RESILIENCE IN THE COMMERCIAL REAL ESTATE INDUSTRY

PROTECTING VALUE FOR AN UNCERTAIN FUTURE

A BOMA Technical Guidance Note

crci | ZURICH Resilience Solutions GDI AINSWORTH STUDIO INTERSEK+

BOMA Canada HIDI Southern Harbour FUTURE READY UNIVERSITY OF TORONTO BOMA Toronto Inspired **leadership** since 1917

CONTENTS

EXECUTIVE SUMMARY

This document is the second of two Technical Guidance Notes on resilience in the commercial real estate industry. The first, *Designing for a Graceful & Survivable Future*, was published in 2019, by BOMA Toronto to increase awareness of what operational resilience is and means for property owners and managers.

This new document, *Protecting Value for an Uncertain Future*, offers practical guidance for operations managers while connecting the data collection practices for operational management and efficiency with corporate portfolio risk management.

We already collect much of what we need to understand our risk exposures, providing an auditable trail of evidence for routine filings and declarations of how the property portfolio is affected by climate change and other contextual trends. Critically, it allows us to focus on what we can control: our operations.

> *We can know and manage how a failure in the power supply will affect us, and therefore what we must do to ensure that our tenants and we can continue to operate effectively. It is the underlying concept behind operational resilience: safe-to-fail.*

It builds confidence and value in the market, distinguishing properties that can support continued operations over those that fail. When we view our properties through an operational resilience lens, many opportunities present themselves in cost and risk reduction while enhancing operating efficiencies and value.

The guidance is arranged in priority of risk exposure:

Driver 1: Site Selection

Examines the risk exposure inherent in a location and offers the opportunity to avoid and manage most of the risks. For example, this can be by ensuring that anything susceptible to flooding is out of the flood zone. We might even focus on a particular type of tenant operation that isn't catastrophically affected by flooding, or exploit the risk by developing the property to provide a refuge for tenants that need to be in the area but are highly sensitive to flooding.

Driver 2: Planning Envelope

Looks at how the impact of a failure can be managed through the choice of building fabric and arrangement. The need to maintain a comfortable (livable) environment during a power failure is becoming a common requirement in municipal green standards.

Driver 3: Incident Sequencing

Looks at the effects of a failure on your operations and how you can plan for a rapid and stable response and recovery. When failure is due to an area effect, river flooding or ice storm, many of those you'd otherwise depend upon are dealing with their own failures, and may not be able to support you even if you have a prior contract or agreement.

Driver 4: Security Requirements

Explores the need for your systems to be secure and the security measures to be resilient. The need to secure stock and tenant property does not cease with flooding.

Driver 5: Integrated Design

Draws all of these strands together and offers the ability to get ahead of hazard predictions and adapt to the latest threat or compliance requirement. The through-life cost efficiencies far exceed the incremental expenditure of chasing successive compliance requirements, whether forced by legislation or stakeholders.

Ultimately, operational resilience is a question of performance. What performance is expected of you and your properties, and can you meet those expectations during periods of stress and shocks? The world economy is in transition, as are the demands and dynamics of commercial real estate. The recent pandemic has been a catalyst for the changes we are all experiencing. You can allow change and failure to control your operations and value, or you can manage the effects of change and control your value.

FOREWORD

Resilience is defined as "the essential ability of an operation or organization to respond to and absorb the effects of shocks and stresses, and to recover as rapidly as possible to normal capacity and efficiency, ideally returning to normal operation stronger than before." — Operational Resilience, University of Toronto, Centre for Resilience of Critical Infrastructure (CRCI).

Being resilient means staying operational

With the increased frequency and intensity of climate-related events, owners and managers in all asset classes in the commercial real estate (CRE) industry must think about resilience in the context of operational capacity and business continuity. Any event that could render the building inoperable for any period will impede or jeopardize the purpose of that asset. Each building is unique; risk profiles vary depending on operational and locational characteristics and interdependencies with critical infrastructure that connects the asset to the community. The two biggest challenges for building owners looking to improve the resilience of their assets are:

1. How to reasonably quantify the inherent risks; and

2. How to determine where to invest.

Infrastructure alone cannot achieve resilience; resilience requires meticulous planning. A robust process to determine a risk profile requires identifying mitigation measures necessary to implement in order to maximize return on investment and minimize risk. Members of the CRE community have a significant role in learning how to be resilient – through awareness, education and industry transformation.

This guide follows BOMA Toronto's *Resilience in the Commercial Real Estate Industry–Designing for a Graceful & Survivable Future* (TGN I). TGN I was the first step in meeting its ResilientTO objectives. It aimed to highlight the "Triple Bottom Line" benefits of resilience and emphasized the need for the CRE industry to consider resilience as part of its risk mitigation and business continuity strategy.

TGN I introduced the Five Drivers of Resilient Development to a target audience: portfolio managers, risk and sustainability managers, general managers, asset managers and development planners. TGN II, *Resilience in the Commercial Real Estate Industry–Protecting Value for an Uncertain Future* addresses a practical focus into operational levels illustrating how to use these Five Drivers and how these Drivers relate to corporate priorities, a critical step in developing an organization's resilience plan. It includes a solid evidence chain that operations managers can deliver to senior levels of each organization through accurate and timely reporting to support corporate decision-making and materials disclosure.

We are proud to publish this new Guidance Note and extend our profound thanks and gratitude to the University of Toronto's CRCI, Dr. Alexander Hay, and his team of researchers for their continued collaboration and partnership. We also extend a special thanks to two of our member firms, First Capital REIT and GDI/Ainsworth: your participation, contribution and continued involvement played a very significant role in publishing this world-leading research. Lastly, we owe a special thanks to Trisha Miazga of The HIDI Group for distilling the research results into this informative Guidance Note.

We would also like to acknowledge Bala Gnanam and Victoria Papp from the BOMA Canada team for their continued leadership and hard work in the resilience arena.

We are confident that this new Guidance Note will be of value to you as you develop your resilience plan.

ResilientTO

Toronto's resilience strategy sets out a vision, goals and actions to help Toronto survive, adapt and thrive in the face of any challenge, particularly climate change and growing inequities.

The strategy is meant to drive action at the city and from business, academia, non-profit organizations and residents to build a city where everyone can thrive.

Susan M. Allen
President & CEO
BOMA Toronto

Benjamin L. Shinewald
President & CEO
BOMA Canada

BOMA Toronto

Inspired **leadership** since 1917

BOMA Canada

ACKNOWLEDGEMENTS

Disclaimer

While every effort has been made to ensure that the guidance given in this Technical Guidance Note is correct, the views expressed and material provided are based on the writing team's experience and offered in good faith and without prejudice. The guidance is for general consideration and is not intended to be treated as specific advice or BOMA policy. No person should act or refrain from acting in any particular matter without taking appropriate advice before doing so. BOMA and the writing team expressly disclaim any liability in respect of anything done, or not done, in reliance, in whole or in part, on any information in this document.

PREFACE

Our world is changing at an unprecedented pace. Technological change is revolutionizing how we communicate, the way we work and the value of that work. Businesses that once employed hundreds of people spread over various locations can now be more productive with dozens operating out of a single site. This concentration of value significantly increases the consequence of loss in the event of a disaster.

Climate change means the local flood that once disrupted just part of a business can now cause complete interruption and possibly loss of the whole operation. The losses resulting from increasingly frequent and more severe weather events continue to climb.

The challenge that operations managers face is how to protect from the effects of a disaster the property function for tenants: how to preserve the value of the business operation by managing the property that enables it. This is what operational resilience is. It also happens to be the first fiduciary responsibility of directors and officers of any company: to protect against loss.

The challenge is complicated by the fact that the standards, codes and practices that define operations are decades old and based on outdated assumptions about the severity and frequency of extreme weather events, loss exposure and building performance. Therefore, operations managers must interpret what the local threats and hazards mean for the property and its occupants and how to deal with them. Ultimately, it comes down to protecting value for an uncertain future.

This Technical Guidance Note is for CRE operations managers

It provides simple guidance in recognizing and understanding operational risks, treating them and communicating this up the chain in a way that the corporation can interpret and use. There are many resources available to operations managers, and part of this Techinical Guidance Note is about raising awareness of what is possible and how to apply it. There is also a vast array of existing and emerging technology that can help mitigate the impact of an event, facilitate response and accelerate recovery. While many stakeholders have contributed to this publication, this guidance has been kept deliberately generic and non-product-specific.

The guidance presented here focuses on "reasonably foreseeable" impacts. Building on a floodplain means you have a reasonable expectation of being flooded. But for our purposes, the bigger issue is building function. We simply intend to draw your attention to risk considerations that have long been assumed in standard practices, but in today's more volatile environment need a reassurance confirmation.

Why Are There No Ratings?

Since only a property's owner or manager-design team can define their specific resilience objectives and parameters, it would be meaningless to compare the resilience rating of one property with another; each has a different risk context as well as different occupants and operations. Instead, this document is about helping you reduce the consequences of an incident and enabling rapid response and recovery within market and operational tolerances.

The CRCI's definition of operational resilience
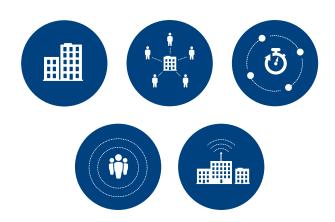
It is the essential ability of an operation to respond to and absorb the effects of shocks and stresses and to recover as rapidly as possible normal capacity and efficiency.[1]

Some basic things about operational resilience to consider from the outset:

1. Most operational resilience measures are either cost-neutral or within the cost of sustainability measures.

2. We measure operational resilience by performance and capability.

3. Inanimate objects cannot be resilient, only robust. Operational resilience is the characteristic of a system to absorb, adapt, respond and recover. For example, when bricks and mortar can self-repair, they can be considered resilient. However, bricks and mortar are components in the system that is a commercial real estate operations.

4. Resilience is not sustainability. We can regard them as two faces of the same coin. Neither gives rise to the other, but cannot exist without the other.

5. A business can be resilient, but it is no longer in business if it ceases to operate. Operational resilience enables corporate resilience.

6. When an operation (or business) is resilient, it actively contributes to, and influences, the resilience of its neighbours and the surrounding community.

What you will get out of this document

You will learn about the Five Drivers of Resilient Development, how to use them in practice, how they relate to the corporate leadership's priorities and reporting obligations, and what resources are available to you.

[1] https://crci.utoronto.ca/about/faqs

CONTEXT

The requirement for resilience is not something new. It has always been a corporate necessity but largely taken care of through codes and regulations. Confident that the future would be similar to the past, property developers and planners knew how much risk could be accepted. Familiarity with these simplified investment metrics allowed new developments to encroach gradually on areas traditionally seen as riskier.

The whole risk exposure changed as extreme weather events started becoming consistently more severe and frequent. One can see a wide range of risk reports and economic assessments by national governments and institutions on what these changes mean and what needs to be done from as early as the 1990s. By 2010, climate change was no longer just a government issue.

As the financial risks became increasingly apparent, regulators started to take action:

- The Task Force on Climate-Related Financial Disclosures (TCFD) conducted the first financial investigation into how corporations should approach the issue, and provided a simple framework for identifying and addressing the risks arising from climate change and reporting on them

- Various securities exchange commissions issued instructions and guidance to their members on material disclosure

- Governments continue to develop legislation, acutely aware of the socioeconomic exposure if pension funds and other institutional investors lose value on their portfolios

The result is an increasingly complex web of regulation, guidance and procedure with which businesses should comply. It has not been easy, and it isn't getting any simpler. Why is this important for the operations managers of commercial real estate?

The simple truth is that it doesn't matter how compliant the business is; if it stops viable operations, it ceases to be in business. It means that corporate resilience depends upon operational resilience, but the two need to be aligned if the corporation is to be truly compliant.

The challenge that operations managers face is that each operation, property, location and tenant is different. So, while we can template much of the corporate resilience practice, we can't do the same for operational resilience.

On the other hand, the corporation is obliged to comply with several measures and reporting criteria that provide clear guidelines and limitations for operations managers in reviewing the operational resilience of their properties. It is worth a brief exploration of these corporate obligations.

Task Force on Climate-Related Financial Disclosures (TCFD)

The TCFD was assembled to investigate how businesses should disclose climate-related financial risks and opportunities within the context of their existing disclosure requirements. Its premise is that through increasing transparency of risk reporting, markets become more efficient and economies become more stable and resilient, and its recommendations were presented December 14, 2016.[2] Set within the risk context of global warming, the approach taken by the TCFD was to focus on making the business issues accessible to managers by measuring them. The aim being that it would lead to the "smarter, more efficient allocation of capital, and speed the transition to a low-carbon economy." It remains quite a visionary document, connecting the long-term future to today's risks and behaviours and the transition to a low-carbon economy.

The core recommendation was to include climate-related financial disclosures as part of directors' annual reports to shareholders and other routine filings. It takes the form of four elements:

1. **Governance**
   How the organization reviews and makes decisions on climate-related risks and opportunities.

2. **Strategy**
   The actual and potential impacts of climate-related risks and opportunities on the organization's businesses, strategy and financial planning.

3. **Risk Management**
   The processes used by the organization to identify, assess and manage climate-related risks.

4. **Metrics & Targets**
   The management and assessment of relevant climate-related risks and opportunities are informed.

[2] Recommendations of the Task Force on Climate-related Financial Disclosures dated December 14, 2016.

The best way to approach this is to compare the existing risk profile with those under different climate change scenarios, and the report suggests using a 2°C rise in global temperature as the first scenario. Material disclosure of climate change-related risks centres on knowing what a 2°C rise in global temperature means for operations, arising from both the stress of change and the shock of extreme events.

Securities Exchange Commissions (SEC)

It is impossible to generalize the SEC requirements because each commission has approached this matter in subtly different ways, whether through mandated metrics, guidelines, procedures or regulations. What is common to all is their concern that potential investors in a corporation's stocks are fully aware of the corporation's risks and how it is dealing with them.

The Canadian Securities Administrators, in CSA-Staff Notice 51-333, guides our consideration of climate change, including the risk of litigation, risk of future regulation, reputation risk, risk to future markets and disclosure of changing market demand, and risk to development. Though these considerations are indistinct, disclosures require supporting risk assessments with evidence-based criteria and studies. It is perhaps unsurprising that few companies had submitted substantive disclosures of their risk exposure to the effects of climate change until recently. The response has been a steady increase in demands from both SECs and shareholder groups to more conscientiously disclose risk exposures.

> *When we could be reasonably confident that the future would be much as the past, these material disclosures could focus on current and immediate future issues with some discussion about strategic risks. That is no longer the case.*

Corporations with an extensive portfolio of industrial and commercial properties and land are urged to look at the portfolio value over its life. That can be challenging because the risks to real property are something operational managers are best-placed to inform. Communication between the corporate head office and the operations manager does not always use the same frame of reference or language. Where the corporate office uses compliance, the operations manager works with performance and capability.

Several compliance/reporting systems are in common use, most notably GRESB[3] and CDB[4]. As with all such reporting formats, they require evidence to have real value to inform decision-making and risk treatment. Too often, reporting can draw on assumptions and opinions in the absence of ground truth operational evidence. When risk reporting does not use evidence, objectively interpreted, we often see optimism bias[5] entering the assessment, skewing both the final reported assessment and internal risk management/prioritization processes.

Institutional Investors

The institutional investors in CRE are mainly the pension funds as the largest real property investors in the GTA and Canada. The general trend in financial asset management is to look forward in terms of risks to portfolio value, instead of projects based on historical data. The JGPIF[6] is currently leading institutional investors in demanding evidence of due consideration of climate change effects. As a result, more investors see climate change risks as normal and afford them due consideration within their fiduciary responsibilities and the push towards low carbon. This trend in investor policies incorporates the UN's Principles of Responsible Investment (PRI). PRI comprises six basic principles:

1. Incorporate Environment, Social & Governance (ESG)[7] principles;
2. Be actively engaged as owners/shareholders;
3. Seek appropriate disclosure;
4. Promote appropriate ESG disclosure;
5. Cooperate in the implementation of ESG;
6. Promote adherence to reporting in the market.

Once again, the challenge for those wishing to attract ethical and sustainability investors is to be able to provide the evidence that supports the disclosure of risks. In the absence of suitable evidence, the default will tend to continue past practice, though this is becoming less supportable. Of particular note is that the Pension Benefits Act (Ontario) requires pension funds to say how they are incorporating ESG in their investment plans.

---

[3] 2019 GRESB Resilience Module Assessment Document. https://documents.gresb.com/generated_files/survey_modules/2019/resilience/assessment/complete.html

[4] CDP Climate Change 2019 Reporting Guidance. www.cdp.net

[5] Optimism bias simply means emphasizing the benefits while down-playing the problems associated with an assessment or proposal.

[6] Operating through external asset management institutions JGPIF (Japanese General Pension Investment Fund) is the largest retirement savings fund in the world and a leading proponent of Stewardship Principles.

[7] Environment, Social and Governance are the categories of assessment criteria used to assess the sustainability and ethical impact of an investment, used by the growing number of "sustainability investors." These criteria are oriented towards the better determination of a corporation's financial performance, in terms of risk and return. A core feature of sustainability investing is whether the investment will have value in the future, rather than just the projected return at the time of investment. ESG has largely replaced Corporate Social Responsibility (CSR) reporting.

UNDRR (formerly UNISDR)

UNDRR/UNISDR is the UN Office for Disaster Risk Reduction (DRR). In 2013, UNISDR expressly linked resilience to sustainability.[8] Since then, resilience has become a core consideration for DRR. Of particular concern is that the increasing losses to catastrophic events will soon exceed the capacity of reinsurers and governments to compensate and the wider harm to economies. This rising concern culminated in an international agreement in 2015 called the Sendai Framework for Disaster Risk Reduction.[9] Most countries, including Canada, signed up to the framework and it is adopted by most international and institutional lenders, insurers and investors.

> *Under the uncertain and extreme effects of climate change, economic sustainability requires industry and governments to take individual responsibility for their loss exposures. More particularly, the owners of a business understand best how that business is affected by failures in systems upon which it relies and can, therefore, treat the risks. In effect, businesses should focus more on actively addressing their risks rather than assuming they can transfer the risks through contracts and insurance.*

When organizations are comfortable functioning in a particular way, it isn't always that simple to change practice. Recognizing this, UNDRR established an industry outreach in each country, known as ARISE, to facilitate the implementation of the Sendai Framework. The mandate for these voluntary industry groups is to find workable solutions to the challenge of being more resilient. This challenge is particularly acute because many organizations interpret resilience differently, based on their perspective. ARISE Canada collaborated with BOMA Canada to develop a Balanced Scorecard-type approach to resilience measurement and, therefore, management. This approach affords a practical top-down assessment of resilience but still requires the operational evidence base to inform it.

---

[8] UNISDR Towards the Post-2015 Framework for Disaster Risk Reduction dated 13 November 2013.

[9] The Sendai Framework for Disaster Risk Reduction 2015-2030 is the successor to the Hyogo Framework for Action (HFA) 2005-2015: Building the Resilience of Nations and Communities to Disasters. The Sendai Framework sets four priorities, which have been incorporated into national and commercial guidance, including this TGN. (1) *Understanding disaster risk* with the important understanding that risk depends on events, exposure and vulnerability; (2) *Strengthening disaster risk governance to manage disaster risk;* (3) Investing in disaster risk reduction for resilience; and (4) *Enhancing disaster preparedness for effective response and to Build Back Better in recovery, rehabilitation and reconstruction*.

Some organizations address climate change through integrated/intelligent risk management structures, including balanced scorecards, typically assigning the responsibility to a vice president of operations. In the absence of a coherent evidence-gathering, analysis and interpreting mechanism, this approach can give the illusion that the organization is addressing its climate change risks, inferring operational resilience. While reflecting a simple optimism bias, it can lead to incorrect climate risk deductions. Quality of operations reporting and interpretation is key to addressing this. It also emphasizes the need to plan for emergencies.

An Emergency Response Plan (ERP) is a vital tool to help reduce the impact of damage of a natural hazard to your property, business and employees. ERPs detail the actions to consider before, during and after a natural hazard event to help reduce damage, restore operations and protect lives. They are also variously known (with some minor adjustments) as an Incident Response Plan or Emergency Action Plan. There can be various phases incorporated into an ERP, including: (1) Strategy Phase, (2) Preparation Phase/s, (3) Response Phase and (4) Recovery Phase.[10]

UN Sustainable Development Goals (SDG)

The SDGs are 17 development goals ranging from gender equality and the eradication of poverty to climate action.[11] The SDGs seek to establish a better and more sustainable world by addressing the core challenges we face as a planet. They are quite simply an articulation of what is right. Multilateral development banks and other institutional lenders adopted the SDGs as criteria against which to assess the value of a proposed development project or investment. Operational resilience enables–directly and indirectly–more than half the goals. The operational resilience of the CRE sector, together with that of the municipal corporation and community housing, is critical to enabling community resilience.

Compliance & Synthesis

Separate from the risk management and reporting requirements on corporations and their effect upon operations, there is a suite of local by-laws to comply with. With the Toronto Green Standard and the Zero Emissions Building Framework in particular, operations managers have a regulatory obligation that actively helps manage operational resilience. One can see it as a compliance issue, or one can see it as an advantage. The fact is that we can typically achieve resilience measures within the costs of by-law compliance. It is just a question of coordination and integrated design, based on an understanding of the operational risk profile of the property.

---

[10] Zurich Insurance Company Ltd's Risk Insights (May 2019) *Events are natural, disasters are not: How lessons learned from previous events can help businesses to become more resilient may be a useful reference.*

[11] https://www.un.org/sustainabledevelopment/sustainable-development-goals/

Putting It Together

As we draw all of these strands together, we see clear connections to each of the Five Drivers of Resilient Development discussed in this TGN. Indeed, the Drivers were devised so that there would be a clear flow of logic from operational resilience to corporate resilience, from measurement to active management. The aim is that while the language and terminology used may change at each level of reporting, the frame of reference and the message remain consistent. As with so much else in large organizations, a common frame of reference allows improved communication and understanding within the existing culture.

> *When we view operational resilience in this context, we get a sense of the true value of each Driver. We see that the Drivers support operational resilience and, by extension, corporate and community resilience.*

It is worth considering what an audit or post-incident review will conclude if we do not implement reasonable risk treatments. It raises the question of what is reasonably foreseeable and underpins material reporting. Writing in the January/ February 2013, edition of Engineering Dimensions, Patricia Koval LLP, a partner at Torys, said, *"In other words, liability might arise where a design professional complies with the minimum standards set out in laws, codes and standards, but these standards fall below those of 'a reasonable person' in the legal sense."*

Simply adhering to the code or standards is not enough. What we consider reasonable is situation-specific: if your power supply comes from a substation located in a flood plain, it's reasonable to assume you will lose power when the substation floods, even if you, yourself, are not flooded. It's reasonable to think beyond direct effects in the building space to the services upon which we rely.

Each organization will have its risk criteria, establishing thresholds for acceptance of risk and what it entails. We cannot know how likely an extreme weather event may be. However, we can know how we are affected by the loss of a particular function or service our operations rely on. We can control how we are affected by extreme events because we understand our operations, measure the consequence of a failure, and so can manage how the effects of the failure propagate through our operations and business.

THE FIVE DRIVERS OF RESILIENT DEVELOPMENT: A REFRESHER

Driver 1: Site Selection

Loss exposure is the most fundamental requirement for a risk to exist. It doesn't matter what the threat is or how much the loss will cost the business; there is no risk where there is no exposure. When there is exposure, we must understand what that exposure means to the property and the operations conducted in and around it. We are then able to treat the risks and minimize business loss.

In the same way that location drives the market value of the property, it is the single most significant factor in the risks that a property faces. Where there is a risk of flooding, for example, it can cause direct losses of property, such as archives and switchgear in the basement, and indirect losses by interrupting electricity supply and accessibility for occupants and service contractors. Recognizing the loss exposure is the basis for all Risk & Resilience reporting. Understanding and managing site selection/Location Risk Assessment (LRA) is the principal part of evidential risk reporting.

Driver 2: Planning Envelope

The inherent ability of the property to continue performing during and immediately following an incident determines the time we have available to respond and recover. In residential properties, the need for residents to survive when heating is interrupted mid-winter limits the time available to restore heating. Maintaining service during an interruption in supply influences the rentable value of the property to its residents. Each resident will have a different tolerance of service interruption. Together, though, it is a market goodwill implication of risk that influences profitability and hence return on investment; it is relevant to financial disclosures.

The Toronto Green Standard and Zero Emissions Building Framework, for example, set guidelines to manage overall energy consumption and greenhouse gases (GHGs) using comfort levels. They also enable occupants to shelter-in-place, allowing the city to prioritize resources on recovery. The ability of building occupants to shelter-in-place during an emergency supports community resilience. The planning envelope is relevant to TCFD, UNISDR/DRR and SDG reporting, by-law compliance and a contribution to the corporate ESG profile.

Driver 3: Incident Sequencing

How you manage the incident relates directly to occupant resilience effectiveness and confidence. Based on the time tolerances and mix of essential functions within the property, you will need to re-position different assets and capabilities in and around the property, prepare standby systems and have the necessary resources and plans for a timely and effective response to the incident. This is about the active management of risk and is relevant to both TCFD reporting and DRR capabilities. In addition, it directly informs your ERP development.

Driver 4: Security Requirements

Often, security is imposed upon a completed design or operation. Weaving it into the fabric of the design and layout of the operation delivers effective and efficient security–as long as no measure impedes the effectiveness of another or the efficiency of the operation as a whole. Security should enhance and not hinder the very operation that it seeks to secure. The principle applies equally to all the systems that the operation depends upon. It also means that if a resilient operation is to be secure, its security systems need to be resilient.

Driver 5: Integrated Design

Integrated Design is a collaborative design delivery model focused on the building and the site as a whole. It breaks down the silos of responsibility, requiring close collaboration and cooperation between all stakeholders, and aligning their success with overall project success. In unifying effort around a common focus, we can realize clearly defined environmental and economic goals and deliver resilience and security requirements throughout the project life cycle without unnecessarily increasing complexity or cost. It is generally proven to produce better overall results and through-life value of properties.

FRAMEWORK

The resilience planning process is a novel way of understanding facility capability and value compared to conventional analysis. The following guide illustrates how the Five Drivers of Resilient Development–Site Selection, Planning Envelope, Incident Sequencing, Security Requirements and Integrated Design–improve resilience within CRE and how improved resilience can add value for the owner/operator.

Stated simply, a comprehensive resilience plan requires analysis and understanding of:

1. The risk inherent to the site;

2. The infrastructure needs of the tenants, compared with the capacity of the facility and supporting infrastructure;

3. The tolerances to shock/stress of the tenant operations, compared with the response and recovery capabilities of the facility;

4. The residual vulnerabilities that need to be secured; and

5. The assurance that shock/stress scenarios will play out as required.

Integrating the Drivers for Greater Impact

You will notice cross-references between the Drivers throughout this document. While applying the Drivers that most closely align with the current facility or project phase will have an impact, we encourage you to read the whole document to understand how the Drivers work together. They can build on each other, and when pursued in sequence will provide a harmonized and significantly more reliable capability.

Each of these concepts has value individually. While the comprehensive plan will provide the most value, each Driver can be completed on its own to advance resilience in your project or organization.

As every context is unique, a prescriptive approach is inappropriate. The goal is to guide your understanding of the principles behind the Drivers, so you can tailor the scope and output of each to suit your situation or application.

References to publicly available sources of information are provided throughout, where we believe they will be useful. We have indicated where certain concepts require the knowledge of subject matter experts within or outside of your organization, like facility engineers/operators, architects, utility providers or insurers.

Consider bringing in risk engineers to assist; the insurance industry can provide more than just insurance advice. As the Zurich Flood Resilience Alliance puts it:

> *"Floods affect more people globally than any other type of natural hazard and cause some of the largest economic, social and humanitarian losses. There is a growing natural hazards protection gap between total economic losses and the insured proportion of those losses that highlights this problem needs to be tackled both by traditional risk transfer mechanisms such as insurance, and by leveraging the insurance industry's knowledge on risk management and risk reduction."*

As is so often, the help you may need is available. The trick is always recognizing what support to ask for and where to find it.

The outputs of each Driver are format-agnostic and will depend on the needs and perspective of the user group conducting the analysis. Where it does involve documentation, the documentation produced will often fulfill the reporting requirements of various sustainability and risk management initiatives. We have indicated this as a *synergy* in the framework below.

Framework for guidance implementation

DRIVER	PROCESS	OUTCOMES		SYNERGIES
		Investment Perspective	*Operations Perspective*	
1 Site Selection	Context analysis, All-hazards analysis, Risk assessment	Inherent site risks for investment decision-making	Design criteria for climate risk and existing building commissioning	TCFD[12] LEED UNDRR
2 Planning Envelope	Dependency mapping, Essential load demand	Infrastructure requirements of the essential functions and tenants	Infrastructure capabilities of the facility	TGS[13] UNDRR[14] UNSDG Utilities
3 Incident Sequencing	Determine Planning Points	Performance requirements, commissioning criteria	Scenario planning, mitigation strategies, commissioning criteria	TGS CDP GREBS
4 Security Requirements	Dependency mapping, Gap analysis	Remaining vulnerabilities, risk-mitigation strategy	Remaining vulnerabilities, risk-mitigation strategy	UNDRR
5 Integrated Design	Full stakeholder involvement	Safe-to-fail design, commissioning criteria	Safe-to-fail design, commissioning criteria	IgCC[15] LEED

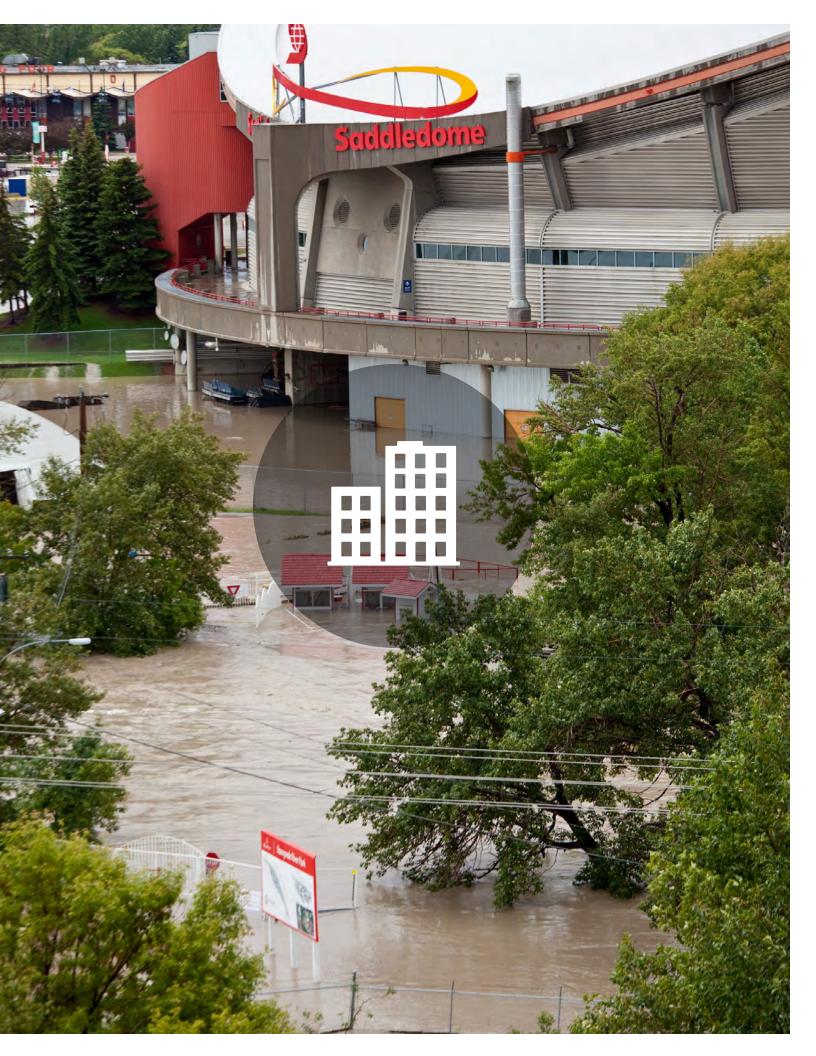[12] Task Force on Climate-related Financial Disclosure.

[13] Toronto Green Standard.

[14] UN Office for Disaster Risk Reduction.

[15] International Green Construction Code.

DRIVER 1:

SITE SELECTION

DRIVER 1:
SITE SELECTION

Objective

Incorporate location-based hazards and reasonably foreseeable consequences into the site selection process and investment decision criteria.

Explanation

The location of a site is the single most significant determinant of its risk profile. Therefore, the most important thing we can do to improve resilience is to understand the risk exposure inherent to the location. The simplest way to mitigate a particular risk is to avoid exposure to it in the first place, which is why location-based risk is best assessed during the site selection process to guide the decision to invest. Then, investigate all hazards in parallel and determine their impacts on the site and the servicing infrastructure. This process allows us to understand which risks we can accept or easily manage and which we must transfer or avoid.

Location, while fixed in space, exists within a dynamic socioeconomic context. Various disclosure frameworks recognize this–both the TCFD and the GRESB Resilience Module address changing social risk and stakeholder impacts, in addition to changing physical risk. The climate is also changing and impacts the hazard landscape in different ways from one region to the next. A systematic analysis of a site across many contexts and over time is a critical step in understanding a facility's risk exposure.

We will first introduce the concepts of context and hazard and the relationships between them. We will then illustrate the process of conducting a Location Risk Assessment (LRA), determining what details are useful, and documenting them so they can be useful throughout the life of the asset.

Guidance

Understanding hazards

Natural hazards are recurring; recurring events are foreseeable. The ice storm that crippled Atlanta in 2014, was preceded 41 years earlier by one that knocked out power for up to seven days. The Sanriku region of Japan, which experienced a tsunami and correlated nuclear meltdown in 2011, had experienced three equally destructive tsunamis in the 155 years prior. The 2013 Calgary flood, which cost more in insurable losses than Hurricane Katrina, was preceded by a similar event in 2005.

> *The events have not changed; it is the frequency and severity of the events that has. When we understand what this means, we can and must plan accordingly.*[16]

While the magnitude and frequency of hazards may evolve, the hazard landscape itself remains fairly constant. For example, we know we don't have to worry about a polar vortex in Miami, nor hurricanes in Calgary. Climate change is a special case of evolving hazard, and we discuss this in some depth below.

Accidental (or technological) hazards are also foreseeable to a certain extent. Toronto suffers over 1,000 water main breaks each year, most of these during winter. As many as 30 ruptures can occur on the same frigid morning. An ammonia or chlorine spill is possible where such chemicals are produced, transported, or stored in bulk. A site near a freight transport route, water treatment plant or refrigerated storage warehouse will be exposed to this risk, while sites further removed will not.

Malicious or deliberate hazards (often termed threats) are impossible to predict, per se, but there are clear trends concerning target selection. For example, transit facilities, mass gatherings and places of worship are attractive targets to single-issue extremists, while organized protest groups frequent legislative facilities. Proximity to such sites can be a greater risk because more traditional target sites prepare for these threats.

Burglary, theft, sabotage, vandalism, terrorism, malicious surveillance and trespassing are all examples of malicious or deliberate hazards. While we tend to use security measures to mitigate them, as we will see in our discussion of Driver 4: Security Requirements, we can often accomplish the same risk reduction using alternative measures. Where security is part of the design strategy, we must carefully integrate it to avoid aggravating the impacts of other hazards.

---

[16] The Zurich Insurance Company Ltd Post-Event Review Capability (PERC) report with the Institute for Catastrophic Loss Reduction (ICLR) *Fort McMurray Wildfire: Learning from Canada's costliest disaster dated September 2019: The number and impacts of disasters are increasing around the world. Effective governance must address the fundamental issues of disaster risk reduction. The likelihood of severe alterations in the normal functioning of a community or society due to hazard events interacting with vulnerable social conditions, depends on three issues: the nature and severity of an impacting event, such as a wildfire, flood, typhoon, or earthquake; the exposure of the community or society to the event; and their vulnerability, the predisposition to be adversely affected.*

Note that hazards can manifest similarly across multiple hazard categories–an errant vehicle, due to inclement weather or a drunk driver, can look similar to a hostile vehicle, in which a driver uses the vehicle as a weapon to kill pedestrians or as a ram to breach a perimeter.

The street flooding from a ruptured water main can look very similar to urban flooding from extreme rainfall. Mitigation can often be largely the same measures but critical coordination is required in their implementation. An all-hazards approach to this study allows us to address multiple hazards with a single efficient solution.

Some hazards tend to occur in tandem: storm surge often accompanies a hurricane; low temperatures accompany a blizzard. We must consider these together, as recovery from a blizzard-initiated power outage will look much different than a power outage due to flooding occurring in the middle of July.

Other hazards are correlated, one causing the other–consider an earthquake causing a gas leak, or a cold snap causing a water main break. We must consider these hazards together, as the incident leading to the secondary hazard will often affect the magnitude of that hazard as well as the capability to respond. Due to the causal relationship, there may be opportunities to interrupt the development of the secondary hazard. For example, a means of shutting off the gas before the line breaks, or ensuring water is not standing when the temperature falls below a designated point.

An aggravating hazard worsens or escalates the impact of another hazard that would otherwise be insignificant or managed in isolation. For example, consider a thunderstorm with typical precipitation and high winds. Wind-borne debris or dislodged rooftop equipment breaching the building envelope can quickly turn a fairly normal rain event into an emergency.

The mere knowledge of a hazard's existence is itself not particularly useful. Once identified, its magnitude at the subject site must be determined. When we understand how bad it can get, we can mitigate the impact accordingly. How close to the subject site is the access road to the water treatment plant, when do they receive chemical deliveries and how much is stored onsite? From which direction are the prevailing winds? How long was the latest heatwave and how hot did it get? How high will the storm surges be in 15 years as sea levels rise? This level of detail requires slightly more research but is generally publicly available.[17]

[17] Reference national, provincial and local studies, i.e. Toronto climate change drivers, Vancouver seismic/tsunami map, Calgary flood risk maps.

Climate risk

During the 2010-2011 winter, nearly 400 roofs across New York and New England partially or fully collapsed due to a moderate snowstorm. A study determined that much of the cause for these failures was the fact that pre-1975 roof design was not subject to snow loads defined in a building code. A rash of roof failures occurred again in 2015, when a Boston blizzard exceeded the regulatory snow loads. Newer structures fared well, but older roofs only survived due to luck or more robust, forward-looking design, perhaps a combination of both.

A recent granular climate forecast prepared for Toronto indicates that in 30 to 40 years, we could see changes in average and extreme weather patterns that would effectively change the city's design climate zone. One study indicated that by 2050, Toronto will feel like Washington, D.C., with temperature increases of up to 5.9°C during summer months, resulting in a 3°C annual mean temperature increase.[18]

> *Another 30-year climate change impact study commissioned by the City of Toronto predicts a mean annual increase of 4.4°C, a 60% increase in the number of humidex days and a maximum humidex value increase from 48°C to 57°C.[19]*

Until recently, we have designed our buildings as though energy and water were cheap and infinite, our mechanical climate control would never fail us and the hazards we face would remain predictable in magnitude and impact. But our world is changing–we can no longer rely on our old assumptions. Predictions and indicators are now hinting at what is coming, and some buildings will undoubtedly fare better than others in this uncertain future.

The site selection process should remain forward-looking to assure continued asset value. Existing facility condition assessments should be assessed not just for their performance and maintenance status. Existing facility commissioning studies typically look at historical performance and existing conditions–we can add additional value to this process by also procuring an energy model to estimate how our mechanical loads will change over time.

[18] Interactive map, ETH Zurich/Crowther Lab, https://crowtherlab.pageflow.io/cities-of-the-future-visualizing-climate-change-to-inspire-action#213121

[19] Toronto's Future Weather & Climate Driver Study: Outcomes Report, SENES Consultants Ltd, October 30, 2012; https://www.toronto.ca/wp-content/uploads/2018/04/982c-Torontos-Future-Weather-and-Climate-Drivers-Study-2012.pdf

Understanding context

The context of a site includes all aspects of its environment, including physical, economic, social, political, network/infrastructure and legal/regulatory. A traditional location assessment for new development or property acquisition will often focus on the economic, social and regulatory contexts in determining the property's value. An engineering feasibility study for such a project will focus on published design criteria for the location and site-specific criteria typically limited to within the property line. Taking a closer look at the context in a structured way can uncover "hidden" risk factors and add significant value to the location risk assessment process.

- **The physical context**
  Includes the ground and soil, water table, vegetation, climate, meteorological averages and minimums/maximums and sun intensity. Much of the physical context is subject to climate change, and many of these factors can impact the suitability of design or mitigation decisions. For example, a high water table can impact rising bollards and other active vehicle-control measures and increase the risk of basement flooding if sump pumps fail for any reason. High winds and fine dust can cause extreme maintenance issues for hydraulic equipment and CCTV cameras.

- **The socioeconomic context**
  Involves the social, economic, cultural and criminal characteristics of the neighbours, vicinity, city and region. Neighbouring residents or tenants who are themselves unprepared for an extreme weather event may look to the subject facility for water or electricity, presenting a security challenge where one did not previously exist. We address this further in Driver 4: Security Requirements.

- **The regulatory context**
  Involves the permissible uses (zoning) and code constraints for the subject site and neighbourhood facilities. For example, an adjacent site zoned for mid- or high-rise construction could impact future solar capacity. Similarly, we would expect an adjacent building constructed before modern seismic code requirements to behave significantly worse than current construction. A seismic event would present a debris, gas or water hazard that affects our property.
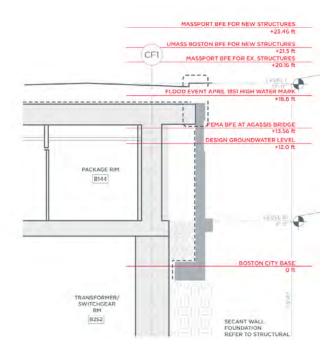
- **The network/infrastructure context**
  Involves services that our site relies upon and its connectivity to the wider region. What is the source of our site's power supply? What about potable water and communications or natural gas? How will goods and services reach the site? How will tenants reach the site – via private vehicle, public transit, on foot? Understanding how the hazards will impact the provision of utilities and services is one of the most critical and useful products of the LRA.

Hazard and context analysis

Conventional risk assessments and feasibility studies are often limited to the project site and will miss critical hazards and dependencies. We begin at the project site and expand our area of observation as wide as required to capture hazard approaches and critical dependencies.

We start with the physical geography of the site. We note that the water table is quite shallow. Cascading impacts are those impacts that, in turn, cause other impacts, such as loss of power to sump pumps, which may lead to flooding of basements, which may then lead to the destruction of elevator equipment and other infrastructure below grade. We note this condition here, and we can take steps to interrupt the cascading impact in Driver 3: Incident Sequencing and Driver 4: Security Requirements.

Markups indicating regulatory flood plain compared to other findings for a structure in the City of Boston, MA.

We note that this could impact basement drainage and dewatering. We check the local flood maps and are relieved to see that our subject site is not in a designated flood plain. However, when we review the accompanying studies, it seems as though the latest flood maps rely on older data and assume the continued operation of a nearby culvert and an upstream dam. Therefore, flooding at our site is likely dependent on both of these infrastructures. The study also reports that less than 100 years ago, a high-water mark came to within five feet of grade at our site. We note that residents received eight hours' notice during previous high-water events. The hazard travel time is the period from when we first identify a hazard to when it reaches the target. We document the indicator and the travel time here, and manage these in Driver 4: Security Requirements.

One-mile (1.6-km) area of interest with future flood heights and crime records or points of interest

We next examine weather and climate data. It appears to be trending upward, and we note the average and extreme highs at our location. We can use these later to estimate the passive survivability of the subject facility during severe weather events. We also note that our location's climate forecast predicts average values in 30 years, which matches the current extreme values. We can get additional climate risk information through our energy assessment. Furthermore, we note that precipitation across the region increases over the same period, which will impact both the magnitude and speed of a flood event, reducing the available warning time.

Socioeconomically, the building is in an entertainment district on the edge of a working-class neighbourhood with a large immigrant population, indicating that many of the neighbours, and perhaps many of the employees, may not be English-as-a-first-language speakers, which can impact emergency response. There are also many theatres and a stadium nearby, indicating significant pedestrian crowds and vehicle traffic on event days. We also note that the site is along the path of an annual marathon. Our building is just inside the secure zone, which will cause access and egress challenges annually.

The crime in the area consists primarily of mischief, nuisance, theft and minimal violent crimes. We should consider the likelihood of theft in our public areas and parking garage.

We contact our power utility, which indicates the location of our supplying substation. It happens to be just on the edge of the regulatory flood plain. We note that while we may not flood during an extreme weather event, we could still lose grid power.

We compare this site to another one a kilometre away, on the other edge of the neighbourhood. It is subject to the same future climate impacts but has a brick and precast concrete façade, as opposed to the glass curtain wall system at the current site. It borders a lower-income neighbourhood with a higher crime rate, particularly aggravated assault and aggravated sexual assault. However, the site is a few metres higher in elevation and is supplied by a different substation, which is further from the flood zone and less exposed to floodwaters.

This second building may be less aesthetically pleasing and in a less desirable area. Still, it is likely to fare significantly better during an intense precipitation event, as well as increased annual temperatures over time. Conversely, staff working late are likely to feel safer in the first building. By including these considerations from the outset, we can ensure that they are accounted for when we calculate the operational expenditures and estimate returns.

The status quo assessment methodology can miss these critical financial, human and operational costs. If we do choose to accept these risks, we should account for this in our financial disclosures.

Further resources

- **Crime Maps (Toronto Police Service)**
  http://data.torontopolice.on.ca/pages/maps

- **Natural Hazards (Natural Resources Canada)**
  https://open.canada.ca/data/en/dataset?organization=nrcan-rncan&q=Hazards

- **Ontario Hazard Identification and Risk Assessment (Government of Ontario)**
  https://www.emergencymanagementontario.ca/english/emcommunity/ProvincialPrograms/hira/hira.html

- **Flood Risk Mapping (Toronto & Region Conservation Authority)**
  https://trca.ca/conservation/flood-risk-management/flood-plain-map-viewer/

Look for your city's equivalent resources.

DRIVER 2:

PLANNING ENVELOPE

DRIVER 2:
PLANNING ENVELOPE

Objective

Understand the facility's capabilities and its servicing infrastructure, and compare it with the needs of the tenant operations. This comparison of capabilities and needs will assist in determining the most suitable use for each space and prioritize any investments that may be required.

Explanation

Sites are better suited to some businesses than others; some suites or floors are more appropriate for select tenants within a facility.

Begin by mapping out the operations that must occur in the space and the critical and essential supporting functions. Your engineers can then determine the load/demand to the facility equipment and utility infrastructure. Your facility engineers and operators may already monitor and report much of this data.

Compare this with the capacity of the utility supply at the zone/circuit, facility and neighbourhood scales. Any gaps between the demand and the capacity indicate opportunities to intervene with sustainability measures or perhaps a chance to match a tenant to a more appropriate space.

Guidance

The planning envelope refers to the demands or requirements that an operation places on the infrastructure/utility on which it depends; in other words, what the facility and its supporting infrastructure must provide to its tenants. A top-down approach to defining the planning envelope requires an accurate functional understanding of the tenant's operational requirements. A bottom-up approach will examine the capabilities of the existing facility and infrastructure and determine what the facility can support.

Those involved in sustainability will be familiar with demand management. In essence, it is the reduction of energy and resource consumption, which is one of the primary goals of BOMA Canada's BOMA BEST® program, the CaGBC's LEED program and the Toronto Green Standard.[20] Demand management enables dependency management. If you are already investing in LEED certification, many resilience measures are achievable for minimal, if any, extra cost.

For tenants, conducting the dependency mapping exercise can be extremely valuable on its own. It will assist in business resilience planning and provide insights that can drive the better use of existing space or the search for new space.

Understanding dependency

A dependency is anything that a tenant operation requires to function. A law firm needs to access its data, so it requires computing infrastructure, electricity and communications. Its staff and clients need a habitable work and meeting environment, so they require lighting, restrooms and HVAC, which in turn requires electricity, gas, water and communications.

A grocery store requires its staff, customers, inventory and points of sale. The points of sale require electricity and communications. The staff, customers and inventory rely on the transportation network, which requires fuel, electricity and rights of way. Some of the inventory requires refrigeration, which requires water, electricity, gas and refrigerants.
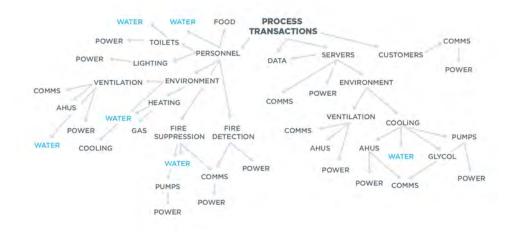
This process of breaking down an operation into its components is called dependency mapping, and is scalable. Each operation is the sum of many individual functions that depend upon services, infrastructure and resources. Each of these dependencies will, in turn, depend upon other services, infrastructure and resources. Tracing these dependencies over three iterations produces a sound local model. We need to distinguish between these component functions so that we know what we need in a crisis.

[20] BOMA BEST®
https://bomacanada.ca/bomabest/aboutbomabest/LEED https://www.cagbc.org/CAGBC/LEED/Why_LEED/CAGBC/Programs/LEED/_LEED.aspx?hkey=5d7f0f3e-0dc3-4ede-b768-021835c8ff92

Toronto Green Standard
https://www.toronto.ca/city-government/planning-development/official-plan-guidelines/toronto-green-standard/

Dependency network for a firm with core mission requiring data processing

At a fundamental level, a retailer's core business is exchanging goods for payment. The ability to receive payments from customers is an essential function of the grocer–without this function, it ceases to operate as a grocer. Other essential functions include receiving and storing inventory and paying employees. Supporting functions might include advertising, researching and testing new products and recruiting/human resources. While these are necessary for the long-term sustainability of the business, they exist in support of the core operation. This distinction will become important as we dive deeper into incident response and recovery in Driver 3: Incident Sequencing.

Understanding demand

We speak in terms of the demand that we place on the infrastructure. The infrastructure delivers the required resource. The demand is described as how much of a resource we need when and for how long. Grid-wide, peak electrical demand is typically during the hottest summer afternoons when building cooling is at a maximum; peak internet demand is between 8 p.m. and 10 p.m., when we collectively finish dinner and sit down to watch television.

Typically, most of the energy consumed by an office building is due to heating, ventilation and air conditioning (HVAC), and it's rising. Worldwide in 2010, buildings accounted for 32% of annual greenhouse gas emissions.[21] By 2019, this was 39%.[22] Under current configurations, summer electricity consumption is typically 20% higher than the rest of the year, and we can expect it to increase by 6% due to climate change.[23] For this reason, Authorities Having Jurisdiction (AHJs) require increased efficiency for building envelopes to reduce the energy demand from mechanical heating and cooling.

Understanding and verifying the actual demand is important. In the early days of LEED certification, many rated facilities performed worse than the reference buildings they were supposed to outperform, so much so that LEED now requires ongoing measurement and verification to demonstrate that the facility functions as intended.

> *Understanding our capability to meet future demand is also critical. By 2050, 90% of the entire global population will have migrated to cities, increasing the stress on existing municipal infrastructure.*

Add this to the additional demand due to climate change and we can see why some jurisdictions are moving towards regulating survivability in multi-unit residential facilities.

Note that we do not have to invest significantly to take advantage of the early analysis of future demand. If we know that precipitation intensity will increase in the future, we can upsize all drains and storm lines now at minimal cost, to avoid backups in the future. We can design the floor slabs for the amenity spaces adjacent to mechanical penthouses to resist the same loads as the penthouses. Then, if we need additional equipment in the future, space can easily be subsumed without costly and difficult floor reinforcement retrofits. We can also provide easily removable wall panels at mechanical floors with the expectation that equipment configurations will change with changing technology and demands. These measures do not cost much now but can save significant investment and operational disruption in the future.

[21] Lucon O., D. Ürge-Vorsatz, A. Zain Ahmed, H. Akbari, P. Bertoldi, L. F. Cabeza, N. Eyre, A. Gadgil, L. D. D. Harvey, Y. Jiang, E. Liphoto, S. Mirasgedis, S. Murakami, J. Parikh, C. Pyke, and M. V. Vilariño, 2014: Buildings. In: Climate Change 2014: Mitiga-tion of Climate Change. Contribution of Working Group III to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change [Edenhofer, O., R. Pichs-Madruga, Y. Sokona, E. Farahani, S. Kadner, K. Seyboth, A. Adler, I. Baum, S. Brunner, P. Eickemeier, B. Kriemann, J. Savolainen, S. Schlömer, C. von Stechow, T. Zwickel and J.C. Minx (eds.)]. Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA.

[22] World Green Building Council (2019) Bringing embodied carbon up front: Coordinated action for the building and construc-tion sector to tackle embodied carbon.

[23] Ralston Fonseca, F., Jaramillo, P., Bergés, M., & Severnini, E. (2019). Seasonal effects of climate change on intra-day electricity demand patterns. Climatic Change, 154(3), 435–451. https://doi.org/10.1007/s10584-019-02413-w

Managing dependencies

We are inherently familiar with the concept of using less energy, but dependency management is less intuitive. Short of generating power or drilling a well, surely there is not much we can do about our reliance on the water and power networks?
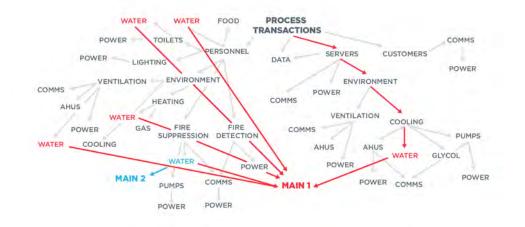
Consider our law firm again. The staff need washrooms, which require power and water, and the water itself requires power for pumping. In Toronto, head pressure in the water mains will get water up to four storeys without a booster pump. By providing a rooftop cistern that uses gravity alone to serve the fixtures in the facility, we have eliminated our water's immediate dependence on continuous power. Removing the need for power to deliver water at pressure on demand, we can shift that power demand profile to a much lower one that averages the same water supply throughout the day. It will have a modest impact on overall electrical demand but significantly impact our ability to function during an outage.

Further, most office buildings do not have operable windows. Fans and ducts pump in outside air, while carbon dioxide is exhausted in the same manner. Depending on the size and occupancy of the space, carbon dioxide levels can reach unsafe levels in a manner of minutes should the HVAC system shut down. Providing operable windows can reduce our dependence on power for ventilation during an outage.
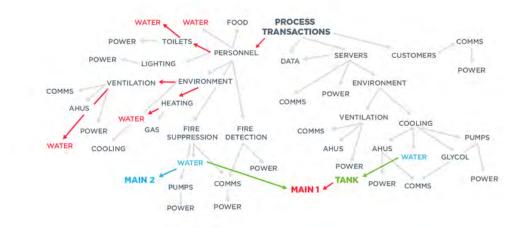
Relying on a diesel generator to keep fans and pumps operational only adds a dependency on a diesel fuel supply, which itself relies on the transportation system. It means we have also increased our vulnerability via any hazard capable of disrupting our fuel supply, like the ice or snow event that caused the power outage in the first place. Further, the government can intervene during an extended area-wide outage to redirect fuel to critical infrastructure facilities in many jurisdictions.[24] Hospitals, communications and water infrastructure, and government facilities will be the priority, regardless of any contracts commercial buildings have with suppliers.
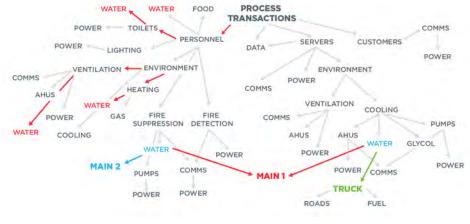
[24] Ontario Emergency Fuel Distribution Protocol https://www.emergencymanagementontario.ca/english/emcommunity/ProvincialPrograms/ci/emergency_fuel_distribution_protocol.html

Dependency network diagram showing how multiple dependencies link back to servicing infrastructure

Dependency network diagram showing how the opportunities are apparent and efficiently targeted to address just the critical processes

Dependency network diagram illustrating how mitigation measures can introduce new dependencies

Defining the planning envelope

Once we have mapped out the functions that comprise the tenant's operations, they can be split into essential and supporting functions. Highlight the logical and infrastructural dependencies, which can expose and manage the gaps between what's required and what's available. These dependencies inform our design criteria for mitigation measures. Splitting the functions allows us to plan for both impaired (emergency) and routine operations and interface with the utility suppliers accordingly.

We can also understand what our future demands will look like and, crucially, the future stresses that we and our neighbours will collectively place on the utility providers. Finally, we can identify if we can adapt the site, or any spaces within, to different and potentially more utility-intensive occupancies. For example, could the rental space be used as a future data centre, laboratory, restaurant/kitchen? It resembles functional programming, and if potential tenants are interested in later adaptation, they should be brought into the process early. Driver 5: Integrated Design illustrates what can go wrong when planning without an integrated process.
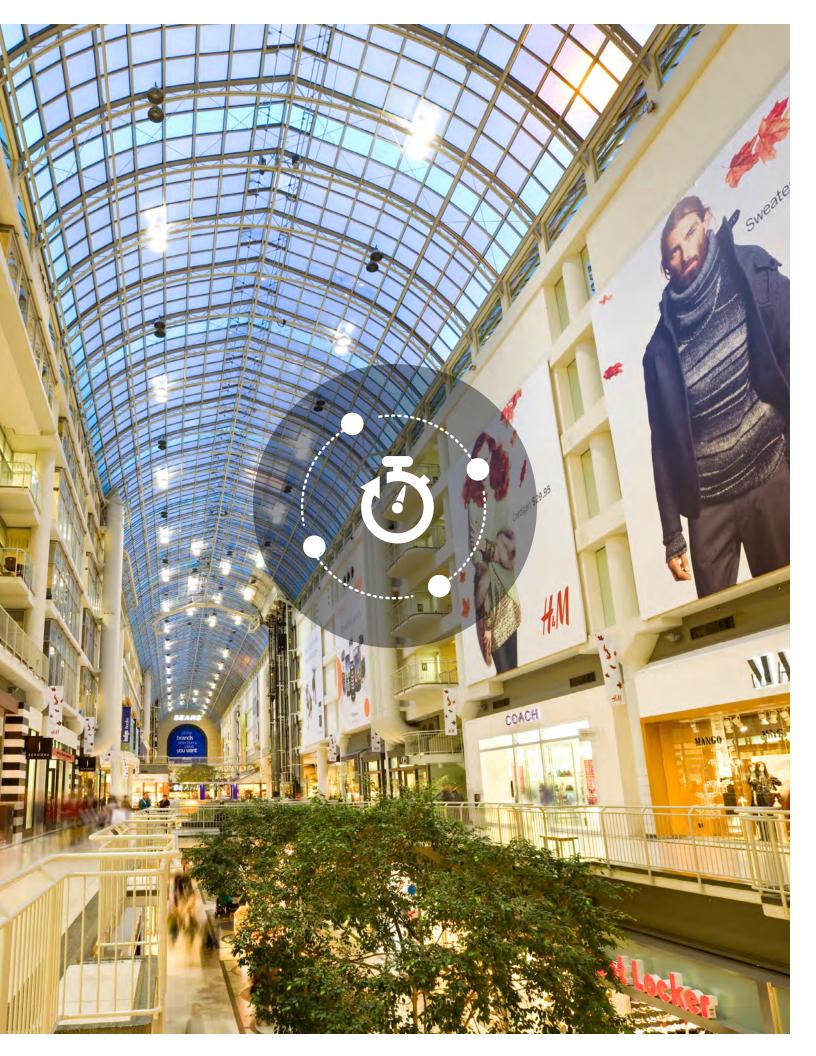
Specialist consultancies can map these functional dependencies, typically using directed-path graphics, for causal chain analysis. It means that you can trace the consequence of a change or incident through the complex system of systems that is today's commercial property. You can capture the financial and operational impact of a failure or service/access interruption.

These models also help you identify impending failure indicators, including early signs before actual harm is apparent–in effect, the early warning signs that something is about to go wrong. The janitorial and maintenance staff typically see these warning signs in their routine, though they rarely recognize their significance. However, if they are armed with cameras and take the same images each day, image processing software can detect differences or anomalies for further investigation. When these anomalies align with those warning signs, you know you have a problem. It means that you can intervene in a problem before it has caused significant harm and operational disruption and significantly reduce your loss.

DRIVER 3:

INCIDENT SEQUENCING

DRIVER 3:
INCIDENT SEQUENCING

Objective
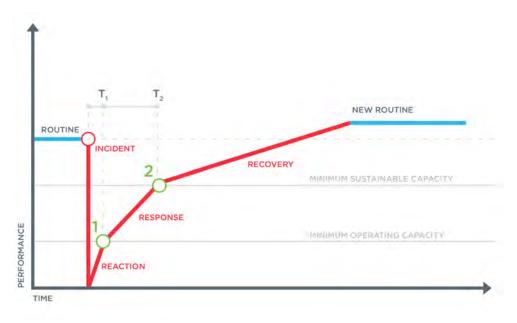
Understand what tenants need to achieve to stay in business, and work backwards to assess the level of facility performance required to enable it.

Explanation

Incident Sequencing incorporates time into our analysis. It is where hazard effects and recoverability of function become important. The critical Planning Points become our design requirements, and any gaps between a tenant's recovery requirements and the ability of the facility to deliver them will define the risk mitigation strategy.

The Incident Sequence Diagram

Recall from our discussion of Driver 2: Planning Envelope that we can classify the various functions within a business as critical/essential, sustaining/supporting and routine. These roughly correspond to the performance levels indicated on the Incident Sequence Diagram below: Minimum Operating Capacity, Minimum Sustainable Capacity, and Routine.

Generic incident sequence diagram

Routine

This is business as usual, pre- and post-incident. Given the opportunity to upgrade equipment and often to streamline operations, the post-incident Routine performance level is usually higher than pre-incident performance levels.

Minimum Sustainable Capacity (MSC)

The level of performance required to break even while recovery measures are implemented to get operations back to Routine performance. Theoretically, there is sufficient net cash flow available to operate indefinitely while the insurers process your claim and you purchase and install new equipment and repair your facility. Reaching this level of performance often requires active response measures that restore functions to support this level of performance within the designated time frame, the Planning Point.

Minimum Operating Capacity (MOC)

The level of performance required to fulfill the corporate mission at an impaired but still functional level. Reaching this performance level should be automated to the greatest extent possible, as we are only reacting to the impacts of the incident and may not yet be aware of its cause. We can define MOC abstractly or in aggregate, as in "able to execute transactions" or "critical loads are powered"; or at higher levels of granularity, as in "18kW uninterrupted to the server room." Note the implied time frame in these statements–these must be defined explicitly to be useful.
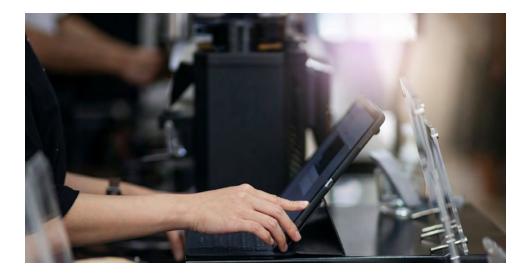
The time available to restore functions to a predefined level of performance is known as the **Recovery Time Objective (RTO)** and is explored further through examples. The restoration of MSC within the RTO is also known as the Planning Point. It defines the point at which a stable level of performance is achieved within financial, operational and market tolerances.
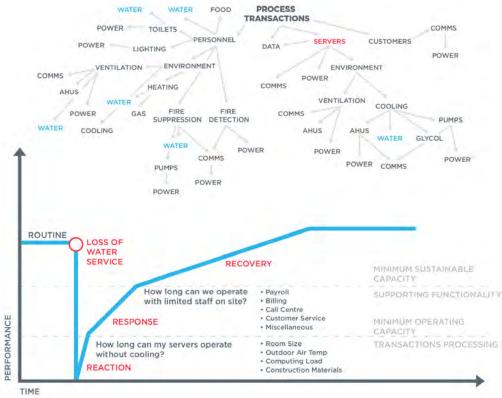
Guidance

Mapping tolerance to failure and recovery objectives

When a facility loses power, each function within that facility will respond differently, and its supporting equipment and infrastructure will have differing tolerances to failure. Retail points of sale (POS) must remain online to assure the integrity of transaction data; as long as transactions need to be processed, the failure tolerance of POS is virtually zero. We might, therefore, explore what the tolerance would be for an interruption in retail transactions. The supporting infrastructure to POS includes its power source, communication to a local network server, and the wide area network to the regional banking/financial system. Therefore, this infrastructure must remain available, as well.

The professional services firm has effectively outsourced the payment function to its financial institution. It simply invoices clients, who then instruct their bank to complete the transaction. So, the firm itself has some tolerance to the failure of this function. As we discussed in Driver 2: Planning Envelope, the firm is in the business of document production and customer service. They require access to their documents and data and a means of communicating with clients. The tolerance to a power failure depends on the availability of an alternative means of communication, the cost of creating the documents and data, and the cost of recreating any lost work.
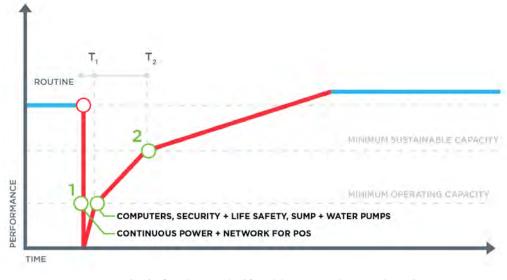
Relationships between the dependency map and incident sequence

Functions with a zero tolerance to power failure are typically those for which an abrupt shutoff will result in corrupted data or a lengthy restart. The retail store would include the POS and associated network infrastructure; for the professional services firm, this would include the local data centre. Access control must remain functional for both tenants–we discuss this further in Driver 4: Security Requirements. These functions are plotted below, along with those required for building code (emergency lighting, elevator controls, etc.) compliance.

Functions with a limited but non-zero tolerance to power failure might include some or all computer workstations, critical tenant equipment or processes, sump pumps and elevators. We don't expect damage if these items shut down momentarily, and our Recovery Time Objective for these items is in the order of seconds or minutes. We show these functions below.
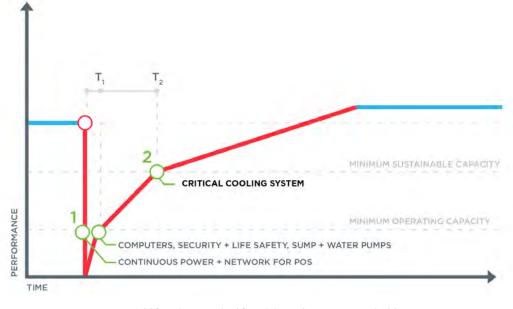
*Plot the functions required for minimum operating capacity and
required recovery time objectives*

Critical tenant equipment will vary by tenant operation. A law firm may rely heavily on its local server room, a design firm on its 3D printers, and a grocer on its refrigeration system. These each have very different infrastructure requirements and tolerances.
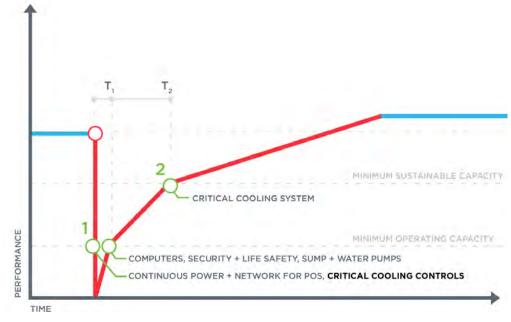
Let us first examine the grocer. A significant portion of its inventory is perishable and either refrigerated or frozen. When power is lost, so is the dependant refrigeration system. The RTO for this system will depend on the ambient temperature, the original set point, the amount of stock in each cooler and freezer, the type of equipment in use and the requirements of the local Authority Having Jurisdiction (AHJ). Our mechanical engineer has calculated that undisturbed, our freezers and coolers can maintain a safe temperature for four and two hours,[25] respectively. We can add these to the incident sequence as T_2 –we have some time to sort this out, but it is a critical milestone we must reach to maintain sustainable operations for any length of time.

---

[25] The actual time tolerances will vary by operation. Some sites will have regular access to the refrigerated areas, while others can afford to shutter them and extend the time available. One of the grocery chains corresponding in the development of this document has approached this with a simple Standard Operating Procedure, which allows for a variance in access, season and routine by mandating a maximum of 2 hours time tolerance from loss of power to removing all produce from store.

Add functions required for minimum long-term sustainable
operations and required recovery time objective

Note that all of the above assumes that we can continuously monitor and audit the temperature in each cooler. We lose the ability to demonstrate compliant temperatures to the local health authority if temperature monitoring is limited to refrigerant lines (rather than interior temperature), or if there is no power backup to the system's sensors and controllers. Compliance requirements are specific to the operation and jurisdiction, but we must prove that the food has been kept consistently at a safe temperature to demonstrate compliance. Smart deployment of sensors and automation here can drastically improve our situational awareness during the incident and can potentially avoid the cost of spoilage. Thus, we add refrigeration controls to T_1 and to our accounting of the *cost of losses avoided*. We will revisit this example in Driver 5: Integrated Design, where we discuss the impact of resilience on the Total Cost of Ownership (TCO).

Add additional dependent essential functions as we discover them

While we began this exercise with a power failure in mind, note that the incident sequence is more or less event-agnostic. We determined we have T_2 hours to restore our refrigeration function, regardless of how it was lost. To mitigate:

- **A utility power failure**
  We could provide a backup generator and a source of fuel sufficient to bridge the outage, or we could provide a solar system with enough capacity to maintain full or even partial refrigeration when islanded from the grid–more on this below.

- **A power failure due to local basement flooding of electrical equipment**
  We could ensure switchgear is above grade. Alternatively, we could provide a means of de-energizing everything below grade while maintaining the main supply, or provide a method of energizing just the service to the critical equipment, bypassing the flooded infrastructure.

- **A refrigerant leak**
  We could ensure that sensors are alarming remotely. A leak after hours can be responded to, and confirm repairs can be made within the time objective and without having to evacuate the entire building. We can similarly mitigate the potential liability arising from a major leak through refrigerant selection.

- **A compressor failure**
  We could provide them in an N+1 configuration, understand the lead time for repair and replacement, and conduct regular preventative maintenance and health monitoring.
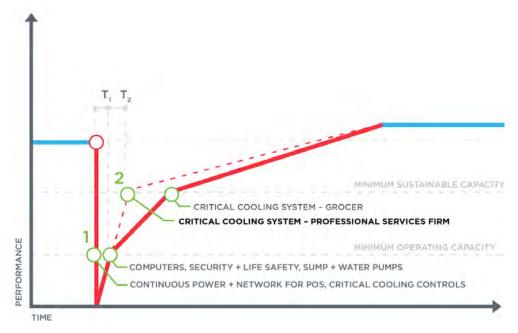
- **Any of the above**
  We could test the time it takes to clear a cooler into adjacent units or a reefer truck that we have on call, so that we know that we can conduct this process before the point of spoilage.

Once the operational requirements for recovery are defined, we can cross-reference this with the list of hazards from our LRA and build mitigation strategies specific to both the tenant and the facility.

Let us turn to the professional services firm and examine how the cooling system recovery time differs. We understand from our earlier discussion that our computing infrastructure must remain online because an abrupt shutdown can impact data quality. Our server room depends on critical cooling. Suppose this cooling is lost while our computing equipment operates and generates heat. In that case, we will have minutes, not hours, to recover cooling functionality before the temperatures in the room exceed 40° C, and we risk catastrophic equipment failure.

*Note how the recovery time objective changes with
the needs of a different tenant*

When we compare the server room's recovery time objective with that of the facility, there appears little scope to accommodate the different requirements. A backup that would satisfy the server room requirements would be costly when applied to the whole facility. The HVAC systems in most buildings are not backed up with emergency power. Where installed, Computer Room Air Conditioner (CRAC) or Computer Room Air Handler (CRAH) units often rely on water or air that the building's cooling system has already chilled. Thus, extending backup power to these units would be moot.

The tenant could invest in a cloud or offsite fail-over solution to avoid a cascading failure. A graceful shutdown will commence when temperatures remain above a critical level for a specified period. This shutdown would move the cooling function further out in time, providing more time to recover from a power outage, equipment failure, or whatever the cause.

Finally, let us examine the impact of our power outage on space conditioning for our tenant's staff and customers. If we lose power to our facility's HVAC system, the consequences depend primarily on the time of year. In the middle of summer, a glass office tower may become unbearably hot in under an hour, although there is no regulatory upper limit for how hot "unbearable" is.[26] In winter, an office tower may become too cold (below 18°C) in hours. The Toronto Green Standard sets criteria on how hot or cold an occupied space may become after 72 hours and two weeks without power supply.
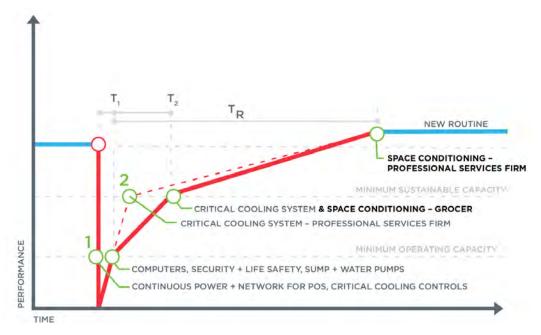
The grocer, located within the thermal mass of the podium level and with a large air volume to change, will maintain comfortable temperatures for significantly longer than the law firm. The glazed façade and smaller air volume will change much more quickly.

Note, however, that the workplace facility itself is not required to meet the professional services firm's minimum operation requirements – the firm can continue to service the needs of its clients for some time without the staff use of its office space. So how long must it be able to operate without an office? Until it can stand up a temporary location, at which point it will be able to run indefinitely–it will have met its minimum sustainable requirement for workspace.

Remember that incident sequencing is agnostic to the source of the initiating event. For example, let's say that the firm has made advanced arrangements to stand up a remote worksite within three to five days following a local or area-wide incident. Through our planning, we ensure that employees can access data in the interim. Therefore, the firm can cope with any event that keeps them out of their building for weeks without incurring a significant business loss.

---

[26] The literature is varied on this, though ultimately one can be sure that the market will decide whether the space is worth the rent or not. Under low (controlled) humidity a temperature range of 18°C to 25°C in winter and 20°C to 27°C in summer is supported by established research and reflected in the ASHRAE guidance. Givoni B (1992) Comfort, climate analysis and building design guidelines. *Energy and Buildings* 18:11-23.

Meanwhile, the grocer is significantly more dependent on the physical storefront. It is where the grocer receives its inventory and where its customers, who live in the neighbourhood, go to purchase its goods. If the grocer loses its facility, it can no longer provide even a minimum level of service to its customer base and has no way to break even. Other tenants similarly dependent on the facility itself would be doctors/dentists, restaurants, spas and other retailers.

Note the differing performance level requirements for space conditioning of each tenant and the resulting impact on recovery time required

The obvious implication for the building owner is that the professional service or knowledge firm is less dependent on their facility and, therefore, much more agile. Their critical function is continuous, reliable data access. If you can't keep them operational through an incident, they will quickly find someone who can.

Accounting for climate change

Climate change in Canada will result in increased extreme temperatures and humidity, as well as more volatile storm events. We now briefly discuss this impact on our incident sequences, specifically on a facility's capability over its life and the time available to respond to an event.

As the climate warms, the cooling load will increase during the summer, and the heating load will decrease during the winter. It means that the frequency of extreme heat events will increase, and our future response time to an extreme heat event or a loss of space conditioning will need to be shorter than our current response time. If one of our ongoing response measures is to draw all the blinds and window coverings in the building, we will have less time to do this in the future.

Similarly, as storms become more volatile, we will likely see an increase in local high-intensity rainfall events or microbursts. These events develop with little warning and can quickly overwhelm roof drains, storm drains and stormwater piping, causing significant overland urban flooding.

> *Where we previously had the 30 minutes required to observe that a storm drain was backing up and then install manual flood gates, in the future, we may have only five or 10 minutes between noticing the backed-up drain and the water rising to our doorstep.*

We will address some design-focused mitigation measures in Driver 5: Integrated Design. From an incident management perspective, given that hazards will be coming at us faster, smart mitigation investments will include measures that can provide earlier detection and automate the response process. Examples include sensors down the street to detect overland flooding before it reaches us or smart motorized blinds that deploy automatically.

Leveraging your operations experts

Our building operators are important resources in the incident planning process. They understand their facilities better than anyone else and can guide the project or assessment team in understanding existing vulnerabilities and expected behaviour under stress or interruption. They can indicate how they currently respond to equipment failures, and the sensors or other indicators they wish were available.

They can speak about the service contracts currently in place, how long each takes to dispatch a technician and often where those technicians are coming from. (If a vendor has three technicians who are qualified to work on a certain controller, and all live in the same suburb which was isolated by the same storm that fried your controller, we should expect to wait longer for a call than the time specified in the service agreement). Crucially, building operators can help to validate the assumptions we've made in developing our incident sequence. For example, perhaps the generator does not start reliably during winter.

Building operators can also provide valuable intelligence on particular tenants or types of tenants that may not be obvious, based on their experience dealing with them. A government agency or charity that deals with the elderly or disabled may have a large proportion of their customer demographic who cannot climb stairs. They may also receive higher volumes of walk-ins at certain times of the week or month and deal with time-sensitive matters. An incident response plan that does not consider these factors will be incomplete, as they will impact evacuation time, facility security during an incident or unplanned closure, and resources and infrastructure required to reach Minimum Operating Capability.

When sustainability and resilience compete

We discussed in Driver 2: Planning Envelope how implementing sustainability measures to manage demand can positively impact resilience by reducing the level of resource dependence on infrastructure. However, sustainability measures implemented myopically can harm resilience because most analysis does not explicitly require accounting for recovery. In effect, one must be careful not to optimize for one design objective while unintentionally worsening another.

One of the trends in sustainable design is right-sizing equipment. While a typical design approach would use a conservative estimate and provide equipment capable of exceeding that estimate, right-sized equipment will closely match the calculated HVAC loads. Smaller equipment is generally more efficient to operate, providing energy savings over the unit's life.

However, such equipment is only right-sized to maintain a set temperature under a specific load. For example, consider a power outage in which the cooling equipment serving a data centre or server room has to restart while the computing equipment on UPS continues to operate. The room temperature will rise quickly, potentially becoming unacceptable before the cooling system has restarted. Then, the temperature will remain dangerous to equipment much longer without excess capacity, increasing the risk of equipment failure.[27] In such cases, rather than sacrificing sustainable design targets, consider a safe-to-fail approach that permits a time-critical response without any external dependency. It may mean an evaporative cooling system connected to a battery bank and an alternative power supply.

[27] Paul Lin, Simon Zhang, Jim VanGilder, Data Center Temperature Rise During a Cooling System Outage, Schneider Electric White Paper 179R1, https://it-resource.schneider-electric.com/white-papers/wp-179-data-center-temperature-rise-during-a-cooling-system-outage

> *When we look at building services as a system of systems instead of as individual services and disciplines, many critical service dependencies can disappear.*

By looking at each system in isolation, we make multiple assumptions about its demand and dependency management. These assumptions can disappear by taking a holistic view. While the operation looked at as a whole may seem more complex, it becomes simpler to analyze.

Another trend is using a warmer supply temperature, which is now permitted by ASHRAE's latest design standard for data processing facilities.[28] The consequence of maintaining a higher normal room temperature is similar to right-sizing equipment. When cooling is lost, we have less of a buffer to absorb the disruption and will reach a critical temperature faster. The energy and associated cost savings over time of operating at a higher temperature may justify accepting an increased risk of equipment failure during a cooling outage. Regardless, we must understand the consequence of the decision on uptime before implementing any measures.

A third example is the application of the Exterior Insulation Finish System (EIFS) and Structural Insulated Panels (SIPs) for both façade retrofits and new construction. These products provide cost-effective and extremely energy-efficient building envelopes. Unfortunately, they can also be highly flammable, and when inappropriately used, can cause a faster spread of flame than either sprinklers or first responders can match.

In both cases above, designing strictly for demand management without offsetting/mitigating design choices may have adversely impacted resilience. The incident sequence is a powerful tool for incorporating incident response and recovery as design criteria in their own right.

Portfolio assessment

Instead of constructing these performance plots from a tenant's perspective, we can build them to represent the capabilities of the facility. In other words, we can determine the level of performance a building can enable during and following an incident.

This approach can be useful for several reasons. First, it allows us to compare properties for their functionality under stress or impairment. Knowing this, we can facilitate a better match between building and tenant. It can also indicate which buildings may require significant investment in the near to medium term or which ones may be inherently less ready for the future. Such properties are good candidates for divestment.

---

[28] American Society of Heating, Refrigeration, and Air Conditioning; Standard 90-01 and 90-04:2019, and Technical Committee Whitepaper TC9.9:2016 Data Center Power Equipment Thermal Guidelines and Best Practices.

Second, we can justify investments using the incident sequencing process. If an energy analysis has warranted a smart LED lighting upgrade, the incident sequence can justify the inclusion of smart shades and emergency power to the network switches.

Finally, it can identify opportunities for more capital-intensive and creative mitigation strategies for clusters of buildings with similar vulnerabilities. We explore some examples below.

Collaboration with utilities
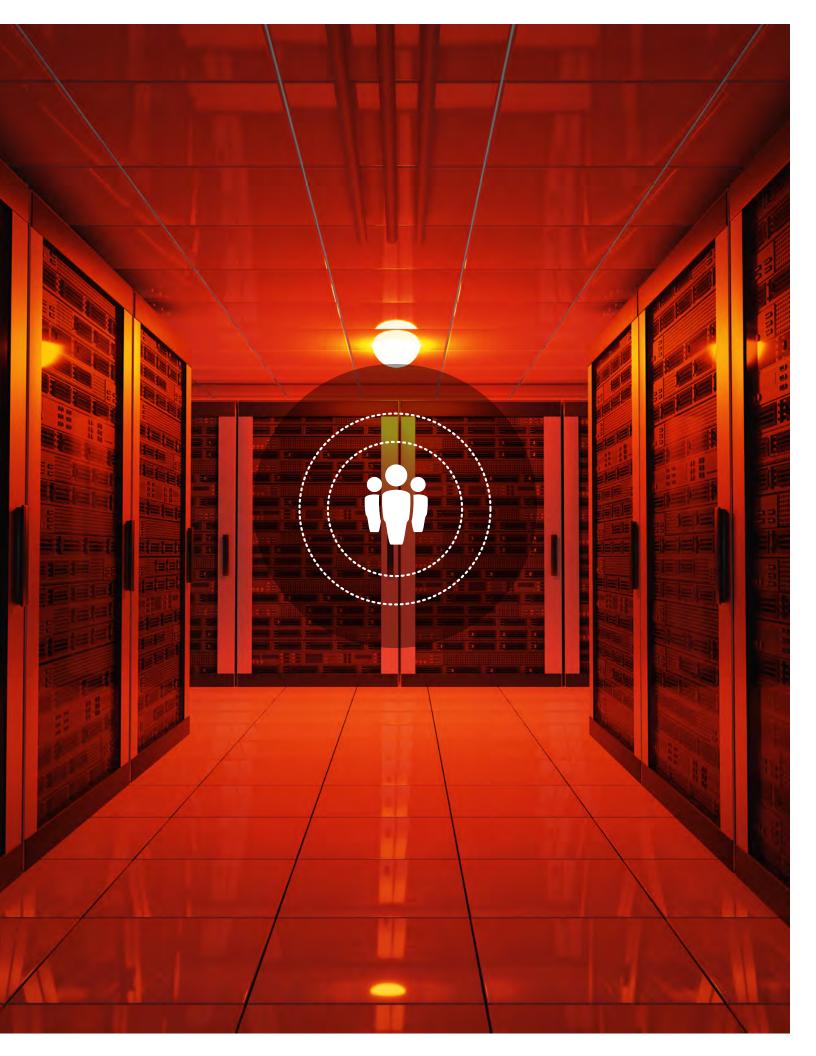
Understanding what levels of continued utility service are possible requires a close relationship with the utility. We need to know that when there is a grid supply power outage, for example, what this means in terms of continued electrical supply, water pressure, mobile phone coverage, transit and even electric-powered vehicle access. The issue of assured minimum levels of utility service is a key risk concern and is set to become more focused over time. The consequence of a business interruption continues to grow as the value of businesses concentrates. So, too, does the sensitivity to data corruption and interruption of access.

For some high-value operations with a high sensitivity to variations in power supply, the clear financial case for risk managers is to off-grid or island completely. However, this misses the safe-to-fail aspect of resilience planning. Islanding may remove the vulnerability to a critical uncontrolled external supply, but it neglects what it means when the fuel supply is interrupted or a switch fails. Better to remain connected to the utility and be capable of islanding than to operate as an island. The advantage of remaining connected is that neighbours can share and support each other during stress or grid failure. It also enables the utility to cluster island-capable customers with resource storage and smart resource management, providing a continued response service within the cluster. The principles are the same regardless of whether one is talking about water, electricity or wastewater. If the resource dependency is critical, it is better to be islanding-capable than off-grid.

Forward-thinking utilities are looking into a variety of clustering support services and critical-use customer services as part of their risk mitigation and customer support strategies. If you require such support, please contact your local electricity and gas utility to learn what measures are being taken to improve reliability and reduce inherent risks, and discuss how you can solve these issues collaboratively.

DRIVER 4:

SECURITY REQUIREMENTS

DRIVER 4:
SECURITY REQUIREMENTS

Objective

Understand where residual risk remains and design your security requirements to fill these gaps. Security functions themselves also need to be protected. An all-hazards awareness must be maintained, and security functions developed to ensure that measures to address one risk do not exacerbate another.

Explanation

Ask your neighbour what security is, and you will hear, "Guards, locks and cameras." Ask your CSO or a security consultant, and you may hear, "The protection of assets: people, property, and information."

Security is much more than this in a resilience context. Security protects the whole operation. During an outage or failure, the security systems must enable the essential functions defined earlier. It means the security systems themselves must remain operational. We must understand at a functional level what we need them to do to understand how we need them to perform during an incident.

Conventional security design typically begins with the assets, if it happens at all. Too often, a new security plan is based on an older one from an existing property, or a security vendor is brought into a nearly finished space to provide some cameras and card readers. Some tenants may provide their minimum design standards that specify which doors must be access controlled.

Operational security design allows the business operation to guide the process. We can then define performance-based requirements for conventional security solutions, ensuring they fully integrate with business processes and security procedures, and leverage them to solve unconventional problems as well.

Guidance

Continuity of security systems

Security systems include all of the physical, electronic and procedural measures we rely on to perform several important functions:

- Deterrence to opportunistic and malicious aggressors

- Access control to the facility and various spaces within the facility

- Alarm monitoring from security-specific sensors as well as process or operational sensors

- Visual and logical situational awareness

- Forensic support

These functions are essential during normal operations–and they remain essential during and following an incident, even as the operating context changes.

We begin by walking through the performance of an access control system during an extended power outage. As soon as the mains power is lost, any magnetic locks in the building will also unlock in most Canadian jurisdictions. Magnetic locks are frequently used on glass doors to lobbies and vestibules at the building's exterior and the tenants' outer perimeter. Suppose we do not also secure these doors with a deadbolt into the frame. In that case, they will be freely accessible until the mains power is restored and the locks have been manually reset at a remote location within the building. Restoration of main power alone will not automatically re-engage these locks.

Electric locks and strikes are typically backed up by local batteries, which can vary from a few minutes to several hours, depending on their design and quality of maintenance. The functionality of these locks, while still powered, will vary depending on how the locks communicate with the user database. Recall from our dependency mapping exercise that modern security systems rely heavily on telecommunications infrastructure. Wireless locksets often communicate via the building's wifi network, and Wireless Access Points (WAPs) will likely not have power. Wired locks will generally function normally until their local batteries die.

While today we would usually connect access control systems to backup (generator) power, systems in older buildings are often not connected. It means that as soon as the local batteries die, the locks will fail, even as staff are trying to maintain operations on backup power. If the locks were specified to fail secure, they would remain locked from the exterior or insecure side while always allowing free egress from the inside. At this point, staff will start propping doors open to continue to work or respond to the situation. We no longer have control over our perimeters.

If backup power cannot be maintained–say we're unable to refuel the generator– life safety systems will also be compromised, and we should evacuate the property. We should recognize that staff will more than likely prop or tape open doors and release maglocks if we put them where they cause significant disruption to routine. Partly human nature to seek the easiest path, it is also a reflection that limiting access to the keys to these door locks, which makes sense when everything works perfectly, generates frustration when the centralized controls fail.

This scenario plays out in many facilities every time there is a major power outage. Building the incident sequence for security systems, even informally as we have done here, will help assure access control resilience in new development projects by highlighting all dependent infrastructure requiring continuity. It will also provide operators of existing facilities with a clear picture of when and where to intervene with procedural measures to avoid some of the vulnerabilities we identified above.

The impact of community resilience on security

A common response to the scenario above is, "We've only had a single attempted break-in in the past X years, and this is a good neighbourhood." Or "We're completely backed up, so we plan to operate business as usual." However, do not neglect to consider how the operating context will change around you during an incident, causing security challenges where none had previously existed.

> *There are many anecdotes of communities remaining orderly during an area-wide incident. Unfortunately, there are also many stories of looting and opportunistic crime.*

One should recognize that residents may become desperate, lacking in necessities to meet their immediate needs and lacking confidence in the government's ability to respond and recover quickly.

If the facility is or appears to be vacant–and even better, unlocked–it can become an attractive target for people who are looking for shelter or to make some quick cash. It will delay our future response and recovery efforts if we need to do additional, unexpected cleaning and equipment replacement. A fully operational and illuminated facility while the community around it suffers in darkness can become an even more attractive target for trespassers. Depending on your security stance, it can be a beacon for community assistance and outreach, as part of your social responsibility agenda.
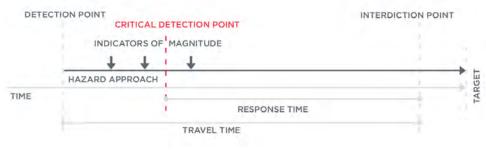
Harmonizing hazard travel and response times

We saw how time played a key role in incident sequencing, and it plays a similar role in security. Hazard travel time reflects the time it takes for a hazard to travel from its first detection to the asset/target we are trying to protect.

Some hazards happen in a flash: a burglar approaches your site, jumps the fence and forces your back door, limiting how you can react.

Others develop over days or weeks: a riverine flood or Nor'easter that's announced by the media, giving us some time to respond.

The same goes for deliberate hazards: we can see an angry crowd gathering in front of the embassy across the street; perhaps we even heard about it on the news last night.

Travel timeline and key points

Once a potential hazard has been identified, we monitor its path while determining whether we need to respond. For example, perhaps our response strategy for flooding involves installing a flood barrier across the ramp down to our parking garage, and it takes our operations team an hour and a half to retrieve the parts from storage and install them. This is the response time for this particular strategy. Perhaps our policy for dealing with a destructive mass gathering is to lock all exterior doors and call the police. If the police usually respond with 10 to 12 minutes and it takes the security guard on duty six minutes to electronically lock the leaf doors and then manually lock both revolving doors, our response times for those measures would be six and 10 minutes, respectively.

The critical detection point is the latest point at which we can detect a hazard approaching and still have enough time to intercede and respond to it. We have a problem if the actual detection time is less than the critical detection point. For example, the last time we noticed an extreme downpour was causing storm sewers on the street to back up, our garage was taking on water within 40 minutes (hazard travel time). A barrier solution that takes 90 minutes (critical detection point) to install is not a measure that will succeed. Similarly, if the protest across the street turns violent and they can reach us within three minutes, and we've only managed to lock half the doors, a 10-minute police response should not be our first line of defence.

Harmonizing our detection and response times does not necessarily require equipment or facility upgrades. However, as we will see, when we include these "upgrades" early in the design, they can usually be integrated at no additional cost. We can often achieve harmonization through procedural measures, albeit with a few trade-offs.

One strategy is to adjust the detection time. We accomplish this by widening our area of observation to include areas below us in elevation so that we can monitor those drains or culverts for backup instead of waiting for a backup right in front of us. There are analytics available that can accomplish this using thermal and infrared surveillance cameras.

Another strategy is to introduce a delay, slowing down the hazard approach and allowing more time to respond. A curb can give us a few extra minutes to patch a leak or find a shutoff valve before adjacent spaces flood, and erecting a temporary barrier in front of your facility may provide a few extra moments required to complete a lockdown. The temporary barrier option will need additional equipment and a workforce to install it and a leading indicator that the rising water presents a direct threat.

If we cannot increase the detection time, we must reduce response time. We can do this by automating some manual tasks, triggering responses to specific leading indicators and assigning additional resources. We might invest in a faster-deploying barrier, or if heavy rain is in the forecast, move components of the flood barrier from storage and stage them near the door before the rain starts falling. Similarly, we can replace our rotating doors with motorized and lockable models or take those doors out of service if we know that a protest is planned this afternoon.

Integration with operations

Understanding how protection will interface with the operations is just as important as understanding what to protect. Security integration is a specialist discipline and many high-security and mission-critical projects require a consultant with this expertise. While not every project warrants the involvement of such a specialist, any competent design or operations professional should be able to apply some of the following basic principles:
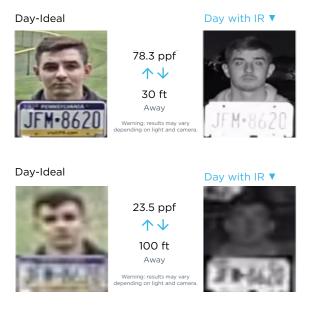
Security measures must be fit for purpose

It may sound obvious, but experience suggests a reminder is warranted. For example, if you pulled video footage from a camera located at your reception desk, what could you do with it? Could you get a clear image of an assailant's face or just the top of their head? Could you see what they passed to the receptionist? Would the picture be of sufficient quality to identify an unknown person or only to recognize a person already known to investigators? Or would the image contain nothing but a silhouette due to glare behind them from the sun or headlights? Do we need to see a face at all, or simply establish that a previously identified/recognized individual walked through the main entrance. Where do we get a high-resolution image from a different camera at eye level?

Impact of camera height on image quality[29] (by kind permission of IPVM)

[29] "Testing Camera Height vs Image Quality", IPVM.com, https://ipvm.com/reports/testing-camera-height (subscription required).

A camera, lock, sensor, fence or any other security measure cannot fulfill its function if you do not give it one. For example, a requirement like "full surveillance coverage of parking lot" is not useful. A better one would include "at sufficient pixel density to read licence plates in existing lighting conditions or perhaps positioned to capture driver faces for forensic identification as vehicles enter and exit the lot." Begin by defining the threat, then determine the operational requirements of the security measure, then select the measure, then specify it to meet the requirements, and then check that it does meet the initial requirements.

Impact of pixel density on image quality[30] (by kind permission of IPVM)

[30] Images from www.calculator.ipvm.com (subscription required).

Security measures must be coordinated with the business processes they support

Again, this sounds like common sense, but this rule is broken consistently. For example, consider an office where an access-controlled fire door is halfway along a corridor. If two employees who work closely throughout the day work on either side of that door, or if that door is along the route to a commonly used space like a coffee station or print room, that door will soon be propped open with the nearest fire extinguisher.

Resist the urge to provide access control on the door in a blind application of standard design, and first determine exactly where the controlled perimeter needs to be. Then work with your code and fire consultants to see where the door can be or if it's possible to place an additional door at the end of the corridor where the controlled perimeter is required. Finally, consider moving the offices or rooms in question to another location where security (and fire safety) are less likely to be circumvented in the name of employee efficiency.

Consider also a restaurant with costly wine on the menu, or an IT department servicing computers for a large company. The high-value storage room is fitted with a card reader, an electrified lock and a camera inside, to provide forensic assistance should anything go missing. If an inventory report indicates that bottles had gone missing last month, is there footage to review? If the inventory reports don't make their way to audit until two weeks into the next month, footage from the beginning of the audit period may have already been overwritten. We would typically store video recordings for just 30 days, and some jurisdictions constrain this even further. The intended use of the footage must be captured in the operational requirements to ensure that we don't overlook business process compatibility issues like this.

Security measures must consider the security force available

The security force wears many hats. During a daytime shift, they could manage visitors; escort people and equipment through the facility; manage deliveries and contractor access; screen vehicles, people, packages and mail; patrol the facility and site; and respond to emergency/safety and security incidents. All of this, and we also expect them to monitor cameras, catch fence climbers and tailgaters, and intercept burglaries in progress. While they do complete training, they are generally not armed.

In designing security infrastructure and developing security plans, we must account for the size and capability of the response force. For example, electronic access control is routinely value-engineered out of projects because, "Security can just lock all of those at the end of the day." Likewise, cameras are routinely value-engineered out of projects because, "The security desk is right there; they can see the whole loading dock from that window." Or conversely, "Nothing happens back there; no camera required, security can just patrol that."

The reality is that most security cameras in commercial facilities provide forensic assistance only, unless linked to detection and alarm capabilities. A human operator can actively monitor only five views at a time for about 20 minutes, that is, four pictures on a single split-screen, and a fifth on a second investigation-screen. We base this on the assumption that he or she is doing nothing else at the time. If the operator is only watching for an anomaly in the regular pattern of life, we can extend that shift to 40 minutes. After that, effectiveness tails off rapidly. Deploying a camera at a problem spot with the expectation that someone will actively monitor and interrupt an incident is unlikely to succeed. The most effective solutions use sensors or detection analytics in conjunction with cameras. This is where the sensor alerts the operator to an anomaly and cues a reaction, while the operator confirms on a specific camera using a full-size investigation screen.
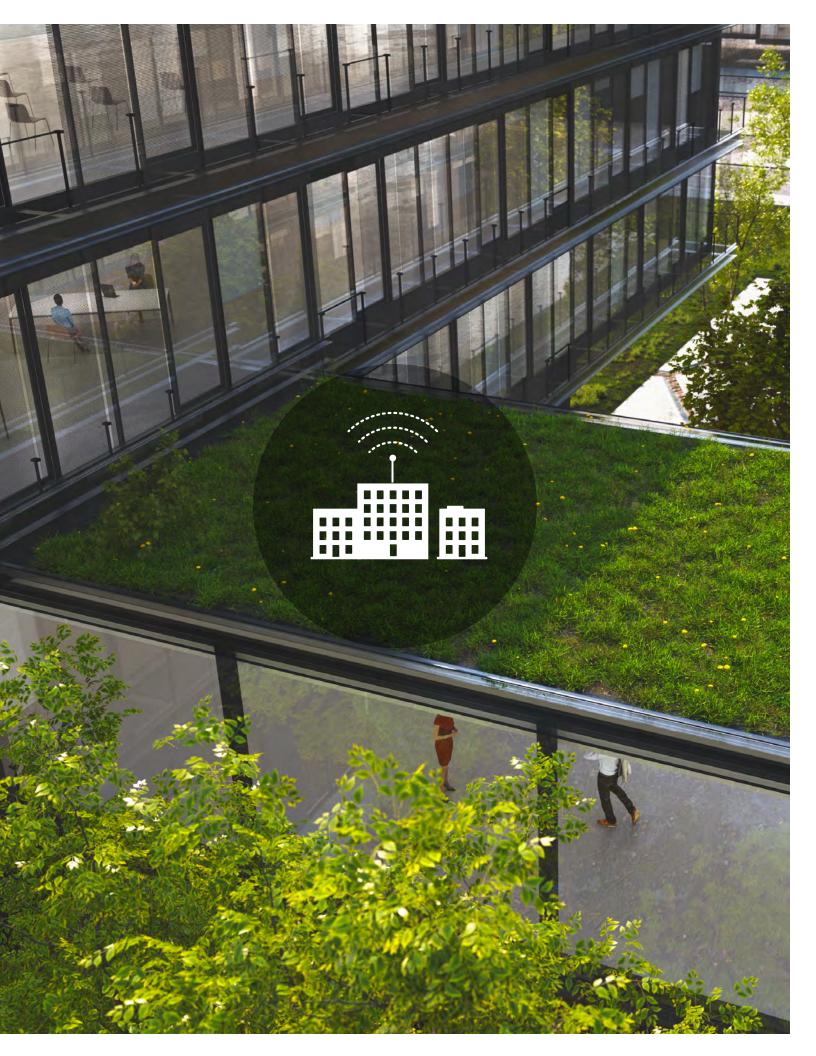
We should also remember that automation has more value than appearing to make the security guard's job easier. Electronic access control at all controlled perimeters will not only save 30 minutes of someone's time every evening. It also facilitates a one-button lockdown in response to a threat outside or an active assailant in the facility. An automated visitor management system can free the security guard from the drudgery of manually copying down drivers' licence and badge numbers, allowing them to focus on observation and relational security/customer service instead. It can also provide an instantaneous audit of everyone in the building or on a specific floor at a given time, should these be required for the incident investigation or emergency response purposes.

Risk matrix with mitigation strategies indicated (courtesy of The HIDI Group)

DRIVER 5:

INTEGRATED DESIGN

DRIVER 5:
INTEGRATED DESIGN

Objective

Understand the value in having all functional and operational interests represented early and throughout the facility life cycle. Requirements and assumptions must be documented, and critical performance requirements verified by testing key processes and systems against failure scenarios to assure that each scenario unfolds as expected.

Explanation

Integrated design is a powerful tool for building resilience because it involves all stakeholders early in the planning process and carries them through design, construction and commissioning. The Integrated Design Process (IDP) is a collaborative delivery model and interdisciplinary design approach that optimizes the building as an entire system across its life span. IDP requires active, consistent and organized collaboration among the owner, tenant/end-user, architect, engineers, builder, specialists and consultants to optimize results, value, efficiency and reduce waste.

This project delivery model is gaining traction in several sectors (P3, mission-critical) but is less common in commercial property.

The IDP Process illustrated[31]

We have seen throughout the previous Drivers how facilities are systems of systems. That is, systems that functionally and operationally depend on each other and cannot be separated. While conventional project delivery treats each system discipline discretely, integrated design accepts this interdependency premise and strives to optimize performance over the whole facility life cycle.

[31] Image taken from "Roadmap For the Integrated Design Process" - BC Green Building Roundtable 2007 - https://buildingdata.energy.gov/cbrd/resource/2109

Guidance

Conventional project delivery

Typical delivery models organize participants into three groups: the owner, the design team and the constructor. Within the design team, we would typically divide the group into architecture, landscape architecture, interior design, civil, structural, mechanical, electrical, plumbing, telecommunications, and so on.

These participants generally work in silos of responsibility that, in practice, result in inefficiencies. The inefficiencies are most acute whenever there is a transition of responsibility from one silo to another. These models often suffer from the lack of integration, collaboration and cooperation of all participants because participant success and project success are not aligned. One or more participants can succeed under these delivery models while the overall project fails.

Inherent weaknesses in conventional delivery models across design, value engineering, construction and commissioning can result in resilient requirements getting lost. Some of these include:

- A lack of collaboration between participants;

- A linear process that strongly reinforces the isolation of responsibility;

- Susceptibility to delays;

- A decision process based on schedule or capital expenses rather than life cycle economic performance;[32]

- Increased difficulty for the architect to act in the owner's best interest due to the contractual relationships;

- Owner loses control of design and execution, and decisions can be made that may or may not benefit the owner;

- Changes to the scope become increasingly difficult and expensive to execute as work rapidly progresses;

- Conflict of interest in a Construction Manager at Risk model; and;

- "Participant Success" is not aligned with "Project Success."

[32] Reflected in a decoupling of tenant/occupier values with owner/developer interests.

Benefits of integrated design over conventional design
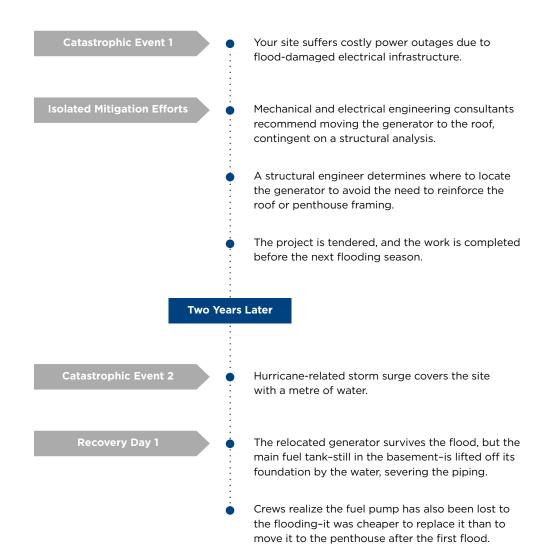
INTEGRATED DESIGN PROCESS		CONVENTIONAL DESIGN PROCESS
Inclusive from an early stage	vs	Involves participants only when essential
Front-end loaded, time and energy invested early	vs	Less time, energy and collaboration
Decisions influenced by a broad team of experts	vs	More decisions made by fewer people
Integrated process	vs	Linear process
Whole system thinking	vs	System often considered in isolation
Allows for full optimization	vs	Diminished opportunity for synergies
Seeks synergies	vs	Diminished opportunity for synergies
Life cycle costing	vs	Emphasis on up-front costs
Process continues for the life of the building	vs	Typically finished at construction completion
Participant and Project success aligned	vs	Participant and Project success not aligned
Decisions made considering the building as a whole	vs	Decisions made without considering the building as a whole
Involves commissioning and post-construction maintenance and operation	vs	Lack of commissioning and post-construction maintenance and operation

Isolated mitigation and unintended consequences

As we saw in Driver 4: Security Requirements, negative consequences can occur when the security discipline follows property design. There can be similar significant failures when risk mitigation and resilience measures are implemented in a silo and without proper integration and expertise.

Catastrophic Event 1	Your site suffers costly power outages due to flood-damaged electrical infrastructure.
Isolated Mitigation Efforts	Mechanical and electrical engineering consultants recommend moving the generator to the roof, contingent on a structural analysis.
	A structural engineer determines where to locate the generator to avoid the need to reinforce the roof or penthouse framing.
	The project is tendered, and the work is completed before the next flooding season.
Two Years Later	
Catastrophic Event 2	Hurricane-related storm surge covers the site with a metre of water.
Recovery Day 1	The relocated generator survives the flood, but the main fuel tank–still in the basement–is lifted off its foundation by the water, severing the piping.
	Crews realize the fuel pump has also been lost to the flooding–it was cheaper to replace it than to move it to the penthouse after the first flood.

Recovery Day 2	●	The flood waters recede but the next possible fuel delivery is 24 hours away.
	●	The generator can only run for two days on the fuel in its day tank before shutting down.
	●	The fuel truck arrives but can't pump because they were expecting to gravity-fill a below-grade tank.
Recovery Day 3	●	Another day passes until the fuel supplier can dispatch a pumper truck.
	●	The generator is restarted. Crews begin cleanup and damage assessment.
Recovery Day 4	●	Your tenant is unable to restart critical IT systems.
	●	Crews realize their server room has water damage: the structural engineer located the generator directly above it and close to a roof drain.
	●	Rainwater pooled around the drain and seeped into the building through poorly flashed roof penetrations.
	●	The tenant's equipment, including much of its data, is destroyed.

This scenario is not exaggerated: variations of this incident sequence played out all across New York and New Jersey before, during and after Hurricane Sandy in 2012.[33] It played out at hospitals, data centres, police stations and fire halls, and other critical infrastructure providers–many of which had received funding following Hurricane Andrew in 1992, to prepare them for the next big storm.

[33] FEMA P-942, Mitigation Assessment Team Report: Hurricane Sandy in New Jersey and New York (2013)
https://www.fema.gov/media-library/assets/documents/85922

Safe-to-fail design

We view situations from the perspective of our education and experience. Planning and design are riddled with implicit assumptions that we are not aware we are making, and a structured approach can help us to draw these out and correct for them. During Driver 1: Site Selection, we illustrated how to assess a hazard through space, time and various operating contexts. This same process can facilitate a discussion that incorporates a hazard's corresponding and coincident hazards, cascading impacts and dynamic operating environment.

In the flood example, everyone could have coordinated from the beginning of the project instead of interacting with each party in sequence.

> *The stated project objective was to protect the generator from a flood, but the actual project objective was to maintain enough power during a flood to supply our life safety and tenant's critical loads. There is a key distinction between the two.*

If we are subject to a flood hazard, a protective strategy will only get you as far as the flood you designed for. Instead of trying to prevent the flood, we can assume the flood and proceed from that point.

Assume that the site will flood. Unless we have dry-flood-proofed our entire building, our basement will also flood, so we know the generator will also flood. That level of flooding means that the neighbourhood will also be underwater, potentially for several days. If we did move the generator and everything connected to it, would we have enough fuel to ride out the flood until the waters receded? If your building engineer/operator is in the room, he or she can answer this question for you. The mechanical engineer might remind you that the fuel tank must remain in the lowest basement level by code, so all the piping should be braced, and the tank replaced with one functioning as a pressure vessel. The structural engineer will indicate that we should design the tank anchorages to resist uplift. The architect knows the layouts of the tenant spaces and may object when the structural engineer suggests doing work above a server room.

Life cycle cost and resilience

While a conventional project cost estimate involves the construction cost only, the incorporation of life cycle cost in a cost estimate gives the project team credit for investments in quality, durability and energy efficiency where they result in lower operating costs over the life of the facility. The benefits this has had on the sustainability of building projects is well-documented.

Similarly, life cycle costing can support investment in resilience by incorporating the cost of risk. Explicitly, the insurance premiums paid over the life of the facility will reflect the cost of risk. However, as operational value continues to concentrate, business interruption costs continue to rise. Today's covered perils may become tomorrow's foreseeable weekly power outage in a changing hazard context.[34] We can no longer expect to transfer all risk to an insurer.

We know that prevention is cost-effective, but nearly 87% of disaster-related spending on aid goes into emergency response, reconstruction and rehabilitation, and only 13% toward reducing and managing the risks before they become disasters.

> *We already know that every USD 1 invested in prevention saves, on average, USD 5 in future losses.*[35]

That statistic is itself compelling, particularly when one considers that as the frequency and severity of extreme events increase, that return on investment/ avoidance of loss will only increase.

Beyond the explicit cost of risk, however, incorporating resilience as a distinct design objective in an integrated life cycle costing exercise can further justify the capital cost of sustainability measures:

- Reduced operation and maintenance costs can offset the capital cost to upgrade the building envelope to include high-performance glazing, insulation and air barriers. These measures also allow us to maintain survivable temperatures for longer during an outage, potentially avoiding evacuation and even maintaining normal operations through the outage.[36]

- Reduced operation and maintenance costs can offset the capital cost of a higher-efficiency HVAC design and BAS system. These measures also allow us to heat or cool small floor plate areas, allowing a skeleton crew to maintain operations during an outage.[37]

- Savings in electricity consumption can offset the capital cost of higher-efficiency lighting design. It will also allow us to stretch limited generator fuel for longer during an outage.[38]

---

[34] Pacific Gas & Electric uses planned power shutoffs to manage public risk during extreme events, https://www.pge.com/en_US/safety/emergency-preparedness/natural-disaster/wildfires/public-safety-power-shutoff-faq.page. The experience during the 2019 California wildfires is a case in point. https://www.npr.org/2019/10/27/773753138/nearly-1-million-customers-to-lose-power-in-planned-pg-e-power-outages

[35] Zurich Insurance Company Ltd (2018) The Zurich Flood Resilience Program Phase 1 from 2013-2018. Other studies by FEMA and others estimate loss-avoidance return on investment in resilience measures as high as 1:9 and even 1:15 in various catastrophes when uninsured losses are included.

[36] HVAC Case Study: Longo's Food Store-57,000 sqft single storey retail building, Stouffville, Ontario. Reference also WBDG-Whole Building Design Guide - "Building Envelope Design Guide - Introduction" https://www.wbdg.org/guides-specifications/building-envelope-design-guide/building-envelope-design-guide-introduction

[37] Plenum Case Study: 3,000 sqft, single storey, inline Starbucks Restaurant, Stoney Creek, Ontario. IDP Process Case Study: 6,000 sqft, single storey CIBC retail, South-Western & Central Ontario. Reference also WBDG-Whole Building Design Guide- "High-Performance HVAC" https://www.wbdg.org/resources/high-performance-hvac

[38] WBDG-Whole Building Design Guide - "Energy Efficient Lighting" https://www.wbdg.org/resources/energy-efficient-lighting.

Integrated systems commissioning

ASHRAE[39] is the building industry's de facto authority on commissioning and has authored several associated guidelines and standards. ASHRAE defines commissioning as "a quality-focused process for enhancing the delivery of a project. The process focuses upon verifying and documenting that all of the commissioned systems and assemblies are planned, designed, installed, tested, operated and maintained to meet the Owner's Project Requirements."[40] Simply put, commissioning is supposed to assure that what the owner wanted is what is delivered.

There is significant value in the commissioning process when the Commissioning Authority is involved early in the project, and when the operational requirements are derived from first principles and well-documented. They can assist in developing plans and scripts to verify the actual functional requirements and the performance under failure, providing priceless assurance to the operator that the facility will behave as expected under pressure.

However, the Commissioning Authority is often not brought onto the project team until after the design is complete. At that point, their greatest potential value to the project is lost.

During procurement and construction, there are five levels of verification:

1. Factory acceptance testing

2. Site acceptance testing

3. Energization/start-up

4. Functional testing

5. Integrated testing

If a Commissioning Authority is not engaged nor a formalized commissioning process specified, individual system subcontractors will generally just ensure their equipment starts properly (Level 3). They may then hand over the systems without anyone completing the fine-tuning required and verifying whether the system meets the design intent.

Functional testing involves system-level verification, for example, that chillers, fans, ducts, fan coil units and controls are working together to achieve the specified conditions in workspaces, LAN rooms and labs. The bulk of the Commissioning Authority's verification oversight generally occurs at this level. Verification is often via representative sampling, where samples of 2% or 10% of units are measured, and if the sample passes, the building passes.

---

[39] America Society of Heating, Refrigeration, and Air-Conditioning Engineers.

[40] ASHRAE Guideline 0-2013, The Commissioning Process, and ASHRAE/IES Standard 202-2018, Commissioning Process for Buildings and Systems.

Integrated testing is coordinated with whole-systems testing and verification. It tests the interfaces between systems, and while commonplace in mission-critical environments, it is still exceptional in commercial environments. A common integrated test is the "black-out" or "pull-the-plug" test, which verifies the performance of everything in the building when the main power is lost. *It is also how we validate our incident sequences.*

Commissioning challenges in a conventional delivery environment

As a representative of the owner, the Commissioning Authority often finds itself in an adversarial relationship with the contractor and a delicate relationship with the engineer. In a conventional delivery model, especially when engaged after design, the Commissioning Authority's job is to verify that what is constructed meets the design intent. They are provided with the engineer's system design and expected behaviours and verify the work accordingly.

In contrast, in an integrated environment (as well as in mission-critical settings), the Commissioning Authority has the freedom, and often the mandate, to verify the design itself. The engineering community can find it challenging to adjust to this culture shift. It requires a significant amount of trust between all participants and documentation of functional requirements that are rarely well-defined in the contract documents.

For example, returning to our server room example from Driver 3: Incident Sequencing, in designing the cooling system for our server room, the engineer had to make assumptions about the thermal resistance and airtightness of the room itself. Level 4 verification would check that the output temperature meets the design and the required BTUs of cooling are present. Level 5 verification would typically check that in the event of a mains power failure, the system restarts properly on generator power and then continues to operate on return to main power. To verify that the room does not overheat during a temporary outage, we would need to run the same test with a load bank generating heat in the room, and measure the rise in room air temperature as the equipment stops and restarts.

If everything meets the specification, but the room still overheats, this does not mean the design was wrong. It may simply be due to a different wall finish, or the room is more airtight than expected. One or more of the design assumptions needs to be corrected and the whole system rebalanced. When everyone is on the same team, this process is not adversarial. The goal isn't *being right*; it's about *getting it right*.

The U.S. Green Building Council now requires Measurement and Verification for some time after occupancy to achieve LEED certification for exactly this reason. Early LEED buildings were extremely efficient on paper, but once constructed, often failed to meet the projected energy consumption targets, some spectacularly so. Verification of actual performance, and by extension the underlying design assumptions, is critical if we want to understand how our facilities will respond to shocks and stresses.

The Growing Role for Resilience Champions

As resilience gains more traction in the commercial real estate industry, we expect a designated role for its oversight to emerge in the design community, similar to how sustainability consultants emerged out of the green design movement.

AFTERNOTE

You have now collected all of this data. You have followed one or more of the Drivers to address the operational resilience of your property. You'll likely be wondering what happens now.

> *All of your work boils down to a question of performance. You determined how the performance of each of the property functions is affected by a failure or other event. You know what resources you need to make good that reduction in performance.*

In Driver 1: Site Selection, your LRA exposed the inherent risks to the site, and you looked into how to avoid or otherwise address them. Generally, these don't require additional resources, and you are improving the assurance of continued performance rather than dealing with a direct reduction.

However, in Driver 2: Planning Envelope, you get to the heart of how the property continues to function during a service interruption. You are buying time with your resources; the property remains habitable for x days in the absence of electrical supply due to these measures, which cost $y.

The same applies to Driver 4: Security Requirements and Driver 5: Integrated Design. Driver 4 addresses the residual risks arising from the measures that arise from the first two Drivers, while Driver 5 brings a design efficiency to the whole. These Drivers address the risks inherent in the property itself, and you can say what the investment means directly in risk exposure, specifically the whole cost of loss.

Driver 3: Incident Sequencing is all about managing the impact of an event on your operating performance. It is the one that most closely connects to corporate reporting. The first thing that you were able to do was say how a hazard would affect the property's operational performance (and its occupants). You have the incident profile that shows the expected level of performance over time. You articulate the effects in terms of production lost, or capability impaired or coverage interrupted. The metric used doesn't matter so much as it has to reflect an output of performance and time that the corporate staff can use.

For example, let's say that the effects of a significant flood will cause a 60% loss in performance. We can calculate what that does to the share price. We can also directly calculate the **total cost of loss** and the **maximum time of business interruption** to inform the underwriters. We can then propose a series of risk treatments that improve the incident profile and repeat the calculations of share price impact and underwriting parameters. The corporate staff can precisely equate the investment in resilience measures to the overall protection of performance.

These calculations are relatively simple. The University of Waterloo Intact Centre on Climate Adaptation Factoring Climate Risk into Financial Valuation, dated March 2020, is a particularly useful guide. Typically, you would calculate the financial valuation of the property/operation affected by the hazards without treatment and compare it with the same valuations after the proposed treatments are applied. We are then able to say how investment in the proposed risk treatments affects the overall valuation of the business. These comparisons are frequently very compelling, but only if the calculation of performance uses reliable empirical data. Nevertheless, it is generally the same data that you routinely collect.

Timely data collection

As the operations manager for one or more properties, you will be interested in maintaining an efficient and reliable operation. In particular, you will wish to recognize issues and address them before they lead to failure, become problems and cause disruption and cost money. It is important to know what is coming. Recent developments in technology allow us to detect minor leaks and damage before they become visible and disrupt operations. Technology also allows us to predict how damage will occur and the impact over time. These simulation tools are commonly accessible with the advent of Building Information Management (BIM) databases.

However, operations practice doesn't always keep up with advances in technology. In this case, leveraging your existing operational routine to collect the data presents a unique opportunity for timely and predictive data collection every 12 hours. We've already mentioned anomaly detection. Use your janitorial and maintenance staff to provide regular scans of the same environment with each routine pass. These scans can be conducted using camera glasses, not dissimilar in weight and appearance to safety glasses. The images are processed, and anomalies are detected and highlighted for investigation by maintenance staff. This capability exists today.

The more valuable the tenant operations, the more valuable timely and accurate indicators of emerging issues become.