CHUBB®

# Risk Management Guide for Technology Companies

Introduction to the guide

# The number and cost of Errors and Omissions claims within the technology industry have been steadily rising.

# The majority of claims are triggered by breach of contract, non-performance or delay in delivery.

At the source of this type of litigation are a number of factors, including the following:

## Increases in project length

Long projects tend to see more changes to specifications along the way, which increases the likelihood of problems with change management and scope creep, allegations of missed milestones, project delay and, ultimately, contract non-performance. Technological advancement or obsolescence may become a factor if the technology provided within the contract is superseded. Further, over time priorities may change – geopolitical issues such as removal of governmental grants, tax breaks or new territory sanctions may all cause issues with long contracts.

## Use of non-standard contracts

Particularly prevelant where a technology firm is contracting with a much larger entity, such contracts are more likely to include unique terms and conditions that work against the technologists.

## Poor project management

Insufficient risk assessments prior to commencement including lack of continuous monitoring and collaboration throughout the course of the project can lead to failure.

## Growing industry competition

Greater competitive pressure on technology providers may increase the chances of over-promising and under delivering on their capabilities.

The purpose of this guide is to highlight some of the challenges technology companies face and provide insight into areas for consideration when contracting with customers.

All content in this material is for general information purposes only. It does not constitute personal advice or a recommendation to any individual or business of any product or service.

# Contract Management

Helpful hints and tips for general information purposes only

Contracts are the first line of defence in the event of a dispute, so clear and unambiguous wordings are crucial.

# Contracts typically include an array of terms and conditions; we have highlighted some requiring careful consideration

## Force majeure

Meaning ‘greater force’, this clause frees both contracting parties from liability or obligation following an event or effect that cannot be reasonably anticipated or controlled. It can include war, extreme weather events, acts of god, pandemics and sometimes business risks such as delay or failure by suppliers.

## Dispute resolution

A dispute resolution clause will outline resolution methods outside of litigation, i.e. mediation and/or arbitration. If there is no dispute resolution clause, then parties can jump straight to litigation unless the parties agree otherwise. Including arbitration or mediation provisions will provide the means to resolve customer disputes other than through litigation.

## Acceptance

Acceptance criteria would normally be included in contracts so there is no confusion as to when acceptance has occurred and the performance obligations are complete. Alongside the acceptance criteria, this clause details the scope, procedure and schedule for testing and what happens if problems are encountered during acceptance testing.

## Term and termination

This clause will define the term of the contract (if finite) and provide the contract renewal conditions, whether automatic or subject to renegotiation. It will also list the specific circumstances under which the contract can be terminated and by whom (for example, due to breach, for the convenience of one or other of the parties) and will outline the rights and responsibilities of the contracting parties upon termination.

# Contracts typically include an array of terms and conditions; we have highlighted some requiring careful consideration

## Outsourcing and resellers of services

Where such clauses exist one would normally expect to see included in these contracts language that limits your liability in the event that one of your suppliers fails to deliver as promised, leading to a delay in your delivery to your customer.

## Ability to re-negotiate

It is important to include a clause allowing for re-negotiation of the contract terms if, for example, a delivery date or milestone cannot be met, or if so many changes occur that the contract terms or performance obligations have become confused or unwieldy. Allowing for re-negotiation in such circumstances can mean breach of contract claims down the line may be avoided.

## Fixed dates

Agreements where there is an obligation to deliver on a fixed date(s) can be problematic if not strictly managed as remedies noted in the contract for delay are often punitive and uneconomic. If faced with this situation consider building in additional flexibility to address unforeseen delays which are caused by third parties.


## Limitation of liability

A limitation of liability clause serves to limit the amount and types of compensation one contracting party can recover from the other. Usual considerations are limited based on type of loss (direct, indirect, special punitive). Limited based on size, type of contract and / or risk profile of customer.

## Performance obligations

These are the specific promises agreed by all parties regarding the performance of the contract. Things to consider when agreeing these are:

- Critical employees expected to be present throughout the course of the contract
- Resellers or other third parties who are involved with a project
- Critical systems required
- Completion of statement of work
- Set milestones throughout contract clearly documented & signed off by both parties
- Re-negotiation clause within contract terms & conditions if there is a change in the scope of services
- Pre-agreed dispute resolution procedures

# Project Management

## Effective management is key to the success of any project. Below are some areas of consideration before, during and after the project life-cycle

### Before

- Documented risk assessment of the project
- Scope of project, feasibility, can customer requirements be met within timeframe given
- Development & quality practices of outsourcers
- Assessment of your customer. Are they a mature business with the required knowledge to collaborate effectively?
- Availability of critical staff/infrastructure both in your own company and your customers
- Regular review of risk assessment throughout project with action taken when factors change
- Consider whether the project would benefit from using a recognised project management methodology

### During

- Important project milestones monitored, acknowledged with customer sign off at each stage in place
- Continuous change management process to document customer requests, assess impact, importance, and cost of any amendments
- At mid-way point of project would an independent review of the progress be beneficial by someone outside the project team?

### After

- Have all areas of work been signed off as completed by the customer?
- Ongoing support and service requirements clearly documented and agreed under contract with customer
- Communicate to your customers any plans you may have to discontinue producing a product or to discontinue a service

# Quality Control

## Robust quality control systems at every phase of development will set standards for acceptable levels of:

- Reliability
- Functionality
- Compatibility with integral systems
- Deployment time
- Performance
- Stability
- Product life span
- Ongoing support and service

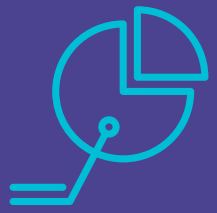
## Areas to consider for the development of a quality product or service should include:

- Alpha testing
- Beta testing
- Formal customer acceptance procedures
- Prototype development
- Statistical process control
- Vendor certification process
- Formal product recall plan
- Documents and records produced to applicable nationally or internationally recognised standards
- Retention of critical contracts, documents and records for clearly defined time standards
- Written and formally implemented quality control programme

# Network Security

It is good practice to have in place a formalised security programme and communicate its specifics to all employees and to ensure that the programme is updated, documented and adhered to.

# Good quality programmes include:



Impact analysis. With possible consequences such as loss of money, operational failures, loss or changes to intellectual property as well as identity theft these areas should be closely monitored.

Awareness training and schedules on how to achieve this, which should be balanced against the rating factors applied by impact analysis and improvements suggested whether internally or externally undertaken by you.

Review of all encryption, firewalls, virus protection, security protocols and intrusion detection used to safeguard the data of others and employee data stored on your networks and servers.

The following risk management considerations apply to companies' external networks as well as internal networks.

## Security management

Aligning an individual or team who has a reporting line directly into senior stakeholders, with ongoing responsibility for:

- Monitoring security threats such as virus infestations;
- Denial of Service (DOS) attacks and password theft;
- Communication of security needs and threats to the board

## Reliability

Consider adherence to best practice with regards to architecture design use of high-quality software, hardware and outsourced service vendors and how often you perform on-going maintenance, patching and upgrades.

## Response and disaster recovery planning

Record, investigate and resolve all security threats. Keeping log of these activities for future reference.

Contingency procedures such as working from home.

Internal and external communication including user awareness and training.

Disaster recovery plans should be regularly reviewed, updated and tested at regular intervals. This programme usually includes both physical incidents, information breaches as well as any compromise to communications security and disruptions of services to third parties.

## IT access authorisation/ revocation

Establish access authorisation procedures for all your systems including BYOD (bring your own device) whether for employees, past employees and contractors. Prevent former employees from accessing your systems by revoking their access or authorisation codes. Consider providing all contractors and employees with security training commensurate with their level of access. Phishing awareness training programs are readily available and could help prevent subsequent data incidents.

+ *See more on next page*

*Continuation*

# The following risk management considerations apply to companies' external networks as well as internal networks.

## Ensuring Redundancy

Design your network in such a way that traffic cannot be lost or interrupted due to a compromise.

Mirror data and back up onto a non-connected/segregated/air gapped part of the network to minimise or eliminate downtime in the event of an interruption to service.

Customer expectations with regard to network reliability, redundancy and availability should be considered and be incorporated within your service level agreements.

## Privileged Accounts

Ensure that separate user and administrative accounts are in place, with users having restricted rights. Administrators should not have administrative rights to their own workstation.

## Multifactor Authentication

Enable Multifactor Authentication on all external remote access into your network (whether by employees or authorised third parties), internal admin and privileged accounts and on access to backups.

Ensure MFA is implemented by use of 'something you know' as the first factor, and 'something you have or are' as the second factor.

## Detection & Response Tools

Activate EDR tools across all endpoints.

Ensure Intrusion Detection and Prevention software is active on firewalls, firewall logs are monitored and retained for 90 days.

## Testing and validation

Invest in regular, frequent network vulnerability scanning by an outside vendor to validate that your security programme is being adhered to. Ensure controls are appropriate and effective as well as highlighting any improvements in the framework adopted.

## End of Life and End of Support Systems

Consider adherence to best practice with regards to architecture design use of high-quality software, hardware and outsourced service vendors and how often you perform on-going maintenance, patching and upgrades.

# Operational Controls

## Intellectual Property rights

Intellectual Property (IP) principally consists of copyrights, trademarks, design rights and patents. Each of these may represent valuable assets for businesses competing in both traditional industries and services as well as players in the innovative sectors.

Protection and exploitation of IP is therefore a key factor for most technology businesses today. The potential for costly (both in terms of damages and legal costs) as well as reputation damaging litigation means that it is vital for businesses not only to protect their own IP but to manage the risk of infringing other IP.

In addition to claims for infringement of IP rights, businesses should be aware of potential liability and reputational damage associated with violations of privacy. In the UK, the Data Protection Act 2018 places controls on the collection and use of information. This is not the subject of this risk management guide.

## Advertising materials and product brochures

Consider a legal review of all advertising and marketing materials with regard to the promises explicitly made or implied to customers.

## Sales and marketing

Consider developing sales and marketing training programmes that aim to control product oversell and over-promising.

*Continuation*

# Operational Controls

## Formal disaster recovery, business continuity and breach response planning

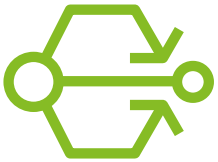
Having a formal DRP and BCP can be invaluable should disaster strike and normal business operations are interrupted. Plans should allow for sufficient IT recovery, prevention of data loss and maintenance of product and service provision to avoid breach of contract claims.

Further, a data breach response plan will assist with containment of any data security incident and mitigate both the immediate and long-term impact on revenues.

All such plans must undergo annual review and testing to remain effective and relevant to current business needs.

## Certificates of insurance from vendors and subcontractors

Obtaining certificates of insurance from all vendors and subcontractors as evidence that they have appropriate Professional Indemnity policies in place, to at least the same limit as your own insurance helps to provide protection should something go wrong.



## Network redundancy and availability

Design your network in such a way that traffic cannot be lost or interruption due to a break in the network. Be capable of backing up or mirroring both customers' and your own data on another part of network or elsewhere to minimise or eliminate downtime in the event of an interruption to service. Ensure that the network allows for load balancing at times of peak capacity.

# Disputes and Allegations of Non-Performance

## Regular Review of Potential Incidents

Carefully analyse all non-performance losses, claims and litigation as well as their causes. Consider including all suits, potential suits, complaint letters, disputes or any other circumstances alleging non-performance of your product or services. A thorough understanding of actual or potential disputes can be a window on future litigation problems and can be used to help identify and eliminate sources of loss.

## Contract Disputes/Non-Payment

If a contract is in dispute or a customer is withholding payment, you should strive to work with that customer to resolve the dispute and avoid litigation. Positive dialogue and frequent, open discussion concerning the viability of any project as it progresses enables both parties to resolve disputes before they get out of hand and allows for corrective action when a project hits a snag.

# Why Ignite?

## Chubb's Technology offering can now be traded on line via our e-trading platform Chubb Ignite.

Chubb Ignite is designed for brokers to trade with us quickly and simply. The intuitive design and client-centric experience allows a broker to quote with us in minutes, bind in seconds and produce instant documentation.

### Self-service on Chubb Ignite What can be done?

- You can see the portfolios of covers all in one place: quotes, policies and renewals, with minimum underwriter intervention
- Ability for you to quote, across all products and receive documentation within minutes
- Flexibility for you to alter cover options, limit and deductible options and also commission levels
- Bind your own risks, whether it be a quote or a renewal and receive policy documentation instantly
- Mid term adjustments are also available for you to make
- Copy and modify your quotes in order to show your client different options

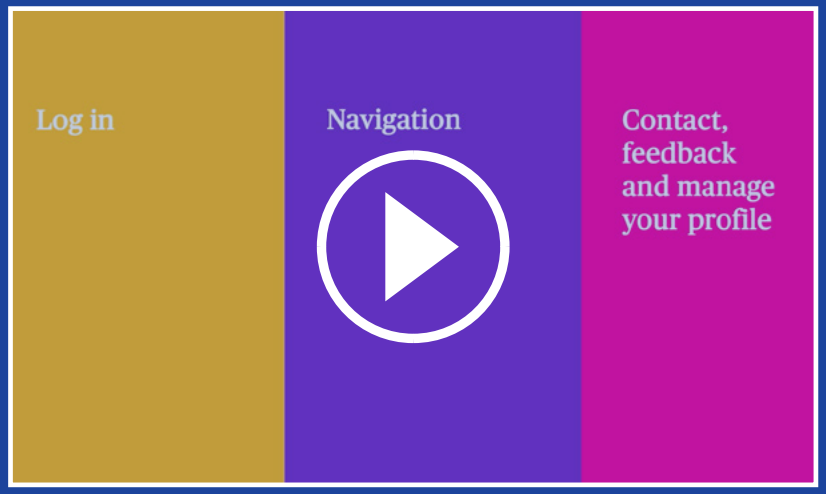
# Why Ignite?

## Logging on to Chubb Ignite

Gaining access is easy. Simply log on to Chubb Ignite and follow the registration process

Watch our short training videos to find out how to use Chubb Ignite:


An introduction to Chubb Ignite




A guide to Chubb Ignite

# Why choose Chubb?

At Chubb, we combine the precision of craftsmanship with decades of expertise to deliver the very best insurance coverage and service to technology businesses of all sizes.

With operations in 54 countries and territories, we have been a global market leader in the technology sector for many years and we continue to evolve to meet the needs of our clients. Our team of technology specialist underwriters in the UK & Ireland are here to support technology clients' as they grow into new and emerging areas and provide the best solutions for Technology risks. We understand that no two business are the same, so we offer tailored solutions specifically designed to suit a companies' needs and buying criteria.

*With a global network of 550 Risk Engineers, Chubb has been providing risk management, loss mitigation and prevention services to our clients around the world for many years.*

Increasing globalisation, new business models, changing technology and evolving risk management philosophies - as a business faces these challenges, we customise our approach to help technology insureds understand and mitigate their technology professional indemnity, cyber, casualty, property and business interruption exposures.

Our Technology Industry Practice is also supported by our award winning claims team which is made up of technology claims specialists and expert loss adjusters situated around the globe. Our claims ethos is to listen and focus on the particular needs of each client. We understand the importance of timely and effective settlements of each claim. We appreciate that how we handle claims is the acid test of what we do.

chubb.com/uk-en/business/technology

Chubb. Insured.℠



UK 8148-IN 01/22