Responsible Care & Security Code (ACC)

Table of Contents

Executive Summary **2**
1. Overview **3**
2.1 Responsible Care 3
2.2 Security Code 4
2. History **6**
3.1 Responsible Care 6
3.2 Security Code 9
3. Implementation: Security Code **12**
5.1 Enforcement: Responsible Care 14
5.2 Cost of (Non-)Compliance 15
4. Evaluation **17**
5.1 Responsible Care 17
5.2 Security Code 19
5. Lessons for AI standards **20**
6. Acknowledgements **21**
Appendix **22**
A. Security Code ACC (2021 version) 22
B. Security Code nefic (Source) 26

Executive Summary

- Responsible Care is a **voluntary industry initiative** dedicated to improving the performance of companies in the chemical industry with regards to the environment, public health and overall security. The Security Code is a component of it that was introduced in 2001.
- Abiding by the rules in the Responsible Care program is a **prerequisite to becoming** (**and staying**) **a member** of the chemical industry trade association. Implementation is often nation-based, but international agreements and trade associations exist.

- A driving force behind the creation of both the Responsible Care program and the Security Code was **dwindling public opinion** of the entire chemical industry, fueled by infamous historical events (the Bhopal disaster and 9/11, respectively).
- Additional incentives for initiating this program included a **desire to get ahead of regulators to prevent a larger regulatory burden as well as financial and legal considerations**.
- Key success factors were the **successful assurance of wide stakeholder buy-in**, including small and large companies, market research on the public's responsiveness to various messages and an overall **climate that was pushing towards increased safety standards**.
- The Responsible Care Program and in particular the Security Code **paved the way** for the CFATS, a regulatory regime focused on the safety of chemical facilities from terror attacks.

- Key components of the security code that are reflected in the CFATS standards are a **risk-based tiered system** and the site vulnerability assessments. Implementation guidance is provided by both the chemical trade associations themselves and the private sector.
- Lack of rigid enforcement mechanisms presented an **early barrier to securing external credibility and re-gaining public trust**. Reforms were made to introduce third-party audits.
- While signing onto the program comes with initial cost, a variety of expected benefits await participating companies that reduce cost in the long run, e.g. **reduced regulatory burden**, **enhanced information sharing, reduced liability, improved public image and improved workforce attraction/retention**.

- There is **mixed evidence** on how successful both programs were in increasing safety.
- It appears large amounts of the benefit come through **indirect effects** such as improvements of organizational culture, normative and mimetic forces, spillover effects and knowledge diffusion.
- Downsides include risks associated with **regulatory relief** and a **lack of sufficient enforcement and sanctioning**.
- The evolution of both programs illustrate a clear **tradeoff** between providing clear and strict standards to satisfy the public and regulators and an incrementalist approach that starts with light-touch recommendations and becomes increasingly accountable and safety-focused.
- Changes over time also show how important it is for regulatory regimes and voluntary standards to **develop and evolve over time** to meet the changing needs of the regulatory landscape.

1. Overview

This report investigates the Responsible Care program initiated by the chemistry industry, with a particular focus on one of its components that was added at the beginning of this century: the Security Code. While there naturally is some overlap between the two, most of the following chapters of this report will follow a more or less strict division to maintain some sharpness of separation and allow for more analytical depth. We begin by quickly introducing the two programs, before diving deeper into their respective histories to identify dynamics that have contributed to their inception and their subsequent development. We then look at how they are implemented and enforced, also taking into consideration the cost of compliance as a relevant factor. Finally, we reach a preliminary conclusion about the effectiveness of these programs before synthesising our findings to draw conclusions about lessons that can be learned for the development of standards and voluntary industry programs in the field of Artificial Intelligence.

2.1 Responsible Care

The Responsible Care program is a global voluntary initiative of the chemical industry to improve their performance in fields ranging from environment, health and safety to security. It started out as an attempt to set standards for inputs, not outputs (Source), allowing participating companies to decide how they would meet a specific requirement, how they measure it, etc. Members who participate in the program commit to (Source):

- Signing the Responsible Care Guiding Principles
- Tracking and transparently reporting company performance on environmental, health, safety and security metrics

  These metrics include, but aren't limited to:

  - *Environmental metrics*, including hazardous air pollutants released, SOx and NOx emissions and water use at our facilities.
  - *Energy impacts*, including the energy efficiency of our facilities and greenhouse gas (GHG) emissions.
  - *Worker and facility safety*, including the number and severity of facility safety incidents, transportation and incidents and worker injury or illness.

- Undergoing third-party audit and certification to Responsible Care Management System (RCMS®)/RC14001®
- Implementing the Product Safety (output-oriented), Process Safety (operations-focused) and Security Codes

Committing to these components is a prerequisite for membership in a variety of associations, most notably the American Chemistry Council (ACC), the Canadian CIAC or the European Chemistry Industry Council (cefic)[1], although the implementation is delegated to the respective national chemical associations in Europe (Source). On a higher level, these nation-based associations coordinate their efforts through the International Council of Chemical Associations (ICCA). According to the ICCA, which was formed in 1989, chemical associations in nearly 70 countries have signed on to the RC standards (Source), among them China (Source), India (Source) and a number of Gulf states (Source). The ICCA also hosts a "Responsible Care Leadership Group which exercises guardianship over Responsible Care globally and connects with other international institutions such as the United Nations Environment Program (UNEP)." (Source)

Thanks to its widespread acceptance and proliferation (and against its original intention), the Responsible Care program has also served to inspire governmental regulatory efforts like the Chemical Facility Anti-Terrorism Standards (CFATS).

2.2 Security Code

The *Security Code* is one of three Codes (the others being the *Product Safety Code* and the *Process Safety* Code) that members of the ACC Responsible Care program must sign on to. It was added in the early 2000s in the aftermath of the 9/11 terror attacks and focuses on ensuring the security of the production and distribution process:

> "The purpose of the Security Code is to protect people, communities, property, products, processes, information, and information systems by enhancing security throughout the chemical industry supply chain. The chemical industry supply chain encompasses company activities associated with the design, procurement,

[1] "Cefic's role is to promote Responsible Care® in Europe and to ensure consistency of implementation by national member federations. Each Cefic member federation is responsible for developing and running its own national Responsible Care® programme with its member companies, and for overseeing implementation by those companies." (Source)

> manufacturing, marketing, distribution, transportation, customer support, use, recycle and disposal of our products." (Source)

A focus on security seems particularly relevant for companies in the chemical industry given they regularly obtain, process or distribute potentially high-risk materials and resources. Therefore, the Security Code primarily aims to protect against the following threats (Source):

- Theft of products on site or while in supply chain
- Use as precursors for chemical weapons
- Use as precursors for narcotics/drugs
- Illicit use of dual-use chemicals
- Product is designed for legally-sanctioned uses but can also be used to harm others
- Plant sabotage
- Cause economic or physical harm to company or industry
- Deliberate release to injure local communities or environment
- Threats can come from both external and internal sources.

The Security Code recommends actions to mitigate against these risks based on a four-tiered system, in which facilities which are considered higher risk need to take stronger precautions and security measures (Source). Shortened from 13 initial management practices to 10 in 2021, the Security Code recommends among other measures that companies shall conduct so-called "SVAs" (security vulnerability assessments) for their facilities, which are then used to determine adequate and appropriate measures of risk reduction (Source). It also encourages coordination and cooperation with other stakeholders: "Through the Security Code, ACC member companies have enhanced coordination, conducted training and safety drills, and shared important security information with local emergency response teams." (Source). Finally, the Security Code includes reporting requirements, which can be subdivided into incident and threat reporting requirements.

Similar to the Responsible Care program itself, the Security Code was first introduced in North-American countries before spreading globally and being adopted in the European Union in 2010. The European version has been condensed down into 7 key components (Leadership Commitment; Risk Analysis; Implementation of Security Measures; Training, Guidance and Information; Communications, Dialogue and Information Exchange; Response to Security Threats; Incidents and Audits, Verification and Continuous Improvement), a detailed version of which can be found in the Appendix.

2. History

3.1 Responsible Care

The Problem

The history of the Responsible Care program begins in the 1980s, when chemical companies started to become aware that public opinion was declining sharply (Source, Source). The percentage of people who were holding a "favorable opinion about the industry fell from 30 to 14 per cent" (Source). What made this observation particularly interesting for the chemical industry was that it appeared it was directed at the industry as a whole, not at individual companies, which presented individual companies with a new challenge:

> "When Dow Canada measured public opinion as a function of distance from its facilities in the early 1980s, the results were instructive. Within six kilometres of the plants, people held specific opinions about Dow that were different from their opinions about the industry as a whole. But beyond six kilometres, peoples' image of Dow was shaped by their image of the industry. As then Dow President David Buzzelli observed, the exemplary behaviour of Dow's plants was practically irrelevant; Dow was being judged by the behaviour of the industry as a whole." (Source)

Where did this scepticism come from? "Surveys commissioned by the CMA in the 1980s suggested that the public did not trust the industry because chemical firms seldom shared information on their operations, the risks their activities posed to communities, and their plans for dealing with industrial accidents." (Source) It surely didn't help that the 1980s saw a variety of chemical accidents around the globe, the most prominent of them the 1984 Bhopal disaster which has been estimated to be the source of 3,000 to 16,000 deaths. These events were not restricted to Asia though, as became painfully obvious only one year later: "In 1985, the leak from Union Carbide's pesticide plant in Institute, West Virginia, underlined that Bhopal-type tragedies could occur in the United States as well." (Source) The chemical industry quickly realised that public backlash was inevitable, which provided a fertile ground for the search for a new industry program centred around safety and corporate responsibility. Or, as Pierre Choquette (president of the plastics division at NOVA) put it at the time: "Responsible Care is absolutely essential to the survival of our industry." (Source)

Incentives

However, improving public opinion was not the only motivation that contributed to the establishment of the Responsible Care program:

- Getting ahead of regulatory efforts was a way to "protect member firms from injurious government regulation" (Source). Chemical companies were aware of the fact that if they didn't act, it was more than likely they would be subject to stricter

and more expensive legislation (Source, Source): "Industry leaders were concerned that high levels of policy activism would impose sizable costs; command-and-control policies often leave firms with little operational flexibility. There was also a fear that the uncertain external political and economic environments would erode investors' confidence in the industry's long-term prospects, thereby hurting its stock prices." (Source)

- There were additional economic incentives to improve their performance in areas like environmental protection and public health: "Roadway Express [an insurance company] is willing to offer discounts to firms that can document their efforts in the Product Distribution Code. Some brokers such as Zurich American and United Capitol are giving discounts up to 30% on environmental impairment liability (EIL) premia depending on the level of implementation of Responsible Care." (Source)

Taken together, these factors aligned to create an ecosystem that made it attractive enough for industry leaders to investigate and explore voluntary initiatives as a means to improve their reputation and secure their profits. But what were the steps that led to the eventual establishment and widespread implementation of the programme? To understand, we need to go back to the 1980s, and we need to go to Canada, where the federal government commissioned a study of 12 chemical industry leaders. This eventually led to a report that included key "Guiding Principles", which later became the backbone of the Responsible Care Program. Accelerated by the Bhopal disaster, a special board appointed by the Canadian chemistry industry association at the time (the CCPA) approved a motion to make Responsible Care mandatory for all members, requiring them to review their safety practices and to publish their findings (Source). It was not until the late 1980s that the CCPA got in touch with the US Chemical manufacturers Association (CMA, now the American Chemistry Council, ACC), which led to its adoption in the US. According to the Boston College Center for Corporate Citizenship, "[m]ore than 200 experts from the industry worked together to write the codes" (Source)[2]. It's important to note a few additional factors that benefited the quick adoption in the US-American context:

Success factors

- Industry leaders went to great lengths to identify the need they were trying to meet with this program, and worked hard to adapt it to its "market": "Before CMA unveiled its "Responsible Care" campaign in 1990, in conjunction with the 20th anniversary of Earth Day, every aspect of the program was test-marketed. The campaign emphasised a "commitment to improve performance" because CMA knew

[2] One year later, in 1989, the International Council of Chemical Associations (ICCA) was formed, which became responsible for the global implementation of the program (Source).

from polling and focus groups that such a message would be "the strongest message the industry can deliver." (Source)

- Wide stakeholder buy-in was ensured by engaging not just the public, but also key industry leaders: "'The key to success is to have top management commitment and buy-ins from companies,' Roczniak said. In the late 1980s, a group of chemical companies' CEOs, together with representatives from the American Chemistry Council, went on a 'road show to sell the idea of an industry-wide code of conduct.'" (Source)
- Benefits for both small and large companies were emphasised: "Responsible Care was championed by the large chemical firms such as Dow and Union Carbide that felt vulnerable to the rising public sentiments against the chemical industry. They undertook the initial steps, first in Canada and then in the United States, to establish it. To create incentives for the smaller firms to support it, they established mechanisms for knowledge transfer, thereby reducing the costs for the smaller firms to adopt this code." (Source)

Evolution

Over time, the Responsible Care Program has evolved to accommodate the increased needs for security and assurance. For instance, the original version did not include any kind of third-party verification, which made their "stated policy [...] to revoke the membership of any company that persistently conducts its operations in a manner inconsistent with Responsible Care" somewhat difficult to enforce. Companies did have to submit self-assessments that outline their progress on targets inspired by the program, but were actively encouraged to "go at their own pace" (Source). The lack of verification mechanisms also meant that public trust was more difficult to regain. Therefore, audits were introduced in the early 2000s, a period that saw a variety of structural changes and adjustments to the program. Among other reforms, the ACC introduced performance-based tracking of certain metrics including the public reporting of these metrics, alongside introducing new performance requirements (e.g. relating to cybersecurity) for chemical companies to follow (Source). One driving factor of these changes was a changing regulatory landscape: "[I]n the early years following the adoption of Responsible Care, laws and regulations already mandated approximately 13% of the program's content. By 2000, government requirements covered about 75% of the program's codes and practices. Thus, a program originally designed to demonstrate leadership beyond compliance could no longer credibly claim that it was pushing the performance envelope" (Source). Nevertheless, the program achieved remarkable growth and international recognition, which culminated in the publication of a global Responsible Care charter by the International Council of Chemical Associations (ICCA) in 2004. In the

following decade, the Responsible Care program was able to grow domestically and internationally, and the ACC that houses the program now has more than 130 member companies which represent between 85-90% of US chemical production by volume (Source) and account for approximately 90% of its revenue (Source).

3.2 Security Code

Background

Similar to how unique historical events and circumstances kickstarted the Responsible Care program, so did a specific part of it come into existence in the early 2000s - the Security Code. Its adoption was largely a reaction to increased concerns sparked by the 9/11 terror attacks in 2001, exacerbated by the revelation that one of the attackers (Mohammed Atta) was reported to have visited chemical plants before deciding on aviation as the means through which he sought to create fear and terror (Source). Faced with the possibility of a future attack, lawmakers and politicians narrowed in on protecting chemical facilities from becoming a potential target. As former Senator Warren Rudman put it in 2003: "You know, the threat is just staring us in the face. I mean, all you'd have to do is to have a major chemical facility in a major metropolitan area go up and there'd be hell to pay politically. People will say, 'Well, didn't we know that this existed?' Of course, we knew." (Source) The numbers seemed to confirm these fears, as a study the Army Surgeon General from 2002 showed: A single successful terror attack on a chemical facility had the estimated power to put up to 2.4 million people's lives at risk (Source).[3]

Legal and financial incentives

In addition to these societal fears, it was a combination of factors that led to the introduction of the Security Code, including - once again - financial incentives on the part of chemical companies:

- *Reduced legal and financial risk*: New voluntary initiatives were expected to limit producer's exposure to legal liability in the case of a disaster (Source). For instance, the Security Code was recognized as a so-called "Qualified Anti-Terrorism

[3] The events of 9/11 were an important, but not the only factor in bringing about the Security Code. Overall, the early 2000s proved to be a nurturing environment for reform, as this report from 2003 details: "In recent years, several major developments have caused the U.S. chemical industry to examine ways to further improve its EHS and security performance. They include expanded regulation of industry processes and products, which increased the number of public right-to-know initiatives and public reporting of EHS performance; greater external stakeholder participation in government and corporate decision making; the continuing trend of restructuring, merger and acquisition, and globalization of business activities and responsibilities; the emerging development of global management systems and standards for EHS practices; and the recognition that better performance is a key element for improving the reputation of a company as well as the industry." (Source)

Technology", which meant that those who abide by it can not be held liable for losses that occur in the event of an attack.

- *Enhanced protection of their own property*: "Some companies, such as Arch Chemicals, Dow Chemicals, and Eastman Chemicals have all invested sizeable amounts of money into the improvement of technology through high-tech cameras, new fences, better IDs, and more guards" (Source). While this does mitigate against the risk of a terrorist attack, it also serves a company's general interest to protect its most valuable assets.

Monetary incentives notwithstanding, companies were largely successful in branding their efforts as patriotic acts that served to protect the nation, and to present their ability to move faster than regulators could at the time as a main selling point of voluntary initiatives. And so, as early as September 2001, the following steps were taken to introduce the Security Code (Source):

- Development of a member company security network
- Exploring systems for internal information sharing
- Provision of access to government experts
- Formation of new Security Committee
- Development of ACC policy positions
- Coordination of security program implementation
- Approval of new Responsible Care Security Code by Board of Directors

Leading the way

Arguably the most important event in the history of the Security Code is one that is not even directly related to the Security Code itself: The introduction of the Chemical Facility Anti-Terrorism Standards (CFATS). An extended case study of CFATS can be found here. The following passages are largely (and in part verbatim) taken from this case study. CFATS is a regulatory program that is often said to be heavily influenced by and/or modeled after the Responsible Care Security Code.

- In both frameworks, security measures were to be taken commensurate with and in accordance with assessed risk levels. Both frameworks focus on actionable and concrete steps chemical facilities can take to improve security.
- The ACC Security Code first introduced SVAs, a practice (and name) the CFATS program adopted.

- Some recommended measures[4] in the ACC Security Code have large overlap with some of the RBPS described above and detailed in the Appendix.
- Cybersecurity was already mentioned in the early 2002 ACC Security Code, long before it became a key concern.
- The ACC Security Code recommends "Training, Drills and Guidance", at least some of which have been picked up by CFATS.
- The ACC Security Code of 2002 also highlighted the importance of sharing security information with local emergency teams, while also "safeguarding information that would pose a threat in the wrong hands" (Source).
- Periodical re-assessments and audits were a crucial part in the ACC Security Code, which was picked up and replicated with minimal modifications by CFATS
- However, the biggest similarity between the two approaches is to be found in the suggested sequence of events that constitute the regulatory process. The Security Code proposes that in a first step, company activities involving security are to be identified, followed by developing a priority list and designing a "security management program". Next, a detailed plan with a schedule and responsibilities is developed which is finally implemented in the last step. This procedure was later mirrored by CFATS when they proposed a similar sequence of events, even though the terminology was not always identical (a "security management program" might best be translated as an "SSP", etc.).
- In other areas, CFATS departed from the course sketched out by the ACC. The Security Code, for instance, recommended third-party verification, conducted by firefighters, law enforcement officials, insurance auditors, and/or federal or state government officials. CFATS, on the other hand, heavily relies on their own team of CSIs. In other areas, CFATS followed other agencies rather than industry-led efforts, for example when determining which chemicals were to be included in the list of COIs. CFATS - for the most part - simply took these (and the respective quantity thresholds) from EPA's Risk Management Programme.

The last few years have seen only small but regular updates to the Security Code. Most notably, cyber-security threats were highlighted in a 2021 update, emphasising their importance and pointing to their relevance in guaranteeing system security (Source). In 2022, a Management Practice was added ("Crisis Management Planning") on the request of

[4] "At facilities, actions can include measures such as installation of new physical barriers, modified production processes, or materials substitution. In product sales and distribution, actions can include measures such as new procedures to protect Internet commerce or additional screening of transportation providers." (Source)

CHEMTREK, an entity housed under the ACC that focuses on hazmat emergency response issues and strategies (Source).

3. Implementation: Security Code

Since the Security Code provides a framework rather than a concrete set of actions to take for companies, the question of implementation arises. This section attempts to give a brief overview of how the Security Code influences chemical companies procedures in practice.

Firstly, it's important to note that following the rules outlined in the Security Code is mandatory for all members of the ACC (mostly manufacturers) and so-called "Responsible Care partners", which are actors distributed through the entire supply chain.

The first thing to understand about the Security Code is that it is a tier-based classification that assigns different levels of security risk to facilities, which in turn determines the level of preventive and mitigative actions that need to be taken to protect against said risk and which helps companies to prioritise between facilities they operate (Source). In the first step, a "Security Risk Index" (Source) is calculated as a sum of different risk levels across three domains: *Difficulty of Attack*, *Severity of Attack* and *Attractiveness of Target*. Depending on the sum of these assessments, a facility is placed in either Tier 4 (low risk), Tier 3 or 2 (medium risk) or Tier 1 (high risk). An example is shown below.

A qualitative score from 3 through 12 can be produced for each RMP scenario.

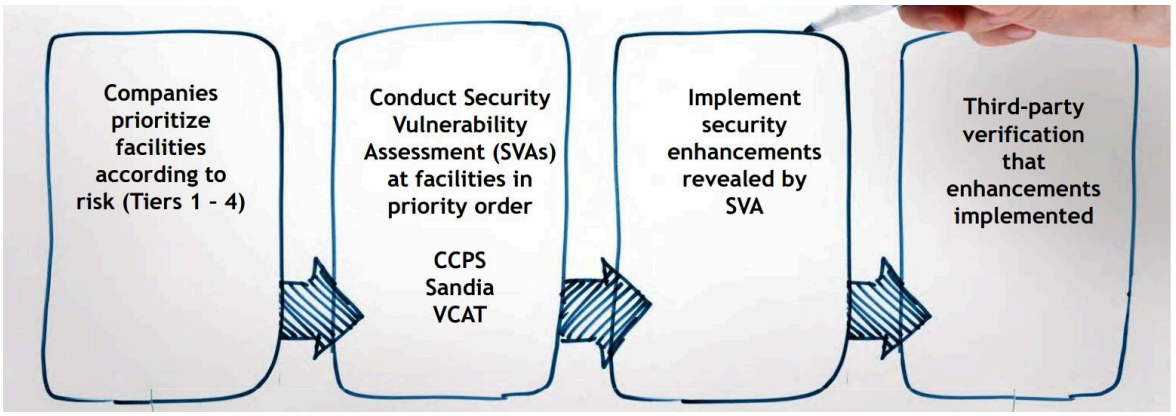
Difficulty of Attack (D)	Severity of Attack (S)	Attractiveness of Target (A)	Security Risk Index (SRI)
1	1	1	3 + 2 + 4 = 9
2	2	2	
3	3	3	
4	4	4	

The highest of the SRI for each RMP process will determine the prioritization tier for the facility.

Security Risk Index									
Tier 4	Tier 3			Tier 2			Tier 1		
3	4	5	6	7	8	9	10	11	12

The facility examined here would be ranked in Tier 2, given its total score of 9.

After having prioritised certain facilities based on this scheme, a so-called Security Vulnerability Assessment (SVA) is conducted for each facility, starting with the one that is highest risk. This SVA serves as an investigation into potential dangers and security threats, based on which specific security enhancements are to be taken. Finally, this implementation is then verified by a third-party auditor (Source). A visualisation helps to illustrate this process:



An implementation guide issued by the ACC summarises this as follows (Source):

- "Identify company activities that currently involve security. Most companies already have security measures in place. Surveying current measures will reveal what has already been instituted and what remains to be done.
- Develop a priority list of activities to be implemented. Some activities are easier, or more important, to implement than others. In setting priorities, take into account such factors as urgency, the need for outside resources, potential exposure, and risk.
- Design a security management program that will implement the Security Code of Management Practices.
- Develop a detailed plan that establishes a schedule, company responsibilities, and resources needed for each activity to be completed. When developing a plan, involve personnel representing various job functions. The plan should be updated on a regular schedule or whenever changes, such as the introduction of a new process, necessitate a review.
- Implement the security improvements. Changes to existing practices are often hard to make. Begin implementing the program in small steps. Build employee trust and involvement by encouraging employee participation during each program step."

Similarly, guidance documents for implementation exists in other parts of the world such as Europe, where cefic (the European equivalent to the ACC) worked with 3 major chemical

companies to publish best practices, including but not limited to the domain of perimeter security, petrol, video surveillance, access control, personnel security and information protection (Source). On top of this, companies can enlist private companies to assist with their implementation of the Security Code and to assure their compliance.

5.1 Enforcement: Responsible Care

Enforcement is one of the elements that have seen most change and development over time. Looking back to how "enforcement" was handled in the 1990s, one can not help but wonder how the proposed system would provide the accountability needed to a) convince the public of their trustworthiness, b) protect against legal liability and c) pre-empt any governmental regulation: "Members conduct self-evaluations annually and rate themselves on a 6-point scale: 1 (no action), 2 (evaluating existing practices), 3 (developing plans), 4 (implementing plans), 5 (management practices in place), and 6 (reassessing management practices)." (Source). It should come as no surprise that this mixture of exclusively self-assessed ratings and the vagueness of their consequences (or lack thereof) did not inspire trust with stakeholders, as this Editorial from 1996 describes: "The Responsible Care program and its goal of improved credibility appears to be seriously impeded by inadequate accountability" (Source). Consequently, the reform period in the early 2000s was used to establish new systems of management to assure compliance, introducing among other measures an independent audit system (Source). In 2003, it was decided that all member companies had to be certified within two years and had to complete the first cycle of facility audits within two years, which was proceeded by additional audit cycles. The ACC also made it very clear that this was not optional: "Failure to successfully complete third-party certification within these time frames will be grounds for a company's removal from ACC" (Source). When these audits were first conducted in 2004, it depended on the company size how many audits a given entity had to undergo: "Larger firms must subject themselves to more inspections. Those that operate 26 to 40 sites must verify at least six. Firms that operate at more than 40 locations have to verify at least eight." (Source) Auditors reviewed the overall security management of a company as well as the on-the-ground implementation in their facilities (Source).

While these changes marked a clear turning point in the history of the Responsible Care program, they did not come out of nowhere. As early as 1996, initiatives such as the "Management Systems Verification" system existed - a mechanism that proposed peer review measures for the implementation of the program (Source). Approximately 60% of member companies participated, given that this initiative was not mandatory for members.

However, the external credibility of these reviews remained limited given there were no third-party auditors, and the results of an MSV were not routinely made public (Source). Even under the new system proposed in 2003, member companies had the privilege to choose their own auditing companies, which further limited external credibility (Source). Unsurprisingly, not a single company was expelled based on non-compliance by the early 2000s (Source)[5]. While widely acknowledged as an improvement, these changes were therefore not able to completely overcome the challenges of a lack of trust from the public and competing companies (Source)[6].

5.2 Cost of (Non-)Compliance

When being presented with a choice to join a voluntary industry initiative (and, subsequently, whether to comply with it or not) or to decide against it, a company has to consider a myriad of factors and possible implications. In this section, we describe a few of these considerations.

One decision-relevant factor is the cost that is associated with measures mandated by the program. For instance, an ACC representative revealed in a senate hearing that "members have invested more than $17 billion under the Security Code to further enhance their security" (Source). Incurring these costs may make a company less able to compete with other companies, especially if these companies do not operate under the same requirements. Hence, we should expect this to be a more relevant factor in markets where fewer companies participate in these programs, whereas once a critical threshold is reached, there might be less fear of being not competitive, while costs (especially of a reputational kind if your company is the only holdout) may rise with increased membership rates.

Nonetheless, the overwhelming majority of chemical companies have decided to join the program absent any mandatory requirement or threat of force to do so, and the ACC openly (and successfully) markets the cost-saving benefits of Responsible Care (Source). Why is that? What does a company stand to gain from signing onto these voluntary initiatives?

---

[5] This, of course, can be seen as either a failure (this program doesn't have "teeth") or a huge success ("everyone is complying so there is no need for punishment") of a mandatory program like Responsible Care.

[6] It should also be noted that it is not clearly established that third-party certification effectively solves the problems outlined above even if implemented at large: A 2019 study found that "there is no statistically discernible effect of third-party certification on facility emissions" (Source).

> "By investing time and money in security efforts, managers can reduce the likelihood of adverse effects on employees, the public, and the environment, as well as help their companies avoid costly losses. In effect, security is a tool for maintaining operations integrity. Even a small incident, such as threatening graffiti by an intruder, can leave employees too distracted to work well and can cost a significant sum to rectify. A large incident, such as a deliberate release of a site's hazardous materials, can injure people, harm the environment, and seriously damage a company by disrupting operations, inviting multi-million-dollar lawsuits, requiring costly remediation, upsetting employees, and injuring the company's reputation. If a risk assessment determines that an access control system and closed-circuit television surveillance are warranted, the cost of those systems is minimal compared to the potential costs from a serious security breach." (Source)

In this statement, the ACC refers to a variety of direct and indirect benefits that can be accrued by members:

- Voluntary industry initiatives often encourage information sharing about best practices, and unlike in other domains where giving up your company's secrets may be seen as a threat or a bad move, in terms of security and safety of facilities, this can be cost-reducing for the large majority of participants of said program.
- Companies often enjoy a counterfactually reduced regulatory burden if the voluntary initiative is perceived as "sufficient" or if a future regulatory effort is modelled after it. If signing onto a voluntary program can lessen or even eliminate the blow that would come from a new and large scale regulatory regime by an invested government, joining the program may well be worth the cost it incurs.
- Participating in a program (and remaining compliant) can work as a boost to a company's reputation. Arguably, this might be less true for chemical companies since they engage less in direct consumer interaction and B2C business, but it still represents one factor that influences a company's success and ability to generate new clients.
- As described above, participating companies can sometimes expect to benefit from reduced premiums for their insurance (see the History section) if they are a member of an association or have signed on to a voluntary initiative. For high-risk sectors of the economy, these reductions can significantly affect the bottom line of a business.
- Insofar as the company is competing with other players for talent and labour, being able to market yourself as a responsible industry leader can help with talent attraction and retention. This would play an outsized role in an industry where

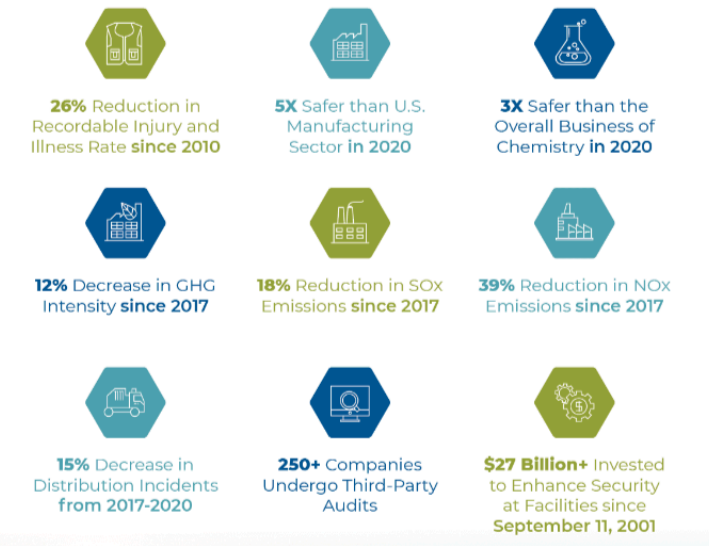
highly-skilled labour is scarce and sought after, where workers have more bargaining power and can choose a company based on ethical considerations.

4. Evaluation

While the overall and long-term impact of voluntary industry programs in the absence of a control group is hard to assess, it still seems important to evaluate the success of a given initiative, since this will allow us to draw inferences on what to replicate and what to avoid in future situations with similar conditions.

5.1 Responsible Care

Unsurprisingly, the American Chemistry Council considers the Responsible Care program unequivocally successful, citing various statistics that show a decrease in injury rates, emissions and incidents overall (Source). The strength of this evidence is difficult to assess, given that we should expect normal technological development to have these effects even in the absence of a voluntary industry initiative. Hence, these numbers should be taken with a grain of salt.



Nonetheless, there is good reason to believe that the program has had an overall positive effect on safety, if only through intermediary effects:

- *Spreading knowledge*. "One of Responsible Care's most important innovations is that it fostered the transfer of technical know-how among chemical companies in reducing their emissions of certain toxic substances. In particular, large companies helped smaller ones in establishing the necessary control systems to reduce emissions, notwithstanding initial unease about the implications for competition. Through this sharing of information and management approaches, the program achieved both greater gains than if each company had worked on its own and a higher level of participation by companies by overcoming concerns that Responsible Care would be too difficult or would cost too much." (Source)

- *Improving corporate and organizational culture* (Source). Another pathway to success is through so-called "normative forces", whereby a standard functions as a tool to establish new industry-wide norms, standards and best practices: "Such new values and norms can be found in the text of the Responsible Care guiding principles and codes of management practices. For example, the codes concerning distribution and product stewardship contain language that suggests that the industry has changed its traditional boundaries from the fence-lines of its plant to the entire life cycle of its products. The code for community awareness and emergency response states in essence that the surrounding community is part of a firm's existence and makes clear the value of incorporating inputs from that community" (Source).
- *Spillover effects*. Programs like Responsible Care have sometimes been observed to have so-called "mimetic forces" - if one company discovers a very cost-effective way to meet a requirement of a standard, it can be shared with other members since incentives to hide their discoveries are low compared to traditional R&D, which helps in alleviating coordination problems. From the beginning, the chemical industry saw this as a chief element of the Responsible Care program (Source).
- *Multiplier effects*. One study found that "previous adoption of the Responsible Care program [...] impacts the decision to adopt a second voluntary program, the international voluntary standard ISO 14001" (Source). Utilised in this fashion, voluntary programs like Responsible Care can kickstart a chain reaction of standard endorsements, contributing to overall improved safety.

In spite of these promising observations, there are also reasons to believe that the Responsible Care Program has not achieved its goal of increasing safety, or worse, has contributed to a decrease in safety standards:

- *Regulatory relief*. Voluntary standards can lead to a decrease in actual regulation, which can have negative effects on safety, as this study indicates: "We find strong evidence of regulatory relief: RC participants experienced fewer and possibly more lenient planned inspections than non-RC participants." (Source) This is not an indictment of the Responsible Care program per sé, since it is possible that fewer or more lenient inspections were the *effect* of a successful implementation of the voluntary standards, but it needs to be considered as a potential side effect.
- *Lack of enforcement and sanctions*. Arguably the Achilles heel of voluntary programs, it has repeatedly been pointed out that "effective industry self-regulation is difficult to maintain without explicit sanctions" (Source). While the expulsion from the association comes with significant cost and can therefore be considered an adequate

sanction, there is very limited evidence of this happening in practice, which could influence companies' assessments of the relevant risk of non-compliance.

- *Reverse effects*. Two studies indicate that participation in the program is actually negatively correlated with achieving the goals connected with it, although no clear causal mechanism could be established:
    - "Our data provide no evidence that Responsible Care has positively influenced the rate of improvement among its members. Indeed, we found evidence that members of Responsible Care are improving their relative environmental performance more slowly than nonmembers" (Source)
    - "We find that on average, plants owned by RC participating firms raise their toxicity-weighted pollution by 15.9% relative to statistically-equivalent plants owned by non-RC participating firms. This estimated increase is large relative to the yearly 4% reduction in pollution among all plants in our sample between 1988 and 2001. Moreover, RC raises plant-level pollution intensity by 15.1%" (Source)

5.2 Security Code

For a variety of reasons, it is significantly more difficult to assess how successful the Security Code. For once, it is a lot "younger" than the Responsible Care program it is part of, and any evaluation of the Responsible Care program post-2001 will include some information about the Security Code, although it is near impossible to untangle this. There is also no "control group" (i.e. companies that partake in Responsible Care but not the Security Code) in the same way that at least somewhat exists for the Responsible Care program. One way to come to a preliminary conclusion about its success might be to look more closely at how it relates to CFATS (see Section 2.3) - the fact that it is widely regarded as its predecessor and has had a major influence on how CFATS was conceived could be seen as weak evidence of its standard-setting powers. At the same time, comparing some best practice recommendations from the Security Code (see for example page 6 of this document) to the actual requirements put forth in the CFATS standards may lead one to believe that it is compromising on safety in the interest of efficiency. Hence, more data is needed to come to a conclusion about the Security Code's success.

5. Lessons for AI standards

- The fast-paced AI landscape requires regulatory programs and standards that have the ability to adapt quickly. A concrete failure mode that became obvious in the case of Responsible Care can originate from a lack of willingness to constantly update and reform standards: "The operating environment for business today changes so fast that 'every 5 to 7 years you need to evaluate the program; otherwise things get too stale,' Roczniak said. In the late 1990s 'ACC let Responsible Care go stale' but after realizing it, the leadership initiated strategic reviews in 2002 and 2009 to map out and address emerging issues for the industry." (Source) The faster the development of the technology that is being regulated, the higher the risk of standards "getting stale".
- AI standards will have to carefully navigate the tradeoff between incrementalism and setting high standards immediately: "The development of Responsible Care typifies the difficult balance that must be achieved by voluntary measures. If standards are set too high initially, industry may be reluctant to participate. Almost all commentators interviewed for this study agreed that peer pressure and culture change require time to evolve. Yet if standards are not rigorous and transparent, the public may criticize the initiative for being ineffective. Proponents of Responsible Care emphasize that the incremental nature of its development contributed significantly to its effectiveness." (Source) Applying this to AI, we may find that insufficient standards in initial stages are less of a concern because the public perception matters less. That said, insufficient standards could exacerbate risk by providing a false sense of security.
- The opportunity to leverage various incentives should be explored at greater depth. Public opinion, effects on talent attraction and retention, legal and financial implications should all be considered as means by which standard-setting procedures can be marketed to companies. For AI, liability for harm caused by advanced AI systems might be a particularly strong lever. Benefits that accrue to a company as a result of their membership need to be communicated clearly.
- Responsible Care was successful because it managed to bring a large majority of companies onboard. Part of this success was made possible by the fact that companies stood to gain something from a mutual change. This may be less true for AI developers and labs where power is currently extremely concentrated. A shift in strategy might therefore be needed, focusing on the few most influential labs rather than wide stakeholder buy-in. Changes in the market landscape should then be

reflected in a changing strategy, e.g. if we see a larger distribution of market share over more companies over time.

- The success of Responsible Care and the Security Code in changing and adapting inspires hope for a world where AI systems are first subjected to fairly weak standards. Lock-in effects seemed to be less of a concern, which could be an argument in favour of pushing for standards sooner, even if the specifics later turn out to be too weak or inadequate for the newest AI models.
- Since a lot of the benefits were of an indirect nature (due to shifts in organisational or corporate culture etc.), it seems crucial to have the voluntary industry efforts be led by a particularly responsible AI lab that can transmit high norms of transparency and a focus on safety to other participants of the same program.

Appendix

A. Security Code ACC (2021 version)

Management Practices	Goal	The organization will...
Leadership and Culture	Senior leadership commits to creating, valuing, and sustaining a strong security culture throughout the organization. Leadership at all levels consistently demonstrates a visible and ongoing commitment and organizational emphasis on fostering continual improvement of security performance across the organization's supply chain.	1.1 Demonstrate the importance of security through words and actions, including an understanding of significant risks and their potential consequences; 1.2 Establish and routinely communicate security performance expectations, including measurable goals, objectives and targets; 1.3 Allocate sufficient resources to meet performance expectations; 1.4 Encourage openness in raising concerns and identifying opportunities for improvement in a secure manner; 1.5 Actively promote a visible culture of security excellence across the organization; and, 1.6 Facilitate collaboration of cybersecurity and physical security functions.
Security Risk Management	Identify, prioritize, and analyze potential security threats, vulnerabilities and consequences using industry recognized techniques and methodologies. An integrated risk management strategy requires an in-depth understanding of the potential interrelated impacts between cyber and physical functions.	2.1 Assess and inventory its key physical and cyber assets; 2.2 Understand the threats and risks to its physical and cyber assets, including operating technology, both separately and together, to support informed decision making; 2.3 Communicate, coordinate, and collaborate to develop a common threat landscape and a unified risk strategy; 2.4 Rank and prioritize security risks using industry based and recognized techniques and methodologies; 2.5 Allocate resources to minimize risk exposure; 2.6 Conduct integrated security vulnerability assessments for industrial and non-industrial sites and key assets; 2.7 Develop processes and programs to secure key assets and the enterprise; and, 2.8 Establish a process to regularly re-assesses security risks, considering the changing threat landscape.
Implementation of security measures	The organization will develop and implement security measures commensurate with identified risks.	3.1 Implement, in a timely manner, policies, procedures, programs and physical and/or technological enhancements as appropriate to address the identified risks; 3.2 Consider leading security practices and the experiences of

		other organizations; 3.3 Address potential risks to business continuity; 3.4 Work with its commercial partners and others in its supply chain to address shared risks; and, 3.5 Align security measures to be compatible with other safety and environmental measures.
Documentation	Documentation of security programs, processes, and procedures.	4.1 Identify and document key elements of its security management system including, but not limited to policies, procedures, and governance for physical, cyber, corporate, and confidential or proprietary business information; 4.2 Maintain documented information on identified security risks and the methodology used to identify them; and, 4.3 Implement measures to secure data and information.
Training and Guidance	Employees, contractors and supply chain partners, as appropriate, are provided with relevant information and made aware of their role in the security management system. Personnel are made aware of security risks associated with their role and the consequences associated with nonconformity.	5.1 Identify and provide training necessary at relevant levels and functions to support the security management system; and, 5.2 Maintain training records per internal document retention requirements.
Security Threat Assessment and Response	Develop, maintain, and continually improve processes to detect, deter, delay, and respond to potential security threats and work to prevent these threats from becoming actual security incidents.	6.1 Evaluating and assessing potential threats and impacts; 6.2 Determining the credibility of the potential threats; 6.3 Activating existing security mitigation/response plans and monitoring developments; and, 6.4 Communicating relevant information to internal and external stakeholders, including law enforcement/government authorities where applicable; 6.5 Initiate existing security mitigation/response plans; 6.6 Take appropriate action, as defined in its existing security mitigation/response plans; and, 6.7 Communicate relevant information to internal and external stakeholders and law enforcement/government authorities where applicable. 6.8 Conduct a post-threat and/or post-incident response review to identify potential causes, learnings, and opportunities for improvement; 6.9 Investigate the cause(s) of system nonconformities and implement necessary corrective actions; 6.10 Implement necessary corrective actions to improve existing security mitigation/response plans; and

		6.11 Share relevant learnings, as appropriate and with appropriate safeguards, to audiences including, but not limited to, law enforcement/government authorities, internal and external stakeholders and/or industry peers.
Crisis Management	Integrate security-related scenarios into crisis/emergency management plans to minimize potential impacts to people, communities, operations, and the environment, as well as potential impacts to suppliers, customers and supply chains.	7.1 Identify reasonably foreseeable scenarios that would activate the organization's crisis/ emergency management plan; 7.2 Determine possible responses to the identified scenarios; 7.3 Define triggers for activation of the crisis/emergency management plan, considering levels of urgency and how to escalate the response if necessary; 7.4 Establish lines of authority and a reporting structure; 7.5 Identify resources needed to support its crisis/emergency management function in the event it is activated; and, 7.6 Plan for both internal and external communications to employees and others working on its behalf, law enforcement/government authorities, members of the public and other key stakeholders.
Verification	Organizations conduct verifications of security management system to assess effectiveness.	8.1 Periodically assess the effectiveness of its security management system; 8.2 Document the assessment method used and the assessment's results; 8.3 Take corrective action as necessary; and 8.4 Maintain records as required by compliance obligations or company policy. Verification may be accomplished through: ● Testing; ● Drills and exercises; ● Auditing; ● External party review; or ● Other means to determine that the security management system meets the organization's security objectives.
Management of Change	The organization manages changes that can impact the effectiveness of its security management system. The management of change process may be specific to the security management system or part of an integrated, organization-wide, multi-discipline approach addressing temporary, limited application, or permanent changes.	Changes the organization will consider include, but are not limited to, those associated with: ● Physical operations; ● Technological, operational, cyber, or other systems; ● Organizational structure, leadership or business-related organization; ● Product or service changes; and, ● Security threats or vulnerabilities identified from audits, inspections, tools, or other sources.

Continual Improvement	The organization conducts reviews of its security management system, including, but not limited to physical, cyber, and operational technology, supply chain and intellectual property protection programs to confirm it is meeting its objectives and/or identifying opportunities for improvement. The review process may result in revisions, changes or redesign of security management system elements as necessary to achieve its security-related objectives and to reflect current internal and external factors affecting the security management system.	Inputs to the organization's review process may include, but are not limited to: ● Results of internal audits, inspections or verification activity; ● Stakeholder inputs and expectations; ● Technological changes; ● Results of management of change reviews; ● Changes to compliance obligations; ● Identified external excellent practices; ● Threats or opportunities to its security profile; ● Results of exercises, drills or technical outputs; and, ● Threat or incident response investigations or after-action reviews.

B. Security Code nefic (Source)

Management Practices	Goal	The organization will...
Leadership Commitment	Senior leadership commitment to continuous improvement through policies, provision of sufficient and qualified resources and established accountability.	1.1. Emphasise security as a fundamental part of the overall management system and/or the Responsible Care program in form of e.g. a written policy or statement to all staff and partners. 1.2. Develop a job description for a person responsible for the company's security program and appoint a person based on the defined needs. 1.3. Define the internal security network and services especially if the company exists of more than one site or facility. 1.4. Take care of the job specific training and qualification for all staff dealing with security. 1.5. Provide the security function with sufficient resources and with direct reporting lines to the management. 1.6. Set and communicate security expectations and goals.
Risk Analysis	Periodical analysis of threats, vulnerabilities, likelihood and consequences using adequate methodologies.	2.1. Assess the most important assets for the company and for each relevant site e.g. research facilities, production plants, headquarters, central computer/computer rooms and infrastructure. Think about the possible impact triggered by theft, loss, damage, disruption, manipulation with malicious intent, rumours or espionage. 2.2. Evaluate the dependence on raw materials, telecommunication (phone, radio and data network), transport and utilities like energy. 2.3. Identify critical chemicals/products and processes whose theft, loss, manipulation or release caused by a malicious act could result in significant impacts for the company or the public e.g. tank farms, dangerous goods loading facilities, high pressure equipment, process control systems. Take into account any relevant assessments that the company has already performed. 2.4. Analyse the essential security threats for the company, the staff, the assets, the products and the knowhow. Know about the motivation and tactics of e.g. thieves, hackers, frustrated employees, organised crime, violent pressure groups, extremists and terrorists. Governmental and local security agencies should be asked to provide initial information and maintain a reporting system. 2.5. Make sure that a security analysis is a fundamental aspect of the overall business continuity planning and decisions on all capital expenditures and investments. 2.6. Determine what is acceptable and what is not
Implementation of Security Measures	Development and implementation of security measures commensurate with the risks.	3.1. Define the goals of a company specific security concept, based on a risk analysis and guided by the principle "Deter, Detect, Delay and Respond". 3.2. Conduct a security survey for the company or the site to assess the already existing security measures. For this purpose build a team consisting of management representatives and experts for security, process safety, infrastructure, IT, emergency response, logistics, human resources, etc. It is important to understand how

		technical, personnel and organisational means of security act together and help to secure other processes e.g. within the supply chain. 3.3. Analyse if there are any gaps between these measures and the risk and the goals defined before. 3.4. Close the gaps by putting additional or modified security measures into place, resulting into a comprehensive plan for site security which should cover all relevant categories. 3.5. Implement the plan and check that scheduled measures have been put in place and are working as desired, especially in case of significant modifications 3.6. Integrate security and information protection needs and requirements into site procedures, contracts and service level agreements, in an appropriate way and whenever necessary
Training, Guidance and Information	Training, guidance for, and information of employees, contractors, service providers and supply chain partners, as appropriate, to enhance security awareness.	4.1. Make sure that staff, contractors, suppliers and service provider are aware of, and respect the company's security rules and procedures. This information should be a fundamental part of the "day one" package for new employees and contactors but also for e.g. visitors, possibly in a shortened version. 4.2. Raise the general awareness for security and information protection by appropriate measures like presentations, workshops, training sessions, posters, flyers and any state of-the-art communication technology or platforms. 4.3. Inform and train staff involved with critical assets or functions in more detail about the particular security and information protection threats caused not only by outsiders but also by insiders.
Communication, Dialogue and Information Exchange	Communications, dialogue and information exchange on appropriate security issues with stakeholders such as employees, contractors, communities, customers, suppliers, service providers and government officials and agencies, balanced with safeguards for sensitive information.	5.1. Establish means of communication, possibly making use of already existing ones within the company - to inform employees, as appropriate, about current security threats and countermeasures, and - to inform management, as appropriate, about lessons learned from security threats, incidents and investigations that have occurred. 5.2. Establish regular information exchange meetings with local/national law enforcement agencies and make sure that they will inform you immediately about upcoming threats. 5.3. Make sure that when there is a change in threat level, site security but also management and other relevant units are informed and will react as required or appropriate. Several threat level systems can exist that may have an impact on the company and these can include national and international systems. 5.4. Build or extend already existing networks within the industry for the exchange of security best practices and other relevant security information.
Response to Security Threats and Incidents	Evaluation, response, reporting and communication of security threats and security incidents, as	6.1. Establish a reporting system for security issues or extend an already existing reporting process 6.2. Evaluate incidents without delay in order to reduce or to limit the impact. 6.3. Establish a Crisis Management/Emergency Response Organisation for handling major security incidents, whereby the use of existing teams is recommended.

	appropriate, and corrective action for security incidents including “near misses”.	6.4. Make sure to be able to rely on local or national law enforcement agencies which provides a 24/7 single point of contact. 6.5. Establish a “lessons-learned culture” for security issues inside the company and with others, as appropriate.
Audits, Verification and Continuous Improvement	The commitment to security calls on companies to seek continuous monitoring of all security processes.	7.1. Integrate security in the “management of change” processes. 7.2. Evaluate on a regular basis the number and severity of reported company internal security incidents and outside security incidents relevant for the chemical industry to keep the security system updated. 7.3. Make sure that the security processes and procedures are reviewed on a regular basis by internal or external experts. 7.4. Integrate security into the regular review system of the company e.g. Responsible Care.