Chapter 3. Contingency Plans

Contents:

0) Introduction

There is only one applicable clause in this chapter. The reason why a whole chapter is devoted to this is because the Clause is often misunderstood and poorly catered for. Many NCs have been written on this clause alone.

1) 6.1.2.3 Contingency Plans (IATF16949)

(Clause Description-Paraphrase)

The organization shall ensure some critical points on contingency planning: (a) identification of emergencies that can interrupt production and delivery. (A list of potential emergencies is given by IATF), (b) Evaluation of the risks and provide appropriate preventive actions and countermeasures. (c) conduct test out and annual review of these action plans, (d) for actual emergencies, notification of customer and interested parties, (d) validation of product conformity after re-start, following an emergency and improper shutdown. (Author: There is another item added 'Cyber-attack', via SI-5)

(Highlights of the clause)

- (Ref to old Standards) There has been a similar clause (6.3.2) of the same title, in the old version of ISO/TS16949. The previous clause was skin deep. It only required the organization to "prepare contingency plans to satisfy customer requirements in the event of an emergency"
- Now IATF provides 9 potential emergencies to be evaluated for contingency planning. Then there is another item added -Cyber-attack, via SI-5.
- Total list therefore is: key equipment failures; interruption from externally provided products processes, and services (shortage or nonconforming quality); recurring natural disasters; fire (outbreak); utility interruptions; labour shortages; or infrastructure disruptions cyber-attack.
- The above list is minimum, you can add more items pertaining to your specific situation.

(Compliance Best Practice)

6.1.2.3 Contingency Plans

1. *To comply with this clause, you need to list out all the potential emergencies. It shall include the 10 items given in Clause Description + SI-5. See* ***Exhibit 3-1.***
2. *Priority for action shall be based on production and delivery impact to customers (not those of your organization).*
3. *These potential emergencies shall be analysed. You should use your operating history, and your current preventives as the baseline for residual risks. You can use the 4X3 risk table for the scoring, to derive the residual risks. See* ***Exhibit 2-6.***

4. *List out the response actions for each item at the extreme right column of the form. To save time, bullet points can be used for most cases. Simple action plans or full project plan should be used only in more critical cases.*
5. *Please note that point 4 above is referring to RESPONSE plan, not improvement plan. Many such mistakes have been spotted in field practices.*
6. *For improvement and corrective actions, they shall be managed outside this form, as an continual improvement plan etc.*
7. ~~*Annually*~~*Annual review of the contingency plan is required, with involvement by Top Management. See* ***Exhibit 3-4.***
8. *Testing (sometimes called simulation) for the high-risk emergencies is also needed. See* ***Exhibit 3-2 and Exhibit 3-3.***
9. *Notify customer and interested parties as appropriate, when emergencies occur*
10. *Contingency Plans must include product conformity validation after the emergencies (where applicable). The testing form has a space to record this point and point 9.*

2) SI & FAQ

SI Nbr	IATF Clause	Description
3	**6.1.2.3 Contingency plans**	The organization shall: a) – b) (...) c) prepare contingency plans for continuity of supply in the event of any of the following: key equipment failures (also see Section 8.5.6.1.1); interruption from externally provided products, processes, and services; recurring natural disasters; fire; utility interruptions; **cyber-attacks on information technology systems;** labour shortages; or infrastructure disruptions; ***Rationale for change:*** *Organizations need to address the possibility of a cyber-attack that could disable the organization's manufacturing and logistics operations, including ransom-ware. Organizations need to ensure they are prepared in case of a cyber-attack.*
17	**6.1.2.3 Contingency plans**	**a) – d) (...)** **e) periodically test the contingency plans for effectiveness (e.g. simulations, as appropriate);** **cybersecurity testing may include a simulation of a cyber-attack, regular monitoring for specific threats, identification of dependencies and prioritization of vulnerabilities. The testing is appropriate to the risk of associated customer disruption;** **Note: cybersecurity testing may be managed internally by the organization or subcontracted as appropriate** ***Rationale for change:*** *Cybersecurity is a growing risk to manufacturing sustainability in all manufacturing facilities, including automotive. Contingency testing has also been identified by organizations and CBs as an area in need of clarification. This update provides details of what is to be tested as part of a cyber-attack contingency plan validation.*

FAQ	IATF Clause	Questions and Answers
29	**6.1.2.3 Contingency Plans**	**QUESTION** **What is meant by the use of the term "cyber-attack" for contingency plan testing?** **ANSWER** A Cyber-attack is an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm. A cyberattack is often a deliberate exploitation of weaknesses in the security of computer systems or networks to gain access to data, alter computer code, logic or data. These actions may have disruptive consequences that can compromise confidential data and lead to cybercrimes, such as information and identity theft, automation-caused operational interruptions, encryption of company critical data or illegal remote controlling of systems or data. Cyber-attacks and cybercrimes are not always a result of a sophisticated series of actions to guess passwords using powerful computer programs run by teams of people from a remote location. They are often actions designed to convince individual persons to release sensitive or private information through email notes (typically phishing), pretexting (impersonating a trusted person or government official), phone calls announcing fake emergencies getting personal information, visual reading of typed passwords, infecting popular websites with malware, text messages with links to sites installing malware, USB drives left on desks, appearing to be legitimate, which are plugged into PCs, and theft of discarded materials containing confidential computer information, etc. Additionally, a cyber-criminal, after gaining access to a company's system, could encrypt company's critical data and demand a ransom to unencrypt the data. Also, GDPR (General Data Protection Regulation) in Europe or similar requirements in other regions specify that organizations are responsible to ensure that personal data retained by the organization is protected and kept secure at all times, reinforcing the importance of being prepared in the case of cyber-attacks. Additional details regarding information technology security techniques is available through ISO/IEC 27001.

3) Supplementary Notes

Legend: HOC= Highlights of Clause, CBP= Compliance Best Practice, S&Q= SIs & FAQ, EXH= Exhibits

Clause	Section	Clarification Subjects
6.1.2.3	CBP	**SN3.1 What do you mean by "according to risk and impact to the customers'?**
6.1.2.3	CBP	**SN3.2 Can I change the baseline (current controls), after doing some improvement?**
6.1.2.3	CBP	**SN3.3 Can I use Business Continuity Plan, instead of contingency plan?**
6.1.2.3	CBP	**SN3.4 Must I use the exact wording for the various types of emergencies, or am I allow to use my own description?**
6.1.2.3	CBP	**SN3.5 If there is an emergencies that does not occur, will not occur, do I still score the risks?**
6.1.2.3	CBP	**SN3.6 If the final risk is low, do I still need to provide action plans?**
6.1.2.3	CBP	**SN3.7 Why is there a need to score the final risk, when it is not mentioned in the clause?**
6.1.2.3	CBP	**SN3.8 Can I combine this analysis with Risks and Opportunities analysis?**
6.1.2.3	CBP	**SN3.9 Why are we concerned with response and not improvement in this exercise?**
6.1.2.3	CBP	**SN3.10 You said manage the additional improvement or preventive measures outside the contingency form. How do I do that?**
6.1.2.3	CBP	**SN3.11 What is meant by testing, or simulation?**
6.1.2.3	CBP	**SN-3.12 Can actual incident be used for testing? How do we do that?**
6.1.2.3	CBP	**SN3.13 Is testing not same as review? Do I need to do both?**
6.1.2.3	CBP	**SN-3.14 Do Top Management really need to be present in the review?**
6.1.2.3	CBP	**SN3.15 When to inform customer in the event of an emergency?**

6.1.2.3	CBP	**SN3.16. What is meant by "contingency Plans must include product conformity validation after the emergencies"?**

SN3.1 What do you mean by "according to risk and impact to the customers'?

It means prioritization shall be based on risk and impact to the customers, not to your own organization. When you do risk scoring, this will be the criteria to use.

SN3.2 Can I change the baseline (current controls), after doing some improvement?

Of course you can. IATF expects you to do that too. If you have improved, then the document (contingency planning sheet) shall be revised, and the final risks re-scored. Remember it has to be a document revision so changes are tracked.

SN3.3 Can I use Business Continuity Plan (BCP), instead of contingency plan?

There is no prescribed form to use. **Exhibit 3-1** is just an example of how to tabulating the contingency plans. Business Continuity Plan tends to have a wider scope and has a slightly different meaning from the Contingency Plan of IATF. But you can use it so long the requirements of IATF are included into your BCP. There are some organizations doing so, and quite neatly too.

SN3.4 Must I use the exact wording for the various types of emergencies, or am I allow to use my own description?

You only need to comply to the requirement in gist, not necessarily in the exact wordings used in the Standard. Manpower shortage and workers-on-strike can mean roughly the same thing. You can use either.

SN3.5 If there is an emergencies that does not occur, will not occur, do I still score the risks?

An emergency is something you cannot predict for sure. The big flood in Ayutthaya of Bangkok was never expected, yet it happened, and flooding out thousands of factories there. The Covid-19 pandemic had never cross anybody's mind yet it happened. You must still do the scoring for the risks listed. You can score either 'Low' or even 'NA'. The heading however, cannot be removed.

SN3.6 If the final risk is low, do I still need to provide action plans?

You can decide on this. It is not important and IATF auditors won't split hair over a low risk finding.

SN3.7 Why is there a need to score the final risk, when it is not mentioned in the clause?

Rating the risk is not directly mentioned as such, but it is implied. 6.1.2.3 (a) states 'identify and evaluate internal and external risks…' So you have to evaluate (score) the risks.

Another supporting point is that scoring the risks is good for you. With the final scores, you only have to focus on the higher risks for simulation. Otherwise you have to do simulation on all risks, since there is no indication which ones are important and which ones, not.

SN3.8 Can I combine this analysis with Risks and Opportunities analysis?

This is quite commonly done, presumably due to the creativity of some consultants. However, that is not the intent of ISO. If it is, ISO would have used a single clause to cover the 2 requirements. Although there are similar elements in both the analysis, their purposes are different. Risk and Opportunity analysis is to understand where the R&O are, and then provide improvement where applicable. Contingency plan, on the other hand, is about response to emergencies. Therefore the 2 exercises are meant to be done on separate platform and documentation.

SN3.9 Why are we concerned with response and not improvement in this exercise?

Contingency plan is meant to deal with an emergency, despite of all the preventives and preparedness in place. It is not about improvement at that particular point in time. What the customer wants is: you

continue to deliver the supplies on time, whatever happens. You have to figure out how you would do that, and that is the response we are talking about. Investigation and improvement can come later, after the customer's key concern is addressed.

SN3.10 You said manage the additional improvement or preventive measures outside the contingency form. How do I do that?

You can carry out the improvement as a continual improvement project. Alternatively, you can go back to R&O and use the format there to manage areas of weaknesses. See 4.1 and 6.1**.**

SN3.11 What is meant by testing, or simulation?

Testing means to test out the response plan. It is usually done by means of simulation, similar to the concept of fire-drill in EMS, or OHSMS, or a recall in FSMS. Organizations often show IATF auditors a fire-drill, pull out directly from EMS as an evidence of Contingency Plan simulation. They missed the point totally. Fire-drills are to primarily to protect lives and properties. The drill does not attempt to review continued supply to customers, despite of the fire.

SN3.12 Can actual incident be used for testing? How do we do that?

Yes, actual incident can be used for testing. In fact it is more superior than a simulation. It has actually occurred; and the response and results can be used to compare with the response plan to gauge effectiveness. Improvements can then be suggested.

SN3.13 Is testing not same as review? Do I need to do both? How to I review a contingency plan?

Yes you have to do both. Let's look at the clauses first. Review is 6.1.2.3f, and testing is 6.1.2.3e, which state both are required. Most organizations do not carry out the review, thinking simulation conducted will automatic cover this requirement. This is incorrect. Testing is only on 1-2 emergency items, but the contingency plan has minimum 10 potential emergencies.

The best method for contingency plan review is to run a review meeting. You gather the relevant people to make up the multi-disciplinary team required, and review through the contingency plan, point by point. To save time, you may also ask each PIC to review on his/her own area and come to the meeting to present the findings and conclusions. The group can then help to give feedback and finalize the review. The conclusion of review may result in revisions to the contingency plans. In the event there are no changes, evidence in the form of minutes taken, or remarks on the review contingency plan copy retained. If you keep a document change history, changes and conclusions can also be recorded here.

SN3.14 Do Top Management really need to be present in the review?

Yes, according to the Clause. But in reality, some flexibilities are allowed. This would be a little over-killing to insist top management to sit through such a meeting. IATF Auditors do understand top management is hard pressed for time. Requesting Top Management to approve the revised documentation should suffice. It will be better if QMR can do a debriefing, in particular, on the changes. It will even be best, if Top Management can be present for some parts of the review meeting to get a feel how this is done.

SN3.15 When to inform customer in the event of an emergency?

This is according to the contractual agreement you have with the customer. Generally speaking, if you are more confident of handling, you can take a longer time to inform. If you are not so confident, you should inform the customer as early as possible. This is to allow them to make other arrangements or assist you in some way. Otherwise you may be slapped by a big claim.

SN3.16. What is meant by “contingency Plans must include product conformity validation after the emergencies”?

This does not apply to all situations. It is only applicable where the production run is interrupted e.g. by machine break down, workers on wildcat-strike. The product in process may be deteriorated due to extended exposure, a change of operating conditions, and processed not according to plan. Under the circumstances, the product must go through the first piece buy-off again.

Continuing

4) Exhibits

Exhibit 3-1. Contingency Plan

Exhibit 3-1.Contingency Plan

Contingency Plan 2019

S/N	Type	Impact to Customer	Current Controls	S	P	R	Response and Mitigation	Detail Procedure
1	Key Equipment Failure	Production interrupted, may affect OT Delivery	Have excess capacity and spare machines.			L	• Switch over to another machine	None
2	1250 ton machine has no substitute	If problem, production interrupted, OT delivery affected. Heavy penalty will be imposed	Agreement with XXX to mutually assist each other in times of emergencies	H	M	H	• Activate the emergency plan CW101	CWI 101
3	External Supply Problem	Production interrupted, may affect OT Delivery	Multisource purchasing already practiced	M+	L	M	• Can buy from another source.	None
4		Transporter failure cause delivery problem	Currently 2 outsourced transporters. We also own 2 trucks	M+	L	M	• Own truck can be used in the event of supplier problem	None
4	Recurring Natural Disaster-flood	Can disrupt total operations	Never happened in the last 70 years	NA	NA	NA	• NA	None
5	Fire outbreak	Production facilities destroyed, affecting production and delivery	Fire safety system is available and well maintained.	M+	L	M	• Keep inventory as per customer specifications	None
6	Utility Interruption-power	Production interrupted, may affect OT Delivery	Backup generator available for light use Additional generators can be rented easily	H	L	M	• The genset will automatically cuts in when failure • Major failure contact rental company. Contact XXX, Tel XXXXXXXX	None
7	Water disruption	Production interrupted, may affect OT Delivery	Can ferry the water in, treated	H	L	M	• Contact contractor to ferry in water. Contact XXX, Tel XXXXXXXX	None
8	Labor Shortage	Production interrupted, may affect OT Delivery	We maintained a safe application quota from the department (direct). Also can use contract workers	M+	M	M+	• Call the labor supply agencies. Contact XXX,	None
							Tel XXXXXXXX, or XXX, Tel XXXXXXXX	
9	Cyber Attack	Can disrupt total operations	Firewall, anti-virus at every terminal. Back up	H	L	M	• Contact XXX, Tel XXXXXXXX • Inform HQ for additional backup	None
10	Typhoon in Thai supplier for fabric	Can delay shipment of fabric from Thailand and affecting our OTD to customers	Safety stock by customer and organization. HQ also keep stock. Keep tight monitoring of weather forecast	H	M	M	• Activate backup stock-points • Contact HQ XXX, Tel XXXXXXXX	None

Legend: Risk Level. H= High (details needed), M=Mid (Min bullet point guide), L= Low (bullet point guide)

Remarks:

Example of Emergency Plan

CWI-101: 1250 T machine Failure Respond Plan

1. Inform affected customers: **Marketing (within 4 hours)**
2. Contact equipment maker for assessment on repair: **Purchasing (within 4 hours)**
3. Contact Partner (XXX company) to get assistance. **Management (within 2 hours)**
4. To work on detail coordination plan with Partner: **Planner/QA/Production (within 1 day)**
5. Meeting of relevant internal department head and personnel on situation: **Chief Coordinator/Management, within 1 day)**

Remarks given in this section explain on the Exhibit. Do not include them as part of your document

- Risk coring is based on SXP Risk Evaluation Table. the 2 arrows above show the connections. Exhibit 2-6
- Conduct simulation for the H and M+ emergencies over 3-year cycle, do a schedule to show planning
- Bullet points are expected for each case. But for High risk items, a detail WI should be established and be adjunct to this plan. See case above
- Annual review is required of this contingency plan, top management is expected to be involved.

Exhibit 3-3. Contingency Plan Testing - Simulation

Contingency Plan Testing 2019

Contingency Plan Test	
☐Actual case ☑ Simulation Case	Date: 17 Sep 2019
Emergency Tested. Transportation failure	People involved XXX, XXX, XXX

Case Study

Requirement:
Delivery to Honda Assembly Melaka by 5pm before warehouse close

Response Actions given in Contingency Plan:

- If breaks down on highway, send a spare truck to transfer and continue

Scenario (Simulation)

1. This is a stimulated case, conducted in meeting room
2. Consider breakdown at 3.30PM at Seremban
3. Plant is 50 km away, but takes 1.5 hours for spare truck to arrive
4. To transfer the goods to spare truck takes about 2 hour manually (forklift not available)
5. Continue journey another 1.5 hours.
6. By the time of arrival to Honda Melaka, it would be 8:30 pm

Conclusion:
Outcome cannot meet customer requirement. Not OK

Improvement options:
1. start journey in the morning, and not after lunch
2. prepare some tools to transfer from truck to truck.
3. tighten controls on truck maintenance

New Response Measures:

- Driver to inform HQ immediately
- Response team shall despatch soonest, with transfer equipment and manpower required
- Appoint a ERP leader to control onsite
- Inform customer if appropriate on expected delivery time

Management Decision

Adopt fully the recommendations.
Run through risk management flow and update as required

Submitted by	**Approved by**

Remarks given here explain on the Exhibit. Do not include them as part of your document

- This is a simulated case, and not based on real occurrence.
- Most simulated case can be conducted on the side lines, without disrupting the operations. But data and information should be as realistic as possible

Exhibit 3-2. Contingency Testing-Real Occurrence

Contingency Plan Testing 2019

Contingency Plan Test

☑Actual case ☐Simulation Case Date: 30 Apr 2019

Emergency Tested.	People involved
Water Supply Failure	XXX, XXX, XXX

Case Study

Requirement:

To continue to deliver to customer ontime

Response Actions given in Contingency Plan:

- Supply form 3 buffer stock
- If advance information given, calculate and produce ahead

Scenario (Simulation)

1. This is a real case, that had happened, with notice from the water authority
2. It was informed that there will be imposed 3 day interruption of water supply between 24-27 Apr 2019
3. Use BZXXX case for study. It requires 384 sets per day.
4. 3 day buffer stock means: 1152 sets required.
5. Our water tank can supply 2.5 days of operation, or 960 set.
6. Total available inventory is 1152+960 = 2112 sets
7. Customer requirement for 4 days = 1536 sets.
8. Therefore inventory and production quantify can supply with an excess of 576 sets
9. On 27 Apr 2019, it was checked on site and view delivery document, the plan could be executed as plan.

Conclusion:

The customer demand can be fulfilled with inventory and production quantities. Actual checked on site on the last day of water disruption confirmed delivery in full. Therefore the plan is effective.

Improvement options:

1. The 3 day buffer is sufficient and can be maintained
2. We should look into alternative water supply by containers, if water disruption is getting frequent
3. Alternatively, install more water tanks
4. Run through risk management flow and update as required

New Response Measures:

- Response to include water supply contractor contact No

For Actual Occurrence Cases

1. Have we notified and provide information as required by customers ☑yes☐No
2. If production was stopped not in accordance to normal procedure, has the product been verified in full conformity to requirement ☑yes☐no. Doc No: FPBO. XXX date 28 Apr 2019

Management Decision

.1. Start to contact water supply contractors, and understanding costing etc
2. Also look at cost of installing extra water tanks

Submitted by	**Approved by**

Remarks here explain on the Exhibit. Do not include them as part of your document

- This is a real case, with advance notice of emergencies.
- The contingency team did the calculation well in advance and found they could handle the situation with good safety margin
- The contingency team actually check implementation at the end of the water disruption, to see if the plan actually worked out.
- The outcome was good. But as the tendency of water disruption was getting frequent, contingency recommends to adopt some preventive measures.
- This is an excellent case of using contingency plan to ensure smooth operation, despite failure of other parties.

Exhibit 3-4. Contingency Plan Review. Page 1

Contingency Plan 2019

Review on 20 Mar 2019
Reviewer: XXX, XXX

No	Emergency Type	Impact	Current Controls	Risk Eval S	Risk Eval P	Risk Eval R	Response and Mitigation
1	Key Equipment Failure	Production interruption, affecting delivery (OK)	• Currently excess capacity, plenty of idling equipment • Approved subcon available (Excess capacity is decreasing as business is picking up)	H (OK)	L M	M H	• Switch over to another machine if a machine breaks down, if available • Contact subcons to process • Maintenance to improve reliability
2	External Supply Interruption	Production interruption, affecting delivery (OK)	• Multi-sourcing practised (OK) • Safety inventory of 2 days (OK) • Subcon A for plating having quality issue later-resolving (resolved) • Subcon B to come on line (came on and OK)	H (OK)	M L	H M	• Get from other approved sources if supply is uncertain (OK to continue) • ~~To source another plating subcon by June (Purchasing)~~
3	Transport Equipment Failure	Delivery affected (OK)	• Outsourced to contractor who promise backup within 2 hours • Org also has own trucks that can be used • So far no issue of transport • Store assistant Mr XXX who has licence for driving truck has resigned (OK- continue)	H (OK)	L (OK)	M (OK)	• ~~Ensure the replacement has the truck licence (HR)~~ • ~~Alternative, get one of other store assistance to get such a licence (HR & Store Manager)~~ • Mr XXX came back to work as driver
4	Recurring Natural Disaster-Flood	Delivery affected The external roads flooded. (OK)	• Build extra inventory during the monsoon months (Oct-Dec) • Request customer to keep extra inventory for the 2-3 months (customer accepted)	H (OK)	L (OK)	M (OK)	• Current measures good enough • In the event of uncertainty, inform General Manager

Exhibit 3-4. Contingency Plan Review. Page 2

5	Fire outbreak	Production facilities damaged, affecting production and delivery. (OK)	• Fire safety system fully in place • Electrical consultant checks on system every 3 months • No incident so far. (OK)	H (OK)	L (OK)	M (OK)	• To increase checks by electrical consultant every (2)month, as plastic is a high hazard industry for fire.
6	Utility Failure (power)	Production interruption, affecting delivery (OK)	• Standby generator can run some machines • If inform earlier, can build inventory • Catch up with over time, or weekend running (new)	H (OK)	L (OK)	M (OK)	• ~~Find contacts to rent large generator if require (Production Manager and Purchasing)~~- • Contact production manager immediately to authorize overtime or weekend running
7	Utility Failure (water)	Production interruption, affecting delivery (OK)	• If inform earlier, can build inventory • Catch up with over time, or weekend running (new)	H (OK)	L (OK)	M (OK)	• ~~Build backup water storage tank~~ . Done • ~~Find contacts to purchase water in tanker loads (Production Manager and Purchasing)~~ • Contact production manager immediately to authorize overtime or weekend running
8	Manpower interruption	Production interruption, affecting delivery (OK)	• Approved subcon available • Catch up with over time, or weekend running • Get more contract workers from manpower supplier • Manpower shortage experience in month of June	H (OK)	L M	M H	• Contact XXX or XXX • Develop a better system of estimating demand to have advance notice for recruitment
9	Infrastructure failure	Production interruption, affecting delivery	• Approved subcon available • Catch up with over time, or weekend running	H	L	M	• See above
		(OK)	• Get more contract workers from manpower supplier (OK)				
10	Computer affected by Cyber Attack or virus	Operation interruption, affecting delivery (OK)	• Computer data backed up every day, automatic • Antivirus at all terminals • Duplicate system available as redundancy, can kick in when the main system fail (OK)	H (OK)	L (OK)	M (OK)	• HOD to ensure compliance by checking monthly (Admin & Finance Manager)

Remarks here explain on the Exhibit. Do not include them as part of your document

- This is one way to conduct Contingency Plan review. A copy of the Contingency Plan is required for the team to review, line by line
- Pencil marking is acceptable. If there is no change, this is your evidence.
- However, if there are changes, the original document shall be revised to show changes. This will be the evidence of review instead
- Not only response plan can change, the current controls may also subject to change and so are the scoring
- Get the top management to sign or request his/her input, as the standard requires their participation

>>End of Chapter 3 <<