Sample Training Request Letter

Use the following sample request letter, or elements of it, to justify the time and budget required to complete SANS training to your manager. Simply copy and paste text into an email to your manager, then make any necessary adjustments to personalize the information. Once you hit send, you’ll be one step closer to gaining the skills required to protect your organization and advance your career.

**Subject: Request for cybersecurity training from SANS Institute**

[Decision Maker Name],

### I’m writing to request time and budget approval to take the SANS Institute’s information security course [LDR525: Managing Cybersecurity Initiatives and Effective Communication](https://www.sans.org/cyber-security-courses/managing-cybersecurity-initiatives-and-effective-communication/) and its associated [GIAC Certified Project Manager (GCPM)](https://www.giac.org/certifications/certified-project-manager-gcpm/) exam.

**Why we need this course?**

Many cybersecurity professionals are highly technical but often unfamiliar with project management terminology, methodologies, resource management, and leading teams. Overseeing diverse groups of stakeholders and team members, estimating resources accurately, as well as analyzing risk as applied to different organizational structures and relationships is a struggle for many new technical project leaders. Today’s virtual work environment only increases these complexities. It is critically important to understand how to leverage a wide range of development approaches and project management framework components to maximize resources across various business units for project success.

After taking [LDR525: Managing Cybersecurity Initiatives and Effective Communication](https://www.sans.org/cyber-security-courses/managing-cybersecurity-initiatives-and-effective-communication/), I will confidently lead security initiatives that deliver on time, within budget, reduce organizational risk and complexity while driving bottom line value.

I will also have interactive learning via 35 different exercises throughout the class.

**Once I’ve completed the course, I’ll be able to:**

* Understand predictive / waterfall, adaptive / agile development approaches and how they interact with product and project life cycles.
* Learn how to use and implement lean / agile tools, complexity models, root cause analysis
* Recognize the top failure mechanisms related to security projects, so that your projects can avoid common pitfalls
* Create a project charter which increases stakeholder engagement
* Document project requirements and create requirements traceability matrix to track changes throughout the project lifecycle
* Clearly define the scope of a project in terms of cost, schedule, and technical deliverables
* Develop a project schedule, including critical path tasks and milestones
* Cultivate user stories to drive adaptive sprint cycles
* Create accurate project cost and time estimates
* Develop planned and earned value metrics for your project deliverables and automate reporting functions
* Effectively manage conflict situations and build communication skills with your project team
* Analyze project risks in terms of probability and impact, assign triggers and risk response responsibilities
* Create project earned value baselines and project forecasts based on actual performance
* Communicate effectively with stakeholders, technical staff, and management teams

**Associated Certification:** [[**GIAC Certified Project Manager (GCPM)**](https://www.giac.org/certifications/certified-project-manager-gcpm/)](https://www.giac.org/certification/network-forensic-analyst-gnfa)

The GIAC Certified Project Manager (GCPM) certification validates a practitioner's knowledge of technical project management methodology and implementation. GCPM certification holders have demonstrated the critical skill sets associated with making projects successful, including effective communication and time, cost, quality, procurement and risk management of IT projects and application development.

* See the “Exam Certification and Outcomes Statements” section of the [GIAC Certified Project Manager (GCPM)](https://www.giac.org/certifications/certified-project-manager-gcpm/) page for a list of covered topics.

**Expected Cost**

I’d like to take LDR525 [fill in either: (1) “in person at [event name], from [start date] through [end date].” or (2) “online, with four months of access to the SANS OnDemand training platform.” or (3) “online, via Live Online from [start date] through [end date].”].

The attached unpaid invoice shows the cost of the course [retrieve this from the course registration page and attach]. Details include:

|  |  |
| --- | --- |
| Course fee  | [$X,XXX] |
| Subtract Early Bird / Online Training Discount | [-$XXX] |
| GIAC Certification fee | [$XXX] |
| OnDemand Bundle fee | [$XXX] |
| Travel and Hotel\* (for live training only)                            | [$XXX] |
| Meals (for live training only)                                                                     | [$XXX] |
| **Total estimated cost:** | **[$X,XXX]** |

\*Special hotel rates for conference attendees range from [$XXX]/night, but I must register before [xx/xx/xxxx].

**Testimonials**

**“I am gaining so much knowledge from this course via the instructor and the exceptional course material."** *- Lakendrick Fisher, USAF*

***“*I really like all the material provided and the examples given. All of them apply to real life so they are very useful*."****– Anabel Sosa, BBVA*

I believe this course will substantially improve my ability to do the specific work we need. It’s written and taught by globally recognized experts and will deliver practical, hands-on training that I can apply as soon as I return to work.

Additional course information can be found on the SANS website at <https://www.sans.org/cyber-security-courses/managing-cybersecurity-initiatives-and-effective-communication/>

Thanks for your consideration,

[Add standard signature]

Attachment:

Unpaid Invoice for SANS training [find at <https://www.sans.org/cyber-security-courses/managing-cybersecurity-initiatives-and-effective-communication/> and attach to email]