asking permission to use someone's stuff, keeping the environment clean for others to use, showing appreciation, respecting differ opinions ,communicating effectively with team members and resolve stressful situations, respecting co-worker's property and individual space, helping and cooperation, accepting criticism and knowledge from co-workers as well, apologizing when necessary, smiling and saying good morning and thank you, giving everyone a chance to share input and bring ideas to life in conversations, muting or turning off cell phone while in the workplace ,taking into account the voices as it can be distracting to others, expressing calmly without passing judgment or criticism and not to send text messages or receive calls etc.

		° Organization must lead by example and model the behaviours that they expect of employees. ° Organization must implement educational courses so that employees understand the benefits of respectful work environment and enhancing the substance of engagement, cooperation and calm. ° If organization experience or observe disruptive behaviour in the workplace, it is important that they do not ignore the incident. Ignoring it can make the workplace feel unfriendly, impact morale and engagement. Problems must be resolved from the beginning when conflict arises and attempting to find a common ground and solution, to prevent and address violence in the workplace and response policy that sets out the processes for reporting and investigating workplace abuse and harassment claims to create a psychologically safe work environment. ° Organization can use different ways to provide rewards, including praise, recognition, money, prizes, gift cards, celebratory meals, trophies and certificates of achievement to create a positive atmosphere in the workplace. ° Organization can develops employees' relationships outside of work such as planning a charity campaign and encouraging employees to participate in fundraising events ,having lunch together or event like a bowling day or day a ballpark.

Table 4: Technical Countermeasures Components

UITCM		
Technical Countermeasures Components		
Component	**Element**	**Description**
Incident response.	AC01-Watermarking Forensic, Intelligence Operation.	• ***A forensic watermark*** is the process of embedding of a sequence of characters or code in a digital document, image, video or computer program to uniquely identify its originator and authorized user. In such a way that it is imperceptible to a human observer but easily detected by computer algorithm. A digital watermark is a transparent, invisible information pattern that is inserted into a suitable component of the data source by using a specific computer algorithm. Digital watermarks are signals added to digital data (audio, video, or still images) that can be detected or extracted later to make an assertion about the data. Forensic watermarks can be repeated at random locations within the content to make them difficult to detect and remove. •The main purpose of forensic watermarking is to protect the interests of content creators against illegal use and distribution of copyrighted digital works. While forensic watermarks cannot prevent such activity altogether, they can make it easier for copyright holders to detect it and to identify people who engage in it. A forensic watermark can alert honest users when they have received illegitimate documents or programs. Forensic watermarks are used in the software and digital video industries. Other applications in

		which the technology holds promise include digital music and electronic books (e-books). • ***Intelligence operation*** is the practice of collecting, evaluation, standardizing, analysing and response to data generated by networks, applications, and other IT infrastructure undergoing potential security threats in real-time. And that includes the processes, policies and tools designed to gather the information relevant to protecting an organization from external and inside threats .That information is used to assess and improve an organization's security posture. • ***Security intelligence's*** main goal is to protect the data an organization has by compiling and scrutinizing as much of the data as possible. • Elements of security intelligence include: ° Log management: The collective processes and policies used to administer and facilitate the generation, transmission, analysis, storage and ultimate disposal of the large volumes of log data created within an information system. ° Security information and event management (SIEM): An approach to security management that seeks to provide a holistic view of an organization's information technology (IT) security. Most SIEM systems deploy multiple collection agents to gather security-related events from end-user devices, servers, network equipment and specialized security equipment like firewalls, antivirus or intrusion prevention systems. The collectors forward events to a centralized management console, which performs inspections and flags anomalies. ° Network behaviour anomaly detection (NBAD): The continuous monitoring of a network for unusual events or trends. An NBAD program tracks critical network characteristics in real time and generates an alarm if a strange event or trend is detected that could indicate the presence of a threat. NBAD is an integral part of network behaviour analysis (NBA). ° Risk management: The process of identifying, assessing and controlling threats to an organization's capital and earnings. Such threats include financial uncertainty, legal liabilities, strategic management errors, accidents, natural disasters and information technology (IT) security threats. ° Network forensics: The capture, recording, and analysis of network events for the purpose of discovering the source of security attacks or other problem incidents. "Catch-it-as-you-can" systems capture all packets passing through a certain traffic point, store the data and perform analysis subsequently in batch mode. "Stop, look and listen" systems perform a rudimentary analysis in memory and save only certain data for future analysis. • Key properties of security intelligence ° Real-Time Analysis: It is not enough to be able to view log records when dealing with exploits and immediate threats. Real-time monitoring is a crucial aspect of security intelligence gathering when identifying threats. Security Intelligence is able to evaluate potential present threats. IT organizations use technological tools such as SIEM software to gather security intelligence

		in real time. ° Pre-Exploit Analysis: Security intelligence blends pre-exploit vulnerability management with real-time analysis. By identifying risks before they become breaches, organizations may reduce and more easily detect attacks. ° Data collection, standardization and analysis: Collecting as much applicable data as possible from pertinent devices on the network, creating relations between those devices, and then analysing their behaviour to identify aberrant actions is the most relevant and complete method of identifying security incidents. Security intelligence is capable of fully understanding a situation, identifying the key components and surrounding information, and effectively notifying security analysts of potential threats. Data are aggregating from the IT infrastructure in the form of network, event and application logs. Security intelligence use complex machine learning, pattern recognition and big data analysis to sift through millions of logs from across applications, translate the aggregated data into a standardized format that is human readable, and analyse the data to detect attacks or vulnerabilities. ° Actionability: Genuine security intelligence must be actionable for the organization. The goal of security intelligence is not to collect, evaluate and store additional data and information, but to identify threats, and present potential threats to security analysts in a meaningful and comprehensive way and generate actionable data that drives the informed and targeted implementation of security controls and countermeasures. • Benefits of intelligence operation. ° Improved regulatory and standards compliance: Tools that collect, standardize and analyse log data can help IT organisations demonstrate their compliance with a specified security standard. ° Enhanced threat detection and remediation: Detecting security threats is a core function of SIEM tools. These tools use machine learning and big data to correlate events that are buried in millions of log files from across the network. That leads to faster threat detection and better response times when indicators of a computer intrusion are detected. ° Simplified Security Operations: IT organizations today can automate many different types of security intelligence gathering tasks through cutting-edge SIEM tools, simplifying their operations and reducing the cost of gathering actionable and useful security intelligence.
Incident response.	AC02-Backup Systems (Spatial /Temporal) Replication.	• ***Backup*** is the process of creating and storing copies of data that can be used to protect organizations against data loss. Recovery from a backup typically involves restoring the data to the original location, or to an alternate location where it can be used in place of the lost or damaged data. A proper backup copy is stored in a separate system or medium, from the primary data to protect against the possibility of data loss due to primary hardware or software failure. The alternate medium can be an external drive or USB stick, a disk storage system, cloud storage container, or tape drive. The alternate medium can be in the same location as the primary data or at a remote location. The possibility of weather-related events may justify having copies of data at remote locations. The purpose of the backup is to create a copy of data that can be recovered in the event of a primary data failure. Primary data failures can be the result of hardware or software failure, data corruption, or a human-caused event, such as a malicious attack (virus or malware), or

		accidental deletion of data. Backup copies allow data to be restored from an earlier point in time to help the business recover from an unplanned event. A system backup is the process of backing up the operating system, files and system-specific useful/essential data. Backup is a process in which the state, files and data of a computer system are duplicated to be used as a backup or data substitute when the primary system data is corrupted, deleted or lost. The purpose of a systems backup is to provide a means to restore the integrity of a computer system in the event of a hardware/software failure, physical disaster, or human error. A system backup consists of either a full backup (copying everything that is considered important and that must not be lost), incremental backup (making copies of the files by taking into account the changes made in them since the previous backup) , or a combination of the two. For best results, backup copies are made on a consistent, regular basis to minimize the amount data lost between backups. The more time passes between backup copies, the more potential for data loss when recovering from a backup. Retaining multiple copies of data provides the insurance and flexibility to restore to a point in time not affected by data corruption or malicious attacks. • ***Replication*** is a process of copying and maintaining database objects. The replicated databases are monitored for changes and resynchronized when a change is made .Database replication makes a copy of data accessible from many various servers instead of accessing one central server, or enables many servers to behave like one (parallel query processing). Replication considered as a mechanism for creating data backups. • ***Spatial replication:*** The idea of this strategy is the creation of several copies of a system. Each replica of the system has its own duplicates of the system's important information, which is synchronized (Several copies in different places).This approach is most suitable in cases when only the minority of the replicas is affected by human error. Consequently the greater proportion of the replicas is accepted as the correct state of system. • ***Temporal replication:*** it keeps more than one copies of system, with each one having its own replica of state of the system. The replicas used in temporal replication are not synchronized (Several copies in different times). Temporal replication makes use of a current copy that represents the actual state of the system and several replicas (historical) will represent the situation of different states in the system's history. Requests to the system together with human operator input are only affected on the current replica. This approach works well for cases whereby human errors affect the system state.
Incident response.	AC03- Remote Memory Wipe For Lost Equipment.	• ***Remote Wipe*** is a system capability or software solution where an administrator has the ability to remotely delete and destroy data on a device or system (totally erase the device's memory, in case the device gets lost or stolen) . This feature is often present in the context of mobile device management, and comprehensive risk management systems usually have a remote erase function. Remote Wipe is an effective way to prevent data breaches, and it can address security concerns in Bring Your Own Device (BYOD) policies and security gaps in distributed company computing networks. Wiping a device is the best way to ensure sensitive data stays out of the wrong hands. When a device is lost, stolen, or otherwise compromised, the company must take action to prevent a data breach. So organization must enable remote memory wipe for lost equipment.
Prevention	AC04-Automation.	• ***Automation:*** The use of information technologies to make decisions on behalf of the user .Such as would be to have a popup menu appear on an employee's computer screen giving notification that it is time to change their password. Automation is highly commendable in cases where it is absolutely impossible for the system user to do the work. An example is where packets are checked

		by intrusion prevention systems at a speed that exceeds that of a human systems administrator. Since many security failures are attributed to humans, then it could be wise to use techniques that involve minimum human intervention. The major strength of automation is that it is more predictable and accurate that its' human counterparts. An example of automation is the old anti-virus program that required system users to decide on whether to clean quarantine or ignore a detected virus. With the modern versions of anti-virus programs, the viruses are automatically cleaned upon detection. The main purpose of automation is overcoming poor user decisions and choices. • Organization should adopt automation in the processes that can be automated to reduce human error.
Prevention	AC05-Data Encryption/Password Protection.	• A password is a series of characters containing alphabets, numbers and special characters. ***Password*** protection means only authorized users or the ones who know the password can access the desired information. Password protection is a security measure put in place to protect sensitive information accessible via computers from unauthorized access. • ***Encryption*** is process of concealing information in such a way that only authorized personnel can access the information encoded within files and unauthorized users cannot. Encryption means to hide information or data into something that is unreadable to anyone with no access to the information. To hide the information, two crucial pieces of data is required: the cipher and the key. Cipher is an algorithm and the special knowledge required to decrypt the encrypted data is called the key. So, a cipher is basically a key to the code. • Data encryption and password protection are using in order to protect sensitive information from falling into the wrong hands. Organization should enable data encryption and, Password protection on storage devices.
Prevention	AC06-Wireless And Bluetooth Safeguards.	• ***Bluetooth*** is a wireless technology standard used for exchanging data between fixed and mobile devices over short distances using radio waves. It is an open standard for short-range radio frequency (RF) communication. Bluetooth technology is used primarily to establish wireless personal area (WPAN), ad hoc or peer-to-peer (P2P) networks. Bluetooth technology has been integrated into many types of business and individuals devices, including cellular phones, personal digital assistants (PDA), laptops, automobiles, printers, and headsets. Bluetooth a technology for creating small personal networks between a wide variety of devices to transfer voice and data without the need for cables. Bluetooth devices easily connect to each other. This was the intent when the specification was developed. Consequently, many devices include Bluetooth in a manner that provides for easy connectivity while exposing the information assets of individuals and organizations to greater risk. • Any organization might have hundreds or thousands of Bluetooth enabled cell phones, smart phones, PDA's, keyboards, and mice in the workplace. The possibility of it interacting with organization's network also grows. This number of wireless devices is increasing the potential for information asset compromise and the potential security vulnerabilities that mobile devices present. The more that employees and contractors use mobile devices to access organizational systems, applications and data, the more important it is to protect such access. Given that mobile devices are inherently moving targets used outside the organization , and thus also outside its firewalls, threat management, spam and content filtering, and other protection tools, it's important to apply a battery of

		best practices to use of mobile devices to keep exposure to risk and loss to a minimum. • Organization must take security measures that can implement to secure mobile devices, that Bluetooth-enabled. It's essential to prevent the mobile devices from opening unauthorized means of access to information and other assets. Organization must develop mobile security best practices that can help protect mobile devices and their users from unwanted exposure or unauthorized disclosure of organization information. Organization must enable Bluetooth safeguards (disable or protect these devices), either incorporate these devices into organization's security architecture, or ban their presence altogether. If organization can't secure it, it doesn't need to touch or interact with organization's network. • The following practices aim at securing the Bluetooth-enabled devices themselves. ° Create a policy: Organization must accept that Bluetooth technology is out there and has the potential to interact with their networks. It's important for organization to be proactive; doesn't wait for a Bluetooth-related security incident to occur. Instead, organization must develop an organization policy that discusses the use of Bluetooth-enabled devices and defines how these devices can interact with the network. The policy should address three main areas: 1-Support: Bluetooth-enabled devices are not a supported technology, and no one should connect them to the organization network. 2-Data: No one is allowed to store any organization data on any Bluetooth-enabled device specifically, passwords and usernames. 3-Repercussions: Discussing in detail the penalties for violating this policy. ° Scan for devices: After organization created and distributed the policy, it is recommended performing a wireless sweep to determine whether Bluetooth is active around organization's physical security boundaries. • The following practices aim to protect the data and applications used in the Bluetooth-enabled device. ° Mobile devices need antimalware software: Any employee who wants to use a mobile device for work should install and update antimalware software for his or her smart phone or tablet and prevents users from accessing the corporate networks if they have privacy leaking apps . ° Secure mobile communications: All mobile device communications must be encrypted, simply because wireless communications are so easy to intercept and snoop on. Any communications from employees who want to use a mobile device to access applications, services or remote desktops or systems should require use of a VPN for access to be allowed to occur. . To protect mobile users from visiting phishing sites, even when they are on a Wi-Fi network that the company does

		not control. These protections must be done at the network level because email filtering is not sufficient. Phishing and spear phishing attacks can be delivered through corporate email, through a user's personal email that may be connected to their mobile device or through SMS messages to the user. Mobile users should be connected over Virtual Private Networks (VPNs) to services that provide secure Domain Name System (DNS) and blacklisting to prevent access to phishing sites. °Require strong authentication, and use Password controls: Employees should be instructed to enable and use passwords to access their mobile devices, beyond that, mobile devices should be used with multiple forms of authentication to make sure that possession of a mobile device doesn't automatically grant access to important information and systems. Organizations should consider whether the danger of loss and exposure means that some number of failed login attempts should cause the device to wipe its internal storage clean (ability to remotely wipe a smart phone or tablet). ° Control third-party software: Organizations that allow to employees to use mobile devices in work should establish policies to limit or block the use of third-party software. To prevent possible security breaches resulting from installation of rogue software, replete with backdoors, and require such employees to log into a remote virtual work environment. Then, the only information that goes to the mobile device is the screen output from work applications and systems; data therefore doesn't persist once the remote session ends. Since remote access invariably occurs through VPN connections, communications are secure as well, and organization should implement security policies that prevent download of files to mobile devices. ° Create separate, secured mobile gateways: It's important to understand what kinds of uses; systems and applications mobile users really need to access. Directing mobile traffic through special gateways with customized firewalls and security controls in place such as protocol and content filtering and data loss prevention tools keeps mobile workers focused on what they can and should be doing away from the office. This also adds protection to other, more valuable assets they don't need to access on a mobile device. ° Require secure mobile devices: Mobile devices should be configured to avoid unsecured wireless networks, and Bluetooth should be hidden from discovery. For examples, when headphones is not in use Bluetooth should be disabled. ° Perform regular mobile security audits, penetration testing: At least once a year, organizations should hire a security testing firm to audit their mobile security and conduct penetration testing on the mobile devices they use. • ***Wireless networking*** is a technology that allows devices such as computers (laptops and desktops), mobile devices (smart phones and wearables), and other equipment (printers and video cameras) to be connected and interface with the Internet without cables. Organizations created a good deal of flexibility with wireless for the employees to work wherever they wanted within an organization's, It will increases in agility, productivity, and morale. Users were no longer forced into working from their desk or conference rooms where network drops resided. But the wireless can be risky. Wireless networks connections can be vulnerable points of access for data or hackers may access employee's connection and compromise sensitive information stored on their devices and in online accounts. So it is important to fix organization security weaknesses before they're exposed, not after. • Wireless security is the prevention of unauthorized access or damage to computers or data using wireless networks, which include

		Wi-Fi networks. The most common type is Wi-Fi security, which includes Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). • Some security practices to prevent wireless risk: ° Wireless routers offer the option of encrypting data, it should be used. ° Using a secure password using current best practices to make sure it's not easily guessed or cracked. ° Not broadcasting organization SSID and when naming the network should making it not easy to guess and making sure that organization SSID doesn't call attention to organization. ° Organization should not allow any guests onto its private network, and create a separate network for organization's guests in organization wireless access points (WAPs) and then provide them a passphrase when they visit organization's offices. Organization would have a system that generates unique access for them. ° Organization should uniquely connect users to wireless network. Uniquely authenticate each user to organization's wireless network is an important item for wireless security. Providing authenticated access to the wireless network requires IT organizations to implement RADIUS servers and connect those to a central directory service. RADIUS server lets organization maintain user profiles in a central database. Hence, organization has control over who can connect with the organization's network. ° Organization should adopt per user (or group) network segmentation with VLANs. Network segmentation via VLANs is important step for improving organization wireless security. The organization can segment it's network so that only users assigned to specific network segments can access those segments. When you utilize a network that has not been segmented, all users are on the same network. That means different employees from different departments share the same network space. For example if computer of an employee in finance section had compromised. That means the entire network is open to that attacker. When organization segments the network, only the finance section would be compromised. This does limit the attack greatly.
Prevention	AC07- Standard Systems/Email Safeguards (anti-phishing, anti-malware etc), prevention system (IDS/IPS,DLP), Firewalls, APT Prevention, Accesses Control,	• Organization should employ automated tools to circumvent poor user decisions, such as developing software to better recognize threats in email messages. • Organization should use anti-malware which includes anti (spyware, viruses, phishing, spam, and email attachments). Technology can be used as a tool to help users identify phishing emails by deploy an email system with security features against insecure emails ,that has the ability to detect and isolate malicious phishing email for protection against the phishing mails by providing an additional layer of protection for email attachments or links inside the mail. Using filter to detecting phishing emails and SPAM by using a specialized filter, designed to focus more on phishing ,viruses, and blank senders emails than other general purpose spam filters, to recognize and prevent emails from suspicious sources from ever reaching the inbox of employees.

	Static And Dynamic Software Code Checkers, Data Classification, IAM, Website Controls.	• Organization should employ ***intrusion Detection system*** (IDS): is a software that automates the intrusion detection process by the process of monitoring the events occurring in a computer system or network and analysing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, accept- able use policies, or standard security practices. • Organization should employ ***intrusion prevention system*** (IPS): is software to detect and prevent identified threats. Intrusion prevention systems continuously monitor network, looking for possible malicious incidents and capturing information about them. The IPS reports these events to system administrators and takes preventative action, such as closing access points and configuring firewalls to prevent future attacks. IPS solutions can also be used to identify issues with corporate security policies, deterring employees and network guests from violating the rules these policies contain. • Organization should ***deploy data loss prevention*** (DLP) software to recognize possible harmful sites, email practices, and other threats it is a technology for the early detection of data exfiltration attempts by a malicious or unintentional insider. DLP monitors traffic and prevents sensitive data from leaving organization' network. It is performed in three steps: 1-system discovery. 2- Leaked confidential data identification. 3- Organization policy enforcement. • Organization should employ firewall: is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. A firewall can be hardware, software, or both. • Organization should employ ***advanced persistent threat's prevention*** system. (APT) is an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive data. • Organization should employ ***access control*** system: is a security technique that regulates who or what can view or use resources in a computing environment. • Organization should employ ***static and dynamic software code checkers***: is a software verification activity that analyses source code for quality, reliability, and security without executing the code. By using static analysis can identify defects and security vulnerabilities that can compromise the safety and security of an application. Just analysing the software without running (static), on other hand analysing software as it is running (dynamic). • Organization should employ ***data classification system***: the process of organizing data by relevant categories so that it may be used and protected more efficiently. • Organization should employ (IAM)***Identity Access Management***: is a technology defining and managing the roles and access

		privileges of individual network users and the circumstances in which users are granted (or denied) those privileges. The core objective of IAM systems is one digital identity per individual. Once that digital identity has been established, it must be maintained, modified and monitored throughout each user's access lifecycle. •Website Controls. Technology can be used as a tool to help users identify spoofed websites. Organization must secure their browsers by : ° Developing of web browser plug-ins to combat phishing. ° Browser add-ons and extensions can be enabled on browsers that prevent users from clicking on malicious links. ° Using a secure browser. It will notify user if a website is suspicious, tell user why and ask user if really want to click on the link. This extra level of security helps protect employees and companies from potential hacks. ° Web Browser Warnings: Web browser security, specifically (toolbars and warning alerts), is not sufficient to warn users against entering their details in spoofed websites as well as other browser security indicators (i.e. browser address and status bars),, and that even when users are presented with security indicators or warnings, they simply ignore them. In order to address this challenge, an active interruption such as pop-up warnings would be more effective than passive warnings displayed in the web browser toolbars. ° Deploying a web filter to block malicious websites. All work computers in the organization should verifies the correct URL and security features for every webpage, to proactively blocking suspicious requests and URLs before they can deliver their malicious payloads.
Detection	AC08-Security Information Event Management (SIEM) Systems, Software to Recognize Bogus Emails, EDR, UEBA, CCTV, RFID.	• Organization should employ ***(SIEM) system:*** is a tool that is responsible for centralizing and analysing logging in one management platform, it collects information through secure network channels from various security-related logs (ranging from client workstations and servers to application servers, antivirus software, network devices, honeypots, firewalls, IDSs), and any other sensors in the network, then correlating the events among them in a database by matching any related characteristics and events .This approach allows the information security administrator to quickly search for events and possibly identify malicious insider activity before it occurs, or as a data-mining tool and evidence for forensic investigations after the accident occurs , and safeguard that can detect and prevent data leakage • Organization should employ ***software to recognize bogus emails*** to avoid Phishing and scam emails. • Organization should employ (EDR) ***Endpoint Detection and Response***: is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities. The tools primarily focused on detecting and investigating suspicious activities and traces of such problems on hosts/endpoints.EDR is focused on providing the right endpoint visibility with the right insights to help security analysts discover, investigate and respond to

		very advanced threats and broader attack campaigns stretching across multiple endpoints. • Organization should employ (UEBA) ***User and Entity Behaviour Analytics***: is a security process that takes note of the normal conduct of users. In turn, they detect any anomalous behaviour or instances when there are deviations from these normal patterns. For example, if a particular user regularly downloads 10 MB of files every day but suddenly downloads gigabytes of files, the system would be able to detect this anomaly and alert them immediately .UEBA can analyse the behaviour across multiple users and ICT devices, such as routers, servers, and endpoints in order to detect complex attacks and to detect potential intrusions and malicious activity and to detect users and entities that might compromise your entire system. • Organization should employ (CCTV) ***Closed-circuit television*** for video recording of employee job performance and detect employee's activity to reduce and stop data loss. • Organization should employ (RFID) ***Radio-Frequency Identification:*** is a technology uses radio waves to identify people or objects. It can be found in car keys, employee identification, medical history/billing, highway toll tags and security access cards. It can used to track employee movements and help provide them access to secure locations. An example of tracking employees can be an organization's basic attendance system. Usually, companies give each employee an ID badge.

The model was created in such a way that every group in the model is linked to other groups, and these groups are mutually dependent and complementary.

1. The-·-·-·-·-·dash-dotted line in black depicts the elements' relationships to surveillance and auditing procedures.
2. The elements' relationships to threat evaluation and security measures are represented by the - - - - - - - dashed red line.
3. The ……dotted line in blue illustrates the relationships between the UITCM groups. Table 5.15 shows the relationships between the UITCM elements.

Table 5: The relations among the UITCM Components.

No	Relation	Description
1	Governance → Defence Tools (Detection, Prevention, Incident response) →Behaviour	Laws and regulations, policy enforcement, Procedure, Standard and Best practice fall under the administrative controls (Governance group), they clearly show the acceptable use of an organization's system, network, and information and what is expected from employees and also the possible consequences of violations. Thus they are the documented theoretical side from

		the cyber security program that provides a roadmap for effective security. Whereas, Prevention, Detection and Incident response tools are the technical and operational side of a cyber security program to increase the chances of preventing, detecting and responding to insider threats (Detection, Prevention, Incident and response groups).Both the administrative controls side and technical controls side represent together an effective security program that is able to both, dealing with incidents proactively and can respond to incidents quickly, through control measures in place, rules and controls in order to detect and get alerted about the actions of its employees. Administrative controls and technical controls together produce deterrent measures that control employee behaviour and reduce or prevent their errors and reduce their consequences, to proactively protecting data and to ensure compliance with regulations, rules, laws, so that it prevents the occurrence of the accident or mitigate its potential risks. Governance group has a direct influence on controlling the employees' behaviour. Laws and regulations, imposes using the technical controls and adopting control measures in place, rules and controls that leads to controlling employees' behaviour. The UITCM proposed a relationship among Governance group, defence tools (incident response, prevention, and detection groups) and behaviour group. The Governance group is responsible to impose and adopt defence tools in an organization, (Detection, Prevention and Incident Response) which in turn constitute deterrent measures that control employee behaviour and reduce or prevent error and its consequences. For example law and regulations, imposes using (SIEM) systems and CCTV which detects negligent employee behaviour. Law and regulations, imposes using automation for password changing reminder to enforcing employees to change their devices passwords, and imposes adopting remote memory wipe In the case employee lost his device.
2	Governance → Culture→ Behaviour.	Organizational culture consists of the beliefs, practices, attitudes, behaviour, reputation and ethics of an organization and its employees. Group norms influence individuals' security behaviour. Thus, perceptions of risks are influenced by the cultural context in which they are formed. What is perceived as a risk is shaped by cultural beliefs, social relationships, power relationships, hierarchies, knowledge, experience, discourse, and practice in organization. People generally follow group norms, and therefore if the group considers information security to be an important and serious problem, then it is more likely that the individuals within that group will value and follow the security policies. Conversely, if risk-taking is accepted within the group, then it is likely that greater risks will be taken. Organizational policies, practices, laws, regulations, procedure, standards, processes, and written values inform and shape organizational cultural knowledge, actions, and, ultimately, perceived risks. They also provide guidance on what behaviours are deemed appropriate, ideal, or inappropriate; they establish expectations and inform cultural knowledge. It is important to make all employees all employees receive and sign a copy of organization's policies. Through this, the employees are made aware of what is expected from their job roles and the penalties for violation of these policies are clearly agreed upon and having security awareness training, with a specific chapter dedicated to unintentional insider threat in order to explain what is expected from them and which threats they might be exposed to. Laws and regulations should set strict organizational rules, provide for penalty against any person who exceeds organization's policy or violates it's rules ,then enforce policy and procedures to ensure compliance with regulations, rules, laws, to deliver a clear message of information security policy to the rest of the organization and develop individual values, institutional values and behavioural expectations for the organization to support the implementation of the management system and deploy security culture to mitigate risks. Based on the above. The UITCM proposed a relationship among culture, behaviour and Governance groups. The Governance group is responsible for spreading the security culture in organizations and the organizational culture greatly influences employee behaviour. For instance, group norms can affect individuals' password behaviour. If organization's laws

		and regulations, provides for penalty against any person who exceeds policy of password sharing, therefore, refusing to share a password could be seen as a compliance with the organization's security policy and not a sign that people do not trust their colleagues. Furthermore, policies regarding the reporting of careless behaviour of a co-worker can help in defending against the unintentional insider threats.
3	Governance → Process→ Psychological→ behaviour.	Problems in data flow and increased workload both can negatively affect operator performance and contribute to errors. Similarly, problems in work setting and management systems, such as lack of available qualified staff or inadequate or flawed policies, may lead to increased workload, increased stress, or other factors that affect information processing and decision making and lead to errors and failures. Problems with work planning and control, such as changes in routine, can affect performance through increased fatigue or stress, which then can affects employee physiological state and behaviour. This situation may negatively affect staff performance and contribute to errors in their works. Deficiencies in employee readiness tends to negatively impact performance due to insufficient knowledge for correct task completion, as well as associated anxiety and stress that further affects judgment and decision making. Stress is a major contributing factor to human error. Stressful situations include unfamiliar or exceptional occurrences, incidents that may cause a high loss of money, data, or life, or time critical tasks. Human performance tends to degrade when stress levels are raised. In addition physiological state resulted from diseases, hormones problems, drug side effects and mental problems that can negatively affect operator behaviour and can contribute to errors. Thus, the UITCM proposed a relationship among process, psychological, behaviour, and Governance groups. Where physiological state affects employee behaviour and Governance group is responsible for mitigating risks of physiological employee state, by some procedures such as necessary tests ,affordable access to health services and suitable work environments and ensuring proper process been implemented in the organization. Organization's laws and regulations should consider psychological problems of employees and thereby reducing the likelihood of the related incidents .For example if organization's laws and regulations do not consider work planning and work setting, that can lead to increasing fatigue or stress. Thus, it affects employee readiness and then his performance and may contribute to human error. If organization's laws and regulations impose mental abilities test and drug test as a condition of employment , potentially non-trustworthy candidates can be identified at the application stage and avoid those who may cause harm to information system.

APPENDIX J: RESEARCH PUBLICATIONS

1. Abdelsadeq ,Z.,Basir,N.,Nizam,S. & Rafei, F .2019."Unintentional Insider Threats Countermeasures Model (UITCM)", *E-proceeding IEEE Xplore Conference*:DOI: 10.1109/ICoCSec47621.2019.8970986.

2.Abdelsadeq ,Z.,Basir,N.,Nizam,S. & Rafei, F .2020."Countermeasures of unintentional insider threats: a systematic review",*E-proceeding KOSIST Synergizing Innovation and Research Through Science and Technology* :(USIM) Nilai, Negeri Sembilan.