CHAPTER

8

Cultures, Structures, and Processes

This chapter explains how to design and develop an organization so that it more functionally manages security and risk. Organizational design conventionally recognizes three main dimensions of an organization, and this chapter's sections study each of these in turn: culture, structure, and process.

Cultures

A culture is a collection of the dominant norms, values, and beliefs in a group or organization. This section explains why security and risk managers should pay attention to culture, how they can assess a culture, and how they can develop a culture to be more functional.

Why Develop Culture?

Of the three main dimensions of an organization (culture, structure, process), culture is probably the easiest to neglect and most difficult to observe and change. Some standards of risk management now prescribe explicit attention to an organizational culture and urge development of a culture that is supportive of risk management and is congruent with the structure and process of risk management. The culture needs to support the structures and processes of risk management; an organization is less likely to manage risks well if its members normatively think of risk management as too burdensome, silly, pointless, or alien. For instance, developing the perfect process for how personnel are supposed to keep the office secure would be pointless if our personnel normatively ignore the process or encourage colleagues to ignore the process. Cultures are also important factors in how different risks are tolerated or rejected (see Chapter 9).

Some failures to manage security or risk correctly could be due to poor or incomplete training, but too often leaders would blame personnel competences and neglect to consider whether the culture needs attention. The personnel could be perfectly trained in the processes and perfectly aware of the authorities and responsibilities, but nonetheless not value or normatively comply with the processes or structures.

Pedagogy Box 8.1 Official Prescriptions for a Risk Management Culture

The British Standards Institution (2000) noted that the "role of culture in the strategic management of organizations is important because: the prevailing culture is a major influence on current strategies and future chances; and any decisions to make major strategic chances may require a change in the culture." It identified failures of risk management "due, at least in part, to a poor culture within the organization" despite the organization's proper attention to the process (p. 21).

Similarly, the International Risk Governance Council (2008, pp. 6, 20) noted that organizations and societies have different "risk cultures" that must be managed as part of risk management.

The Australian/New Zealand and ISO standard (International Organization for Standardization, 2009b) stresses in one of its 11 "principles for risk management" that risk management should take account of "human and cultural factors" and that the "framework" should be tailored to and integrated into the organization.

Assessing Culture

Culture is difficult to observe because it is less tangible than structure and process, but a researcher could directly observe organizational personnel in case they betray normative noncompliance with, negative valuations of, or incorrect beliefs about security and risk management.

The researcher could survey personnel with classic questions such as "Do you believe risk management is important?" or "Do you follow prescribed processes when nobody else is watching?"

Sometimes, a bad culture is betrayed by repeated failures to implement processes, to exercise authority, or to take responsibility for risk management. Ideally, such repeated failures should be observed currently by regular monitoring and reviewing and should prompt an audit that would diagnose the root causes (as discussed in Chapter 11).

Developing a Culture

Changing a culture is difficult, but obvious solutions include exemplary leadership, more awareness of the desired culture, more rewards for compliance with the desired culture, more punishments for noncompliance, and more enforcement of compliance.

Of course, we should also consider whether the negative culture is a reaction to something dysfunctional in the structure or process. For instance, perhaps employees are copying noncompliant leaders; perhaps employees have good reason to dislike some of the prescribed processes, such as processes that are too burdensome or that incorrectly assess certain risks. If the structure or process is at fault, the structure or process needs to change positively at the same time as we try to change the culture positively.

Ultimately, culture is changed and maintained only by congruence with structure and process, training of and communication to personnel of the desired culture, and cultural congruence across all departments and levels from managers downwards.

Pedagogy Box 8.2 Developing a "Security Culture"

"Much of the focus in security management tends to be on specific operational needs, such as security policies and plans, but there is also a need to take a step back and look at how to develop a culture of security within the organization, including developing capacity. One of the most important priorities is to make sure that all staff know the organization and its mission in any given context. It is not uncommon for many staff, including national staff, not to know much about the agency that they represent. Staff need to be told what the organization is about . . . In addition, treat security as a staff-wide priority, not a sensitive management issue to be discussed only by a few staff members behind closed doors. Specifically:

- Make sure that all staff are familiar with the context, the risks and the commitments of the organization in terms of risk reduction and security management.
- Make sure that all staff are clear about their individual responsibilities with regard to security, teamwork and discipline.
- Advise and assist staff to address their medical, financial and personal insurance matters prior to deployment in a high-risk environment.
- Be clear about the expectations of managers and management styles under normal and high-stress circumstances.
- Make security a standing item (preferably the first item) on the agenda of every management and regular staff meeting.
- Stipulate reviews and if needed updates of basic safety and security advice, as well as country-wide and area-specific security plans, as described above.
- Invest in competency development. It is not uncommon for aid agencies to scramble to do security training when a situation deteriorates. Investment should be made in staff development, including security mitigation competences, in periods of calm and stability.
- Ensure that security is a key consideration in all program planning.
- Perform periodic inspections of equipment by a qualified individual, including radios, first aid kits, smoke alarms, fire extinguishers, intruder alarms and body armor.
- Carry out after-action reviews (AARs). The focus is on assessing what happened and how the team acted in a given situation, not on individual responsibilities. It is a collective learning exercise." (Humanitarian Practice Network, 2010, pp. 13–14)

Structures

Structures are patterns of authorities and responsibilities. The authorities are those departments or persons assigned to determine how security and risk should be managed. The responsible parties are supposed to manage security and risk as determined by the authorities. The three subsections below respectively explain why the development of structure is important, give advice on developing the internal structure of an organization, and give advice on developing functional relations between organizations.

Why Develop Structure?

Structure is important because security and risk receive improper attention when the responsibilities or authorities are unclear or dysfunctional. The risk manager's role in advocating risk management is indicated by parts of the Australian and British governments that formally refer to lower risk managers as "risk champions."

Structure is important also to outsiders who want to know with whom to communicate. Imagine a stakeholder who wants to contribute to your security but cannot find the best authority within the organization (or cannot find an interested authority)—the wasted time, effort, and frustrations count as unnecessary transaction costs, could damage your reputation, and reduce the chances of future opportunities.

Structure is important to the efficiency of an organization, since clearer authorities and responsibilities reduce the transactions costs and redundant activities associated with confused or redundant authorities.

Developing Internal Structure

Understandably, most actors are private about their security and risk management structures, but we know that the structures of organizations are pulled in many directions by resource constraints, bureaucratic interests, political issue-linkage, and simple path-dependency, so organizational structure is commonly suboptimal, particularly in very small or poor organizations and in very large organizations (which have more resources but are subject to more vectors).

Two main trade-offs are within the control of the organizational designer: the trade-off between managerial control and burden and the trade-off between domain and cross-domain expertise.

Trading Managerial Control With Burden

Organizational designers need to be careful that they do not vacillate between:

- lots of well-specified authorities that are overwhelmed by responsibilities and inefficiently dispute each other, and
- poorly specified authorities that are unaccountable or unsure.

They should be careful too not to vacillate between:

- highly centralized management, which should be materially efficient but is remote from lower managers and possibly unaware of managerial practices at lower levels, and
- decentralized management, which could be more efficient for the system as a whole, if lower managers are self-motivated and skilled, but also hide dysfunctional practices from higher managers (Newsome, 2007, pp. 18–22).

Trading Domain and Cross-Domain Expertise

Traditionally, within government and large commercial organizations, the official centers of excellence or influence have been the departments of finance, defense, intelligence, internal or homeland security, and information management. Each of these departments offers some generalizable skills in risk or security management, but none can offer expertise across all departments and domains.

A small organization or operation is likely to be specialized in a certain domain. For instance, a financial services provider is specialized in financial risks. In large organizations, with cross-domain functions, domain specializations are required within departments, but are problematic across departments. In recent decades, this tension between intra- and inter-domain expertise has been seen in the success with which official and private organizations have successfully raised awareness of risk and security management and their structures and processes, while failing to manage all risks equally.

Some organizations have appointed directors of risk management or of security with cross-domain responsibilities: many of the persons are accountants, information technology experts, or former military or law enforcement personnel. Their professional pedigree should inspire some confidence, but each domain is particular and cannot offer experience or expertise across all domains. Cross-domain security and risk management needs cross-domain experience and expertise. This sounds rational, but naturally some people are more open to wider knowledge and skills than others ("foxes" are preferred over "hedgehogs"—to recall Isaiah Berlin's typology).

Security and risk managers from different domains can be stereotyped (although stereotypes allow for many exceptions). For instance, stereotypical financial officers are good at assessing the stark financial risks of projects (such as potential lost investment) but are less qualified to assess the technical risks (such as potential technological failures) that would compound the financial risks (such as the extra costs of urgently procuring an off-the-shelf replacement for the intended product of a failed project).

Stereotypical security and defense professionals are good at estimating the capabilities that they would want to use, but they are less qualified to assess technically the products that potential suppliers would offer them in order to deliver those capabilities. Good examples can be found in British government procurement of defense equipment (see Pedagogy Box 8.3); most democratic governments have experienced similar problems. Consequently, private advocates of technology risk management urge project managers to hold regular reviews of the technology risks with "technology champions and a peer group of subject-matter experts."

> As technologies move from the research bench to product development, there is an inherent tension between the technology champions and the product chief engineer. The technologist creates new concepts, new surprises, and new risks. He or she is optimistic, is successful if his or her ideas are adopted, and may overstate the merits. The chief engineer, on the other hand, tries to solve problems, avoid surprises, and minimize risk; he or she is successful if the product meets the specification on schedule, irrespective of the technology used. (Hartmann & Myers, 2001, pp. 37–38)

Similarly, stereotypical information managers and information security managers are experts in information technologies, but they have proven less competent at managing the risks of procurement. Most infamously, in 2002, the British National Health Service launched a National Programme for Information Technology with a budget of £6.2 billion, but after costing more than twice as much, most of its projects were canceled in 2011 by a different political administration, on the recommendation of a new Major Projects Authority.

Stereotypical intelligence or internal security professionals have proved themselves better at identifying threats than at procuring solutions. For instance, the U.S. Department of Homeland Security has been caught out procuring unproven technologies, such as systems ("puffers") designed to test the human body for the scent of explosives. From 2004 to 2006, the Transportation Security Administration acquired 116 systems at 37 airports, despite poor detection and availability rates during tests. All were deleted at a procurement cost of at least $30 million.

Pedagogy Box 8.3 The Structure of British Defense Procurements, 2000–2013

For decades the British Ministry of Defense (MOD) has struggled to procure equipment on time, within budget, and with the capabilities specified. In the 2000s, after many procedural changes, the main structural change was the merger of the Defence Procurement Agency and the Defence Logistics Organisation to form Defence Equipment and Support (DE&S). Savings were expected from consolidation of redundant assets and colocation of most staff at a site near Bristol. At the time of the merger in April 2007, the two parent organizations employed 27,500 people. In fiscal year 2009, DE&S received a budget of £13 billion and employed 25,000 people. However, the costs of improving staff skills absorbed most of the potential savings accrued from shedding staff, while the disruption retarded the new agency's performance, although urgent operational requirements (UORs) also contributed.

One preexisting managerial dysfunction was not changed: Almost annually, the House of Commons Committee of Public Accounts complained that program managers rotated in on short tenures of 2–3 years without accountability for the performance of programs that typically ended after their tenure:

> There is poor accountability for long-term equipment projects, such that no-one has had to answer for this prolonged failure of management. Senior Responsible Owners do not remain in post long enough to ensure continuity on large scale programs, making it difficult to hold anyone responsible for whether they succeed or fail. (U.K. MOD, 2011c, pp. 6, 8)

In early 2009, the MOD commissioned a report (known as the Gray Report, after Bernard Gray, the lead author), which found that the MOD's equipment acquisitions had arrived on average 5 years late and collectively cost £35 billion more than planned. Gray reported that the MOD was unfocused, "with too many types of equipment being ordered for too large a range of tasks at too high a specification." Gray reported that the acquisitions system had retarded military operations.

The programs with the worst time and budget overruns and rates of postponement or failure related to armored and fighting vehicles. In May 2011, the National Audit Office (NAO) reported that the MOD had initiated 8 armored vehicle projects since May 1992 at a sunk cost of £1,125 million.

- Three projects (Tactical Reconnaissance Armoured Combat Equipment Requirement; Multi-Role Armoured Vehicle; Future Rapid Effect System Utility Vehicle) had been canceled or suspended without delivering any vehicles and at a total cost of £321 million.
- Three projects (Future Rapid Effect System Specialist Vehicle; Warrior Capability Sustainment; Terrier Armoured Engineering Vehicle) remained delayed without delivering any vehicles at a total sunk cost of £397 million and total forecasted costs of £9,105 million.
- Only two projects (Viking All-Terrain Vehicle [Protected]; Titan and Trojan Engineering Vehicles) had delivered the required vehicles, but the numbers were comparatively trivial (total 166 vehicles required at a sunk cost of £407 million).

The report concluded that "given the expenditure of over £1.1 billion since 1998 without the delivery of its principal armoured vehicles—the Department's standard acquisition process for armoured vehicles has not been working."

Meanwhile, new vehicles or upgrades for legacy vehicles were required urgently for operations in Afghanistan (from 2001) and Iraq (from 2003). The British Army had sent some tracked fighting vehicles to Iraq and Afghanistan that were difficult to sustain and employ. British ground forces required more survivable versions of its wheeled logistical, liaison, patrol, and "force protection" vehicles. At first, the British upgraded legacy vehicles, which would be easier to sustain and to adapt after operations in Iraq and Afghanistan, but during 2007, the government authorized more substantial new models and upgrades to existing models. In 2007, about 40 UORs related to five types of armoured vehicle:

- two American-produced base models for Heavy Protected Patrol Vehicles (same as the American class known as Mine-Resistant Ambush Protected Vehicles); and
- three upgraded legacy vehicles—a better protected, armed, and automotively improved version (the Bulldog) of the FV432 (tracked) armoured personnel carrier, an armored and armed version of the BvS 10 (Viking) light articulated tracked all-terrain vehicle (previously procured for amphibious and arctic operations), and a ruggedized, partially armoured, and armed version (WMIK) of the most numerous four-wheeled vehicle (Land Rover).

Most logistical ("B") vehicles also required a protection kit. Many more types of new models of vehicle would be procured—mostly "off-the-shelf"—in following years, few of which would be required beyond current operations. Most of these vehicles arrived on operations during the period of net withdrawal rather than net reinforcement. Some never fulfilled the UORs that had been used to justify them.

The NAO blamed the Ministry (including implicitly the ministers) for poor planning and biases toward naval and aerial platforms.

> [T]he cycle of unrealistic planning followed by cost overruns has led to a need to regularly find additional short-term savings. Areas of the Defence budget where there have been lower levels of long-term contractual commitment, such as armoured vehicles, have borne the consequences of decisions to fund large scale and long-term projects in other sectors.

The NAO blamed the MOD also for specifying high capability goals, then failing to compromise given the technology available.

> Complex requirements have been set which rely on technological advances to achieve a qualitative advantage over the most demanding potential adversaries. However, for vehicles procured using the standard acquisition process there has not been an effective means to assess the costs, risks and amount of equipment needed to meet these requirements in the early

(Continued)

(Continued)

> stages. These demanding requirements often reduce the scope to maximize competition which in turn can lead to cost increases, delays to the introduction of equipment into service and reductions to the numbers of vehicles bought to stay within budgets. (U.K. NAO, 2011, p. 6)

The NAO suggested that the MOD could improve its standard acquisitions process by learning from UORs, which identify incremental requirements and technological opportunities beyond current acquisitions but warned that the MOD would need to combine planning for full sustainment and value for money beyond current operations. The NAO recommended that the MOD should improve its technological awareness and pursue evolutionary development within realistic technological opportunities.

> Firm delivery deadlines and budgets could further ensure realism in setting requirements. This could be achieved by engaging more closely with industry to assess vehicle requirements, based on mature technology, that are initially sufficient—and better than vehicles already in service—but having the potential for future development. The Department should consider buying vehicles in batches, with each subsequent batch offering improved capabilities within a lower initial budget approval, but based on a common vehicle design to minimize any differences in logistic support and training requirements. (U.K. NAO, 2011, p. 11)

The NAO had not fully investigated the structure, process, or culture of acquisitions, and some anonymous officials complained that the NAO was better at identifying past failings than solutions and better at blaming the MOD than the political decisions with which the MOD must comply. The political administration (Labour Party, 1997–2010) was not prepared to cut any procurement program during its many wars but instead incrementally trimmed the funding or projects from practically all programs, many of which consequently could not achieve their specified capabilities.

The budgeting system also created structural problems. As in the United States, national government in Britain is paid for from annual authorizations, within which the MOD matches money to programs, with little spare capacity at the time, so when one program overran its budget or suffered a cut in budget, money was robbed from other programs or the program's activities or objectives were cut. The Committee of Public Accounts found that from 2006 to 2011 the MOD had removed £47.4 billion from its equipment budget through 2020–2021, of which 23% (£10.8 billion) covered armored vehicle projects. The Committee recommended that the MOD "should ensure that future procurement decisions are based on a clear analysis of its operational priorities, and must challenge proposals vigorously to ensure they are both realistic and affordable. Once budgets have been set, they must be adhered to. The Department's inability to deliver its armoured vehicles programme has been exacerbated by over-specifying vehicle requirements and using complex procurement methods" (U.K. MOD, 2011c, p. 5).

The Treasury was most influential over UORs, since it capped the budget for all UORs and often meddled with individual UORs, with the result that MOD departments fought mostly internally over the few UORs that could be approved—those approved tended to be the cheaper UORs. Since the users of the products of these UORs often were multiple or inconsistent, the user was weakly represented in

these decisions. Special Forces were the most consistent and politically supported users, so tended to enjoy the best success rate, but often with undesirable outcomes for other users. For instance, the MOD acquired a new light machine gun for the whole army—it had satisfied the requirement from the special forces for an ambush weapon but was practically useless in most of the long-range defensive engagements in Afghanistan. Similarly, the MOD acquired lots of small fast unarmoured vehicles that were useful for special operations but soon deleted from the fleet. Some of the vehicles that were acquired via UORs met justifiable UORs (the more survivable vehicles were most required), but they were usually acquired without training vehicles, so users often first encountered new types of vehicles only after deploying.

The Labour government had promised to publish Gray's report in July 2009 but reneged until October, then deferred most consideration until the next Strategic Defence Review. A national election (May 6, 2010) delayed that review.

On February 22, 2011, 9 months after taking office as Defence Secretary Liam Fox announced his first reforms of the MOD's procurement process, which he condemned as "fantasy defence procurement" and a "conspiracy of optimism." He promised that procurement projects would not proceed without a clear budgetary line for development, procurement, and deployment. He announced a Major Projects Review Board (under his own chairmanship) to receive quarterly updates on the MOD's major programs—first the 20 most valuable projects, followed by the rest of the 50 most valuable projects. The Board met for the first time on June 13, 2011. Following the meeting, the MOD asserted that

> Any project that the Board decided was failing would be publicly "named and shamed." This could include a project that is running over budget or behind expected timelines. This will allow the public and the market to judge how well the MOD and industry are doing in supporting the Armed Forces and offering taxpayers value for money.

The Defence Reform Unit's report was published on June 27, 2011. The Report made 53 wide-ranging recommendations, the most important of which was for a smaller Defence Board, still chaired by the Defence Secretary, but without any military members except the Chief of Defence Staff. The three Service Chiefs were supposed to gain greater freedom to run their own services. The services would coordinate primarily through a four-star Joint Forces Command. The MOD would form separate Defence Infrastructure and Defence Business Services organizations. Another recommendation was to manage and use senior military and civilian personnel more effectively, transparently, and jointly, with people staying in post for longer, and more transparent and joint career management. An implementation plan was expected in September 2011, for overall implementation by April 2015. The process of acquisition was not expected to change, although the structure would. The Select Committee on Defence (U.K. House of Commons, 2011b, Paragraph 207) recommended that the MOD should appoint "suitably experienced independent members" to the Board.

On September 12, 2011 (speaking to the Defence & Security Equipment International show in London), the Defence Secretary claimed that Britain's "forces in Afghanistan have never been so

(Continued)

(Continued)

well-equipped." In Afghanistan at that time, British forces employed about 10,000 military personnel and 22 different models of armored vehicle at a cost in 2011 of £4 billion (from contingency reserve, above the core defense budget of £33.8 billion in fiscal year 2011–2012). The U.K. MOD was in the middle of a 3-month study into the Army's future vehicle fleet—clearly most of the armoured or fighting vehicles returning from Afghanistan (by the end of 2014) would not be required for the core fleet; some could fill core requirements but the cost of repatriating, reconfiguring, and sustaining even these vehicles would be prohibitive in an era of austerity.

On May 14, 2012, Defence Secretary (since October 2011) Philip Hammond announced to the House of Commons his latest reforms.

> Under the previous Government, the equipment plan became meaningless because projects were committed to it without the funding to pay for them, creating a fantasy program. Systematic over-programming was compounded by a "conspiracy of optimism", with officials, the armed forces, and suppliers consistently planning on a best-case scenario, in the full knowledge that once a project had been committed to, they could revise up costs with little consequence. It was an overheated equipment plan, managed on a hand-to-mouth basis and driven by short-term cash, rather than long-term value. There were constant postponements and renegotiations, driving costs into projects in a self-reinforcing spiral of busted budgets and torn-up timetables. Rigid contracting meant that there was no flexibility to respond to changed threat priorities or to alternative technologies becoming available. It is our armed forces and the defense of our country that have ultimately paid the price for that mismanagement. The culture and the practice have to change.
>
> We will move forward with a new financial discipline in the equipment plan. There will be under-programming rather than over-programming, so that we can focus on value rather than on cash management. That will give our armed forces confidence that once a project is in the program, it is real, funded, and will be delivered, so that they can plan with certainty.

Hammond announced that further reductions in British commitments to the most expensive programs (aircraft and aircraft carriers), on top of reductions since 2010 in military and civilian personnel, bases, and other assets and equipments, finally had eliminated the gap, worth £38 billion (then worth US$61 billion), between commitments and budgets out to 2020. (Over the next 10 years, the MOD planned to spend nearly £160 billion on the acquisition of equipment and data systems, including, for the first time, a "contingency reserve" fund worth £4 billion. Only £4.5 billion of that spending was allocated to new or upgraded armored vehicles. The annual budget was worth £34.4 billion in the fiscal year in which he made his announcement. For the year beginning April 2013, the annual budget would be £34.1 billion.)

On January 31, 2013, after the Treasury had cut future funding, the MOD announced the first fully funded defense equipment procurement plan to be reviewed by the NAO, worth £60 billion over 10 years (although this is also the period that some economists forecasted for continuing public austerity).

Developing Interorganizational Coordination

Coordination between organizations implies benefits such as mutually improved security and reduced collective costs. The Humanitarian Practice Network (2010, pp. 17–18) promised the following benefits:

- A better alert system: Agencies receive a fuller picture of actual or possible security threats or alerts in their environment, which increases the chances of avoiding an incident. This can be supported by a "communications tree" using mobile phones, e-mail, and radio. It can also be supported by a common emergency radio channel.
- Better risk assessment: A central record of all incidents and near misses in a given operating environment is a better basis for a risk assessment than a partial or incomplete record.
- Strategic and tactical monitoring and analysis of the operating environment and its security implications: Every agency has to do this and will normally contact others informally to obtain information. Where there is trust and confidentiality is respected, it is possible to collaborate in a more structured way.
- Cost-effective extra capacity or services: Rather than each agency individually carrying the costs of bringing in or hiring additional skills, specialists can be brought in on a collective basis. The costs for a training event on security can also be shared.
- Liaison and engagement with the authorities: Rather than negotiating individually, agencies can potentially make a stronger and more consistent case together.
- Advocacy with donors: If the security situation deteriorates and several agencies conclude that they need extra financial resources for additional mitigating measures, they may be able to make a more effective case with donors collectively.

Security coordination implies deliberate cooperation, more than commercial relationships, political alliances, or rhetorical friendships. For instance, after 9/11, the United States signed many bilateral agreements with other governments in which both governments stated their shared commitment to fighting terrorism; sometimes the United States promised money to help the other government develop its counter-terrorist capacity; however, few of these early agreements specified how the two governments were supposed to coordinate their counter-terrorist activities, to measure their coordination, or to hold each other accountable for their coordination. Meanwhile, other governments, with whom the United States had made no new agreements, coordinated better (Newsome, 2006).

No international standard for interorganizational coordination has been agreed, but the Humanitarian Practice Network (2010) noted the following common practices:

- Informal networking, for example, periodic meetings or an informal network of security focal points.
- Interagency security measures, such as a shared residential guard network, sharing of field-level security focal points, or security training.
- Introducing security as a theme in existing interagency working groups.
- Interagency security and safety offices, which can be independently resourced and led, or hosted by nongovernmental organizations.

An interagency security mechanism may have several functions, including

- Convening security meetings
- Providing security alerts, cross-checking unconfirmed information, and facilitating information dissemination
- Carrying out risk assessments and pattern and trend analysis and communicating the results in threat reports
- Providing introductory security briefings, as well as technical assistance and advice to individual agencies, and training
- Crisis management: Providing support with contingency planning and facilitating in-extremis support; for example, if an agency suffers a critical incident such as a kidnapping, the platform might be able to provide additional analysis and support through local networks.
- Liaison with governmental authorities, international and national military forces, including UN peacekeeping forces, and private security companies (p. 19).

Coordinating security between organizations is not easy, even when objectively each organization has a self-interest in coordination. Commercial competition inhibits coordination, although security against third-party threats does not need to affect commercial competitiveness. Many private actors assume that official authorities will protect them, but officials cannot be expected to follow every private actor or activity, particularly in remote locations. Some private actors inflate their self-reliance, without realizing the benefits of coordination or the interdependency of risks. Table 8.1 summarizes the possible impediments and approaches to coordination.

As an example from Table 8.1, consider structural or geographical separation as a barrier to coordination between organizations. A commonly understood solution is to exchange "liaison officers." For instance, the British national government sends Government Liaison Officers to local Emergency Control Centers, the Ministry of Defense appoints Joint Regional Liaison Officers to each of the Emergency Control Centers, and local governments appoint a "Host Organization Lead Officer" to manage mutual aid. Organizations are supposed to appoint (news) Media Liaison Officers too.

Processes

A process is a series of actions or activities toward some end. The subsections below explain why the development of a prescribed process of security and risk management is important and gives examples of standard processes to choose from.

Why Develop Process?

Each of us has a process for managing the risks of everyday life, but not all processes can be perfect, and we should not allow every possible process. With useful experience or guidance, we could develop a process that reminds us to perform actions or activities that are necessary to proper security and risk management. As an organization, we should standardize that process to help managers perform closer to the ideal. A standard process also helps interoperability and communications between personnel and organizations. Most authorities or standards today prescribe or suggest a process by which risk or security is supposed to be managed (see Table 8.2).

Table 8.1 Impediments and Approaches to Security Coordination

Impediments		
Category	**Examples**	**Approaches**
Material	*Resource constraints*	*Resource pooling, risk sharing, shared controls, review risk assessments, and efficiency of controls*
	Physical separation	*Liaison officers and communications*
Cultural and social	*Linguistic or cultural differences*	*Multicultural employees or experts*
	Self-reliance culture	*Set coordination as a corporate objective*
	Internally oriented culture	*Develop external orientations*
	Pursuit of relative gains	*Reward absolute gains*
Structural and strategic	*Competing objectives*	*Cooperative objectives*
	"Buck-passing" (passing one's own responsibilities to another)	*Accountability to a third party*
	Redundant authorities	*Consolidate authorities*
	Ambiguous responsibilities	*Define responsibilities*
Procedural and Personnel	*Ill-defined or incompatible processes*	*Standardize a process*
	Lack of expertise	*Train or employ experts*
Political	*Political issue linkage*	*Prohibit changes outside of major policy changes*
	Politicization	*Nonpartisanship*
	Political sensitivities	*Compartmentalized information assurance*

SOURCES: Based on Newsome, 2006; Newsome & Floros, 2008; Newsome & Floros, 2009.

Choosing Between Processes

Standard processes are usually communicated visually as a list, series, or cycle of steps. As far as I know, all standard processes have at least three steps. For instance, British government has defined risk management with three steps (identifying, assessing, and responding to risks), although it has prescribed processes with four to six higher steps and much explanatory text on the lower steps and activities (U.K. Treasury, 2004, pp. 9, 13). The U.S. government has no standard but the GAO's five-step process (see Table 8.2) is probably the most authoritative and specified within U.S. government, so for these reasons, at least, it deserves fuller description here (although I do not consider it ideal).

Table 8.2 The U.S. GAO's Process for Managing Risk in More Detail

Higher Step	Summary of Activities	Example Activities	Example Outcomes
Establish our strategic goals, objectives, and constraints	Gather information on our ends and means	Discovery of what the strategic goals are attempting to achieve and of the steps needed to attain the goals	Information on our desired end states; our strategic goals and subordinate objectives; the activities required to reach objectives; our priorities, milestones, and outcome-related performance measures; and the limitations or constraints that would affect outcomes
Assess risks	Identify key elements of potential risks	Analyze threats; estimate vulnerability of assets; identify consequences of threats to assets	Information on threats, vulnerabilities, and potential outcomes
Evaluate alternative responses	Evaluate alternative controls on the risks	Consult outside experts on the controls; cost-benefit analysis of controls	Information on the effectiveness and costs of alternative controls; specifications for the controls
Select responses	Consider and choose between alternatives, given information from previous step and other managerial information, such as funding	Establish organization's risk tolerance; establish managerial valuation of controls and assets	Information on managerial choices between controls and allocation of resources
Implement and monitor the responses	Implement controls and a system for updating our security	Implement the controls according to the strategy; test the controls periodically; relate to peer and to higher risk management	System for monitoring effectiveness of risk management; system for developing risk management in response to new assessments or lessons learned

SOURCE: Based on U.S. GAO, 2005c.

Illustrating the inconsistencies within U.S. government, the DHS (2009, p. 111) recognizes a *risk management framework* as a "planning methodology that outlines the process" in six effective steps (see Table 8.3).

The most internationally influential process since 1995 is the Australian/New Zealand standard (also the ISO process since 2009), with seven well-established higher steps. It defines the "risk management process" as the "systematic application of management policies, procedures, and practices to the activities of communicating, consulting, establishing the context, and identifying analyzing, evaluating, treating, monitoring, and reviewing risk." It distinguishes the process from the "framework" (the "set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the organization") (ISO, 2009a, pp. 2–3). Other authorities refer to processes, "frameworks," and "models" interchangeably (Australian and New Zealand Joint Technical Committee, 2009, pp. 13–21).

The steps of these processes largely align (see Table 8.3), although some processes are missing important steps. For instance, much theoretical work would support establishment of our internal

objectives and the external context at the start of the process and prescribes communication with stakeholders throughout the process, but these steps are explicit in few of the processes in Table 8.3. The British Treasury's guidance, the Australian/New Zealand/ISO standard (2009), and the International Risk Governance Council (2008, p. 7) each treat *communication* as a continuous activity throughout the process. The Australian/New Zealand/ISO standard treats *monitoring and reviewing* too as a continuous activity, but the British Treasury does not specify these activities. The Australian/New Zealand/ISO standard refers to good communications, monitors, and reviews leading to "mature" or "enhanced" risk management that shows continual improvement, full accountability for risks, application of risk management to all decision making, continual communications about risk, and full integration of risk management into organizational structure.

Pedagogy Box 8.4 The ACTION Process for Managing Criminal Risks

1. **A**ssessing risk (mostly by identifying criminal threats and hazards and their potential victims)
2. Making **C**onnections (largely between criminals and between criminals and targets)
3. Setting **T**asks to control the risks (mostly preventing crime and preparing to respond to crime)
4. Collecting **I**nformation about the effectiveness of the controls
5. Refining the **O**rganization (properly structuring authorities, responsibilities, monitoring, training, and decision making)
6. **N**otifying others (mostly communicating about the risks and controls to stakeholders) (Kennedy & Van Brunschot, 2009, p. 125)

SUMMARY

This chapter has

- defined culture,
- explained why we should care to develop the culture of security and risk management,
- advised on how to assess a culture,
- advised on how to develop a culture,
- defined structure,
- explained why the design and development of organizational structures is important,
- given advice on developing the internal structure of an organization,
- shown how to develop relations between organizations,
- defined process, and
- compared different standard processes.

Table 8.3 Different Processes for Managing Risks, With Their Equivalent Steps Aligned

Australian/ New Zealand (1995) and ISO (2009)	Carter (1994, pp. 71–73)	Waring and Glendon (1998, pp. 8–9, 25)	Turnbull and Internal Control Working Party (1999)	U.K. NAO (2000, pp. 42–44)	U.K. Prime Minister's Strategy Unit (2002); U.K. Treasury (2004)	U.S. GAO (2005c)	U.S. FEMA (2005)	U.S. DHS (2009, p. 110)	Public Safety Canada (2011a, p. 14); also follows ISO (2009)	International Risk Governance Council (2008)
Establish the context	-	*Set policy*	*Set objectives*	*Clarify objectives*	*Understand context*	*Set strategy*	-	*Set goals and objectives*	-	*Preassessment*
Identify risks	*Identify risks*	*Identify hazards*	*Identify and evaluate risks*	*Identify risks*	*Identify risks*	*Assess risks*	*Identify threats*	-	*Ongoing hazard analysis*	
Analyze risks	*Evaluate risks*	*Assess hazards and consequences*		*Assess risks*	*Assess risks*		*Assess values of assets*	*Identify assets*	*Analyze impact on critical infrastructure*	*Appraisal*
		-					*Assess vulnerabilities*	-	*Determine aggravating or mitigating factors*	
Evaluate risks		*Estimate risks*					*Assess risks*	*Assess risks*	*Risk analysis*	*Characterization and evaluation*
Treat risks	*Control risks*	*Evaluate controls*	*Treat risks*	*Respond to risks*	*Respond to risks*	*Evaluate alternative responses*	*Consider mitigation options*	*Prioritize and implement protection programs and resiliency strategies*	*Recommendations to decision makers*	*Management*
		Select control				*Select response*				
	Mitigate	*Implement*				*Implement and monitor*				
Monitor and review	*Improve*	*Monitor*	*Review*	*Monitor and review*	*Review*			*Measure performance*	-	
		Audit								
		Review						*Take corrective action*		
Communicate and consult		-	*Communicate*	-	*Communicate and learn*	-	-	-	-	*Communication*

QUESTIONS AND EXERCISES

1. Why does culture matter?
2. Give some symptoms of a dysfunctional culture.
3. Why might personnel fail to follow a process, despite extensive training in the process?
4. How could you assess a culture?
5. Describe the conventional ways to develop a culture.
6. When might we assess a culture as dysfunctional but change the structure or process?
7. What is the difference between authority and responsibility?
8. Why would your internal organizational structure matter to security managers or risk managers outside of your organization?
9. What are the two main trade-offs that an organizational designer faces when structuring risk management within an organization?
10. What is good or bad about security and risk management authorities that are
    a. highly centralized,
    b. highly decentralized,
    c. highly specified, or
    d. unspecified?
11. Of what should you be wary, when promoting a security and risk manager from one domain within the organization to responsibilities in another domain or across domains?
12. What are the five main categorical impediments to interorganizational coordination?
13. How could we mitigate problems associated with geographical separation of two cooperating organizations?
14. How could we develop the cultures of two organizations that are supposed to be cooperating but tend to self-reliance?
15. How could we change a tendency for one organization to pass its responsibilities to another organization?
16. What should we do in response to complaints from two organizations that they manage risks differently?
17. What could we agree with another organization if both organizations are worried about political linkage of our shared management of security or risk with irrelevant issues?
18. Why should managers not be allowed to choose their own process for managing security or risk?
19. Reconsider the U.S. and Australian/New Zealand processes.

a. What is different and the same between them?
b. Develop a process that combines the best of both.

20. Reread Pedagogy Box 8.3 above about the structure of British defense acquisitions.
    a. Identify examples of imperfect authorities.
    b. Identify examples of imperfect responsibilities.
    c. Identify examples of procedural failures.
    d. What sort of organizational culture would you expect as a result of or in support of the identified structural and procedural failings?
    e. What were the structural reforms introduced in 2011?
    f. What were the procedural reforms introduced in 2011?
    g. What further structural or procedural reforms would you recommend?